



Agenda Item 4.1

<b>Meeting</b>	<b>Audit, Risk and Assurance Committee</b>
<b>Date</b>	<b>6 February 2024</b>
<b>Location</b>	<b>Video Conference</b>
<b>Title of Paper</b>	<b>ICO Audit - Recommendation Action Tracker</b>
<b>Presented By</b>	<b>Deputy Chief Constable Professionalism</b>
<b>Recommendation to Members</b>	<b>For Discussion</b>
<b>Appendix Attached</b>	<b>Yes: Appendix A - ICO Audit Recommendations Dashboard</b>


**PURPOSE**

The purpose of this paper is to provide the Audit, Risk and Assurance Committee with a progress update of activity undertaken in respect of ICO Audit Recommendation Action plan for Governance and Accountability and Personal Data Breach audit strands.

Members are invited to discuss the progress detailed within the report.

## 1 BACKGROUND

- 1.1 A report on Police Scotland's management of recommendations made by ICO in respect of Governance and Accountability and Personal Data Breach reporting. The report is produced on a quarterly basis for Members review. A copy of the Dashboard is available at **Appendix A**.
- 1.2 All recommendations are assessed in terms of the risk they present to Police Scotland using the Internal audit grading structure for consistency of approach. All recommendation are assessed as follows:

 Moderate risk exposure - controls are not working effectively and efficiently and may create moderate risk within the organisation

## 2 FURTHER DETAIL ON THE REPORT

- 2.1 Refer to Appendix A – ICO Audit Recommendations Dashboard.

## 3. FINANCIAL IMPLICATIONS

- 3.1 There are no financial implications in this report.

## 4. PERSONNEL IMPLICATIONS

- 4.1 There are no personnel implications in this report.

## 5. LEGAL IMPLICATIONS

- 5.1 There are no legal implications in this report.

## 6. REPUTATIONAL IMPLICATIONS

- 6.1 There are no reputational implications in this report.

## 7. SOCIAL IMPLICATIONS

- 7.1 There are no social implications in this report.

**8. COMMUNITY IMPACT**

8.1 There are no community implications in this report.

**9. EQUALITIES IMPLICATIONS**

9.1 There are no equality implications in this report.

**10. ENVIRONMENT IMPLICATIONS**

10.1 There are no environmental implications in this report.

**RECOMMENDATIONS**

Members are invited to discuss the progress detailed within the report.

OFFICIAL



# ICO Audit Recommendations Dashboard

# Reporting overview

28-30 June 2023 –	Audit conducted
6 September 2023	Action Plan Submitted
13 September 2023	Audit Published
• 12 December 2023	At the request of DPO, an informal discussion regards the intended activity for November and December took place on 12 December. This engagement was positive and enabled further exploration of potential remediation actions.
19 February 2024	Submission of update - action plan and evidence
4 March 2024	Interim Progress Follow-up  Evidence of progress to be provided on actions marked 'high' and 'urgent', and a written update on any medium/low actions in the action plan.
September 2024 (date TBD)	Completion Sign Off  SIRO will provide written assurance that actions which were against low or medium priority recommendations have been completed and provide documentary evidence that actions against high and urgent priority recommendations have been completed.

The Information Commissioner reserves the right to consider formal enforcement measures if PSoS does not make any meaningful progress to address the actions ICO have highlighted as 'urgent' and/or 'high'.

# Activity Focus – Nov/Dec '23

Total Recommendations	In focus	Closed	Pending	Progressing	Delayed
43	21	2	6	9	4

## PSoS Risk

All risks are recorded as Moderate risk exposure - controls are not working effectively and efficiently and may create moderate risk within the organisation

## ICO priority Key

### **Urgent Priority Recommendations -**

These recommendations are intended to address risks which represent clear and immediate risks to the data controller's ability to comply with the requirements of data protection legislation.

### **High Priority Recommendations -**

These recommendations address risks which should be tackled at the earliest opportunity to mitigate the chances of a breach of data protection legislation.

### **Medium Priority Recommendations -**

These recommendations address medium level risks which can be tackled over a longer timeframe or where some mitigating controls are already in place, but could be enhanced.

### **Low Priority Recommendations -**

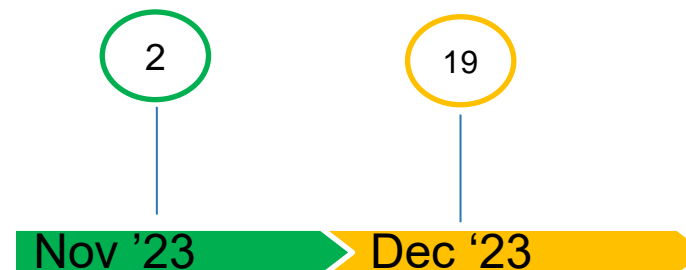
These recommendations represent enhancements to existing controls to ensure low level risks are fully mitigated or where we are recommending that the data controller sees existing plans through to completion.

## Activity Focus – Nov/Dec '23

---

21 recommendations were the focus of activity during November and December period.

- 2 recommendations have been closed.
- 6 recommendations are pending and require approval for closure via Data Governance Board and external publication thereafter.
- 9 recommendations have progressed but require further activity prior to closure.
- 4 recommendations are delayed, awaiting decision/output of Resource Maximisation Group – Delayed.



### Challenges to delivery

- Multiple business area interdependencies
- Resource and financial pressures
- Consultation

# Closed

Recommendation	ICO Priority	PSoS Risk	Date	Status
A06 Meeting Notes of DGB	High	M	Nov 23	DGB minutes recorded with effect from 2 November 2023.
A07 Standing Items on Departmental Management Meetings	Medium	M	Nov 23	<p>All Data Owners Groups and Data Retention Oversight Group now have:</p> <ul style="list-style-type: none"> <li>- Agenda</li> <li>- Action Log</li> <li>- Decision Log</li> <li>- Papers for discussion (i.e. not all verbal updates)</li> <li>- Standing item on the agenda for Matters to be Escalated to DGB</li> <li>- DGB reference on TOR</li> </ul> <p>Info Governance SOP is also currently under review and where opportunity exists to add further clarity this will be included.</p>



# Pending Approval - DGB

Recommendation	ICO Priority	PSoS Risk	Date	Status
A04 Record specialist roles acceptance	Medium	M	Dec 23	Options explored to find a cost effective method of ensuring those in specialist roles are aware that they have additional role responsibilities and that these are documented. Paper for decision tabled at DGB 1 February 2024 and thereafter implementation.
A05 Risk Management Policy	Medium	M	Dec 23	Review tabled at DGB, however previously not captured as formal record. Review undertaken. A paper clarifying the annual review of privacy notices, policies, SOPs and APD will be submitted to DGB on 1 February 2024 for approval and closure.
A09 Appropriate Policy Documents Review and Version Control	Medium	M	Dec 23	Review tabled at DGB, however previously not captured as formal record. Review undertaken. A paper clarifying the annual review of privacy notices, policies, SOPs and APD will be submitted to DGB on 1 February 2024 for approval and closure.
A10 – Policies & procedures regularly reviewed.	High	M	Dec 23	
A36 Privacy Information - Formal and Regular Review	High	M	Dec 23	
A32 formal review process for privacy information	High	M	Dec 23	Privacy notices were reviewed on 14 December and reformatted for accessibility requirements.  The forms will be submitted w/c 15 January for assessment of reading age prior to publication.  Options will be provided for alternative language requirements.  A paper clarifying the annual review of privacy notices, policies, SOPs and APD will be submitted DGB on 1 February 2024 for governance & assurance.

## Delayed - Pending Decision of Resource Maximisation Group

Recommendation	ICO Priority	PSoS Risk	Date	Status
A27 Formal Process to Determine and Record Lawful Basis Decisions	Urgent	M	Dec 23	<p>PSoS is clear on where consent is used, but noted this must be recorded accurately on its ROPA (IAR).</p> <p>Controls for recording lawful basis already present within DPIA and ISA processes.</p> <p>The IAR will be updated as noted below and used to initiate formal review schedule in conjunction with the DPIA tracker and ISA tracker.</p> <p>The update of the IAR is included on the IA Roadmap for 23-24.</p> <p>To further enable this work, a postholder is being identified and will be dedicated 100% for a temporary period of (up to 12 months) to:</p> <ol style="list-style-type: none"> <li>1. Update the data held</li> <li>2. Update the in-life processes</li> </ol>
A28 – Consent – Clarity	Urgent	M	Dec 23	
A30 Consent - Regular Review of Consents"	Urgent	M	Dec 23	
A31 Consent - Processes to Confirm Age	High	M	Dec 23	

# Activity Progressing

Recommendation	ICO Priority	PSoS Risk	Date	Status
A03 Review Information Assurance Officer and DPO Roles	High	M	Dec 23	A consulting paper was laid before JNCC on 21 December which informed members of a proposed change.
A11 Staff Understanding of Policies & procedures	High	M	Dec 23	Induction process being reviewed to assess suitability for inclusion. Evidence of reporting training compliance continues through CDO SMT & PASG to SIRO and through DGB. Evidence of monthly notifications and chase-ups continues to be available. Compliance rate remains lower than agreed threshold. Opportunities for CI being reviewed: dashboard reporting option in development by LTD and a reactive review schedule for training content refresh will be considered.
A13 Induction Training	High	M	Dec 23	Governance controls introduced for the effective monitoring of this -similar to those deployed for annual refresher training. Added as standing agenda item to P&D DOG. Efforts continue in improving training compliance rates, but compliance rate remains below agreed threshold therefore this recommendation cannot be discharged.
A14 Refresher Training	High	M	Dec 23	Efforts continue in improving training compliance rates however, compliance rate remains below agreed threshold therefore this recommendation cannot be discharged.
A29 Consent - Records	Urgent	M	Dec 23	An accuracy review of all processing records has been undertaken which included review of all Privacy Notices, DPIAs and ISAs.  The reference to consent as a lawful basis has been removed and replaced by Public Task in relevant instances.  Formal recording and review process is being considered as part of the IAR work.
A34 Privacy Information – Review communications to date	Medium	M	Dec 23	The model referenced by ICO is the model currently in use for privacy information communication and we will continue to improve as the technologies we use for processing evolve. (in) Review of techniques in use was undertaken and improvement opportunities identified for passive communication – interdependency with new Comms platform implementation.

# Activity Progressing

Recommendation	ICO Priority	PSoS Risk	Date	Status
A35 Review privacy notices	High	M	Dec 23	<p>Privacy notices were reviewed on 14 December and reformatted for accessibility requirements.</p> <p>The forms will be submitted for assessment of reading age prior to publication.</p> <p>Options will be provided for alternative language requirements.</p> <p>Annual Privacy Notice Review tabled at DGB, however previously not captured as formal record. A paper clarifying the annual review of privacy notices, policies, SOPs and APD will be submitted DGB on 1 February 2024 for governance &amp; assurance.</p>
A41 DPIA guidance – regular review	High	M	Dec 23	Review underway.
A43 DPIA – Review Schedule	Medium	M	Dec 23	Review underway

# Activity Focus – Nov / Dec '23

Total Recommendations	In focus	Closed	Pending	Progressing	Delayed
9	4	0	1	3	0

4 recommendations were the focus of activity during November and December period.

- 1 recommendation pending and awaiting approval for closure via Data Governance Board.
- 3 recommendations have progressed but require further activity prior to closure.

4

## Challenges to delivery

- Multiple business area interdependencies
- Resource and financial pressures
- Consultation

Dec '23

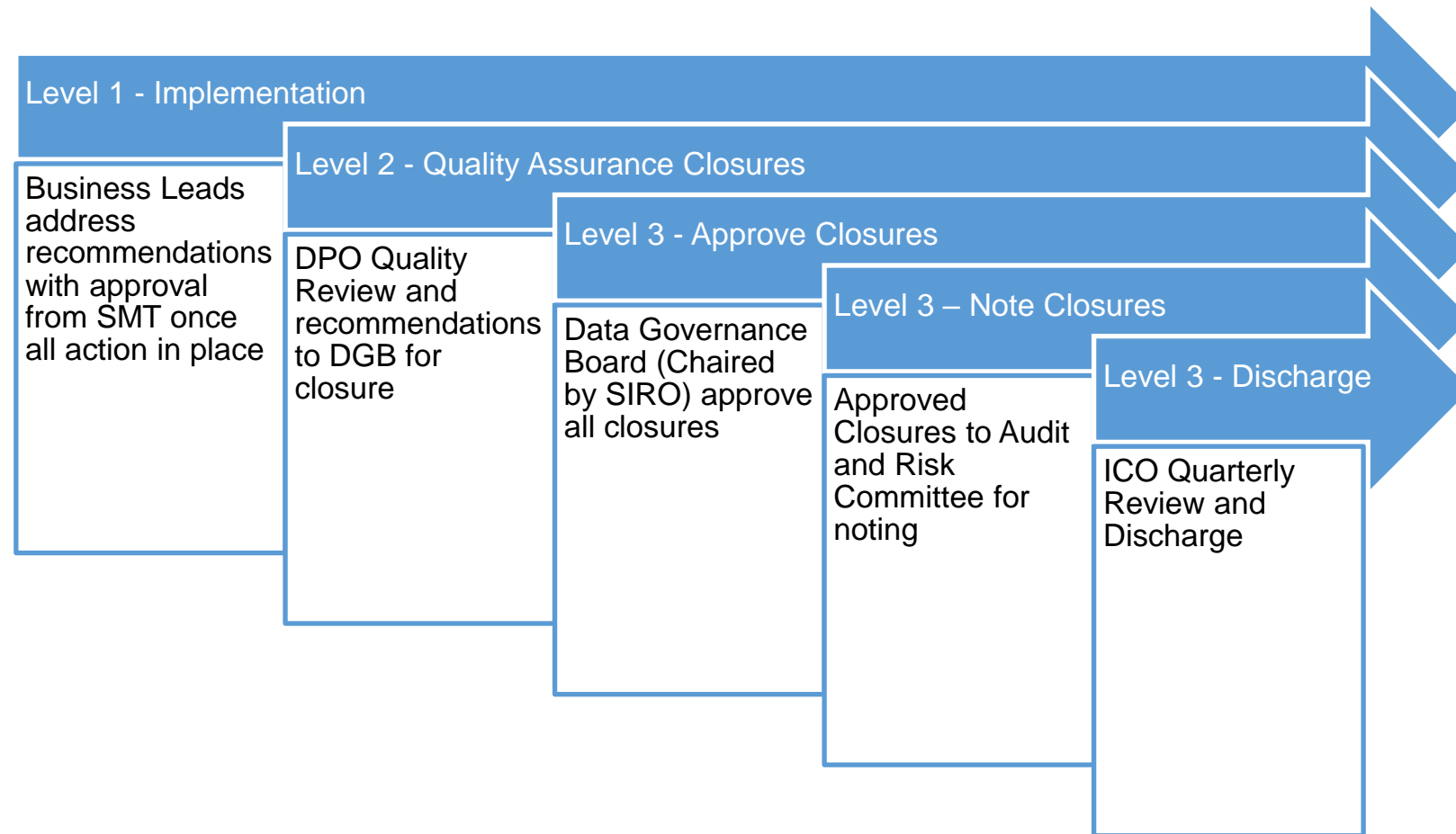
## Pending Approval - DGB

Recommendation	ICO Priority	PSoS Risk	Date	Status
B02 Policies & Procedures – regular review of DP compliance and version control (linked to A10)	Urgent	M	Dec 23	Review tabled at DGB, however previously not captured as formal record. Review undertaken. A paper clarifying the annual review of privacy notices, policies, SOPs and APD will be submitted to DGB on 1 February 2024 for approval and closure.

## Activity Progressing

Recommendation	ICO Priority	PSoS Risk	Date	Status
B03 Improve Training Compliance	High	M	Dec 23	Evidence of reporting continues through CDO SMT & PASG to SIRO and through DGB. Monthly notifications and chase-ups continues to be available. Dashboard reporting option in development by LTD was raised at the P&D DOG on 30/11/23 and further development work is being undertaken. Reactive review schedule for training content refresh is being considered.
B05 Review technical & org controls for detecting PDB	High	M	Dec 23	Ongoing monitoring of completion rates for training.  Continued escalation of issues to DOGs  Training compliance rates remain below threshold therefore action cannot be discharged.
B07 Review Record Retention SOP to include entry for breach log	Low	M	Dec 23	Records Retention SOP has recently been reviewed, updated and published following mandatory consultation. Submission has been made to Policy Support seeking addition and assessment as to whether this will require to go back through consultation. Recommendation will be discharged as soon as change implemented and published.

# Governance



\* All actions recorded in 4Action for effective management.