Scottish Government

Audit Outcomes Report

February 2023

Version 1.0

Information Commissioner's Office

Contents

1. Introduction

The Information Commissioner's Office (ICO) is responsible for enforcing and promoting compliance with the Data Protection Act 2018 (DPA 2018) and the UK General Data Protection Regulations 2018 (UK GDPR). Article 58 of the UK GDPR and Section 129 of the DPA 2018 gives the Commissioner power to carry out consensual audits of data controllers, in order to assess their compliance with good practice and legal requirements for the processing of personal data.

2. Scope

The agreed scope of the audit was based on concerns from existing intelligence around the data processing activities of the Scottish Government, input from the ICO Scotland Office, and the expertise of the audit team, with input from the Scottish Government's Data Protection Officer (DPO) and Head of Information Assurance and Data Protection.

The scope of the audit was agreed to cover three thematic areas:

Governance and Accountability – The extent to which information governance accountability, policies and procedures, performance measurement controls, and reporting mechanisms to monitor data protection compliance to both the UK GDPR and other national data protection legislation are in place and in operation throughout the Scottish Government.

Information Risk Management – The extent to which the Scottish Government has applied a "privacy by design" approach. Information risks are managed throughout the organisation in a structured way so that management understands the business impact of personal data related risks and manages them effectively to assure the business of the Scottish Government.

The Role of the DPO – The extent to which the Scottish Government has complied with their obligations under UK GDPR to appoint an independent DPO who is properly trained and resourced.

In addition, the Scottish Government requested that the ICO provide feedback on data protection risks and considerations in relation to the setting up and running of public inquiries within Scotland.

3. Approach

The agreed approach for the audit was a series of targeted engagements across a number of distinct areas of the Scottish Government and Executive Agencies that fall within the data controllership of the Scottish Government, in order to provide representative sampling of data protection performance and compliance.

Each engagement resulted in an exception report provided to the Scottish Government, detailing specific recommendations relevant to those areas. Themes and generalised comments will be drawn out of these engagements to provide an overview of the Scottish Government's level of compliance in this report.

The areas of the Scottish Government the ICO engaged with were:

- the Scottish Government's Central Information Governance (IG) function
- the Scottish Public Pensions Agency (SPPA)
- the Agricultural and Rural Economy Directorate (ARE)
- the Justice Directorate
- the Digital Health and Care Directorate (DH&C)
- the Propriety and Ethics Directorate.

The thematic areas of Governance and Accountability and Information Risk Management were reviewed in every participating area. The third thematic area of the audit, the Role of the DPO, was specific to the Central IG function.

4. Methodology

Audits are conducted following the Information Commissioner's data protection audit methodology. The key elements of this are a desk-based review of selected policies and procedures, remote interviews with selected staff, and a virtual review of evidential documentation.

Where weaknesses were identified during each engagement, recommendations have been made, primarily around enhancing existing processes to facilitate compliance with data protection legislation. In order to assist the Scottish Government in implementing the recommendations each has been assigned a priority rating based upon the risks that they are intended to address. Further information on the ICO rating system can be found in the Appendix. The ratings are assigned based upon the ICO's assessment of the risks involved. The Scottish Government's

priorities and risk appetite may vary and, therefore, they should undertake their own assessments of the risks identified.

Each thematic area was given an overall assurance rating as a result of the audit. These ratings are High, Reasonable, Limited, and Very Limited. Further information can be found in the Appendix.

4.1 Repeated Findings

It was noted during the audit that findings related to the Central IG function would apply across the whole of the Scottish Government, and as a result efforts were made not to repeat those recommendations across the further engagements with individual directorates and executive agencies. As a result some of the further engagements do not have significant numbers of recommendations, with the majority of issues having been identified during the Central IG engagement.

5. Overview

5.1 Governance

The Scottish Government has a particularly complex structure as a data controller, due to the extremely broad nature of the responsibilities it holds and the extensive requirements of the legislation that created it. Under data protection legislation the Scottish Government is a single data controller, with eight Directors General (DGs), covering 52 directorates and 10 executive agencies. As a result they are a single data controller covering dozens of extremely different functionalities, ranging across every aspect of Scottish public life. The directorates and agencies covered in the course of this audit were chosen to provide a representative sampling of different areas of operation and data processing.

There is a single DPO responsible for fulfilling all the responsibilities of the role as outlined in Article 39 of the UK GDPR. They are assisted in this by the Information Assurance and Data Protection (IADP) team, however this team does not sit under the management of the DPO in order to facilitate the DPO's ability to provide independent oversight and advice. Responsibility for day to day data protection compliance sits within each directorate, with the DPO and IADP team providing support and guidance as required.

The Scottish Government has appointed a Senior Information Risk Owner (SIRO), responsible for ownership of all Scottish Government information

risks. This position sits at DG level, and oversees an extensive risk management process that is deeply embedded across all areas of the Scottish Government. Individual executive agencies do not fall within the Scottish Government SIRO's scope of responsibility, and have their own senior risk owners in place.

The Information Governance (IG) Board provides oversight and governance of all IG issues, assisted by the Information Governance Practitioners Group which brings together operational level IG staff from across the Scottish Government and wider agencies to facilitate knowledge and resource sharing. In addition there is a Cyber and Information Security Sharing Group which provides similar opportunities for security staff across the Scottish Government.

5.2 Information Risk Management

There is a standardised approach to risk management used across the whole of the Scottish Government, including the executive agencies, with risk registers being used to track and manage risks in a pyramidal approach. Bottom level risk registers sit with major projects and individual business units, feeding upwards into division, directorate, and then DG level registers, and finally into the overarching Scottish Government corporate risk register. There is a well embedded methodology in place for the escalation of risks from lower level risk registers onto higher level registers.

Data Protection Impact Assessments (DPIAS) are standardised across the Scottish Government, and a reasonable level of awareness was found in most areas regarding their use. There is substantial guidance available to staff on how to complete DPIAs, and assistance can be sought from the DPO, the IADP team, or from a network of risk champions embedded across the Scottish Government.

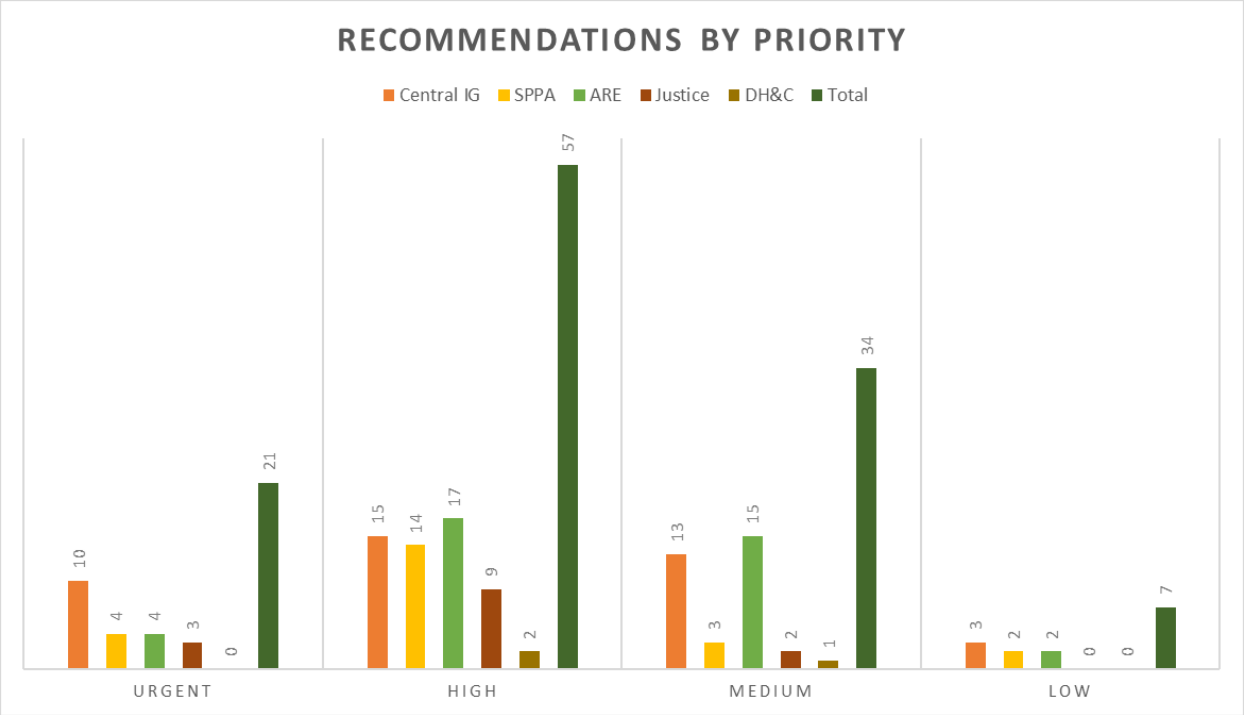
A lot of the work undertaken by the areas of the Scottish Government looked at during this audit happens in project or programme format. Some areas appear to have a strong understanding of the importance of information risk management to successfully carry projects through to completion, and several directorates indicated a very positive attitude towards consultation with the ICO under Article 36 of the UK GDPR.

6. Summary of Findings

The table below shows a breakdown of the assurance ratings of the individual engagements carried out through this audit.

	Governance and Accountability	Information Risk Management	Role of the DPO
Central IG	Reasonable	Reasonable	High
SPPA	High	Reasonable	Not Assessed
ARE	Reasonable	Reasonable	Not Assessed
Justice	Reasonable	Limited	Not Assessed
DH&C	Reasonable	Reasonable	Not Assessed

The graph below shows the breakdown of recommendations by priority across all aspects of the engagement, as well as the total number of recommendations for each priority.



The Scottish Government have indicated that they intend to address each of the recommendations made, and to create a risk based implementation plan to share with the ICO.

7. Key Findings

7.1 Governance Structures

Due to the structure of the Scottish Government and the legal underpinning for its creation, the DPO is required to oversee processing activities relating to a wide array of different public functions, which in

most other situations would be their own independent data controller. As the DPO is a standalone post and has not been allocated a team to assist with their work, they are reliant on the assistance of the IADP team to provide the additional resourcing necessary to fulfil their functions under Article 39 of the UK GDPR.

The arrangements for this assistance are informal, and appear to be successful because of the effective working relationship between the DPO and the Head of IADP. Given that the DPO relies on the IADP team in order to fulfil their formal duties, the Scottish Government may benefit from formalising the provision of resources to the DPO. As a minimum there should be a formal delegation of powers in place, making explicit which of the Article 39 tasks are being delegated to whom. However the Scottish Government should consider whether the permanent allocation of resources to the DPO may also be of benefit, rather than requiring them to borrow resources on an ad hoc basis.

Responsibility for compliance with data protection legislation sits at a divisional level, with the DPO and IADP team providing guidance and support but the operational work of compliance being undertaken by directorate staff. There is substantial variance between directorates, with some having allocated substantial, specialised resources and others having allocated little to nothing in the way of dedicated data protection resource. There is a risk that similar issues may be dealt with differently in separate directorates, due to differences in the allocation of expert resources, with the potential for a breach of Article 5(1)(f) of the UK GDPR.

The Scottish Government should review the availability of trained data protection resource in each directorate, and should ensure that the IADP team match their provision of support to the availability of resources in each area of the organisation. In addition, the Scottish Government should consider designating a role within each directorate or DG area as a key point of contact with the DPO and IADP team, potentially as either a deputy or assistant DPO or as part of the duties of a Deputy IAO role, and with reference to the bespoke needs and resourcing of each business area. The purpose of this role should be to ensure there is a sufficiently trained or specialised resource available within each directorate to provide on the spot assistance or guidance, and to facilitate smooth working relations with the DPO and IADP team.

7.2 Record of Processing Activities

The Scottish Government were unable to demonstrate a fully compliant Record of Processing Activity (RoPA), whilst much of the required

documentation is held it is spread across a range of sources and during interview there was a lack of awareness demonstrated regarding what all relevant documentation there was and where it was located. Much of the information is held in the Information Asset Register (IAR), and many interviewees pointed to the IAR when asked about a RoPA. However the IAR does not, on its own, meet with the requirements of Article 30 of the UK GPDR, in particular as its focus is on recording specific assets rather than acts of processing.

In addition, it was noted that there have not been any substantial efforts at data flow mapping or information auditing carried out across the Scottish Government. Some efforts have taken place, but they have been restricted in scope and the majority of interviewees were unaware they had taken place, and had not had the opportunity to input into them. Extensive and accurate data flow maps will assist the Scottish Government in ensuring that their RoPA is accurate, their IAR is up to date, and that their DPO is able to effectively input on processing activities as required.

When undertaking information audits or data flow mapping, it is important for the Scottish Government to ensure that this is not done in a silo by central IG staff. Input should be sought from staff across all directorates, and from a relevant range of seniorities. Restricting inputs to only those in certain roles or at more senior levels may result in inaccurate results, as the specific details of processing are often known most accurately to staff involved in day to day operational work.

7.3 Risk Management

Information risks are managed as part of a wider approach to general risk management. This framework is documented across a range of policies, procedures, manuals, and guides, and it was identified during the course of the audit that not all staff had an appropriate awareness of the specifics of the risk management framework. There was a fragmented and inconsistent awareness of how information risks were supposed to be managed and where responsibility for those risks sits. As a result, there is a serious risk of the Scottish Government failing in its Article 5(1)(f) of the UK GDPR obligations to properly secure personal data using both organisation and technical measures.

The Scottish Government should pull together the disparate sources of information on risk management into a single, authoritative resource, and should undertake ongoing efforts to drive awareness amongst relevant staff across central IG, directorates, and executive agencies. In addition,

where the practices of executive agencies diverge from the main Scottish Government these differences should be fully documented and authorised by relevant senior staff.

Current practice allows each directorate and executive agency to establish their own risk appetites. This had resulted in inconsistencies in how seriously different parts of the organisation treat information risks, and how those risks are escalated from operational levels to directorate and DG level risk registers, and whether they are escalated further to the corporate risk register. It is reasonable for each directorate and executive agency to have a level of discretion in how they approach information risk management, as they do operate in a variety of contexts and situations. However, the Scottish Government should provide guidance on risk appetite and risk escalation, and should standardise approaches across the organisation wherever possible.

7.4 Senior Information Risk Owner

It was identified during the course of the audit that the Scottish Government's SIRO holds ownership only for Scottish Government information risks, and does not take ownership of information risks for executive agencies. Executive agencies are required to take absolute responsibility for owning their own information risks, and no arrangements are in place for the Scottish Government to receive assurances about how these risks are being controlled. Given that executive agencies come under the ownership of the Scottish Government as a data controller, this creates a serious risk to data subjects for whom the Scottish Government is responsible as they do not take responsibility or ownership for controlling those risks when the processing activities sit with executive agencies.

Whilst the appointment of a SIRO is not a legal requirement, it can be a highly effective step in controlling risks by ensuring there is a clear point of ownership and assigned responsibility. However, having an appointed SIRO who is not responsible for owning all information risks within the organisation creates additional risks. The Scottish Government should identify whether they expect their SIRO to have ownership of all information risks facing the organisation, and if so they should take urgent steps to reform risk management practices across all executive agencies to add in lines of ownership to the Scottish Government SIRO. If not, the Scottish Government should revise their appointment of a SIRO to accurately reflect the duties of the role, and should ensure that each area of the organisation not under the scope of responsibility of the SIRO has effective, equivalent risk ownership in place.

7.5 Information Asset Owners

The Scottish Government has designated a substantial number of Information Asset Owners (IAOs), all sitting at Deputy Director level. Extensive guidance has been produced for IAOs, covering their duties and responsibilities, and there is a bespoke IAO training course developed by the Scottish Government. However, during the course of the audit several IAOs identified that they had either not undertaken the IAO training course at all, or had not done so in several years. In addition, some IAOs were unclear about which or how many information assets they held responsibility for.

IAOs who have not received up to date training in their responsibilities, or who are unaware of the assets that they own the risks for, are potentially unable to control those risks effectively, which creates significant risks to data subjects through non-compliance with Article 5(1)(f) of the UK GDPR.

The Scottish Government should ensure that anyone moving into a role that requires them to act as an IAO receives the relevant specialist training as part of their induction to that role. This training should be subject to periodic refreshment for all IAOs, with the Scottish Government determining the interval between refresher training sessions with a view to the potential impact of failure to control risk to their information assets and data subjects.

7.6 Data Protection Impact Assessments

Overall the procedures surrounding DPIAs are well established and embedded across the organisation. However, it was identified in several directorates that some DPIAs may be undertaken and signed off without any input from the DPO or their designated representatives. In addition, it was identified that in some areas projects can get well underway before a DPIA is carried out. The reasons identified for failure to consult with the DPO and for the late completion of DPIAs included lack of awareness amongst relevant staff, and a low prioritisation of data protection in some areas of the organisation.

When the advice of the DPO is not sought for a DPIA, this is a breach of Article 35(2) of the UK GDPR, and risks that key points of data protection legislation may not be properly addressed within the DPIA, potentially leading to additional breaches of the legislation or a data breach. Similarly, when a DPIA is not undertaken before processing of personal data takes place, this is a breach of Article 35(1), and when a DPIA takes place too late in the process to implement risk controls or to shape the

processing sufficiently to minimise or mitigate risk to data subjects this is a breach of Articles 5(1)(f) and 35(7) (d) of the UK GDPR.

The Scottish Government should ensure that clear and effective processes are in place in all areas of the organisation to allow for effective consultation with the DPO during the DPIA process. These processes should be communicated to all relevant staff, and guidance should be made available to ensure that staff are fully equipped to comply with these processes. Further, the Scottish Government should communicate to relevant staff the necessity of complying with these processes, and the potential consequences for both the Scottish Government and their data subjects if a DPIA is not completed properly. The Scottish Government should also carry out a systematic review of all ongoing processing of personal data to ensure that there are fully compliant DPIAs in place in all instances.

Additionally there is no standardised approach across the Scottish Government for the review of DPIAs. In some areas it was reported that DPIAs do undergo periodic review, in others that DPIAs are considered "live" documents for the duration of projects and so undergo continual updates, but in other areas there was no consideration of reviews or updates leading to some DPIAs potentially becoming substantially out of date and ineffective at controlling risks. In addition, the DPO and IADP team do not have any mechanism or opportunity to follow up on their advice to project teams regarding DPIAs, in order to gain assurance that their recommendations have been implemented appropriately. As a result there is a risk of a breach to Article 35(11) of the UK GDPR, which requires that DPIAs should be reviewed when there is a change to the relevant risks, and Article 5(2) as the DPO and IADP team will not be able to demonstrate compliance with the requirements of Article 35(7).

The Scottish Government should standardise the approach to reviewing DPIAs, and put in place a baseline expectation, though individual business areas should be permitted to carry out more frequent reviews if they feel it is appropriate to the nature of the processing being undertaken. The Scottish Government should also implement processes to allow the DPO and IADP team to gain assurances that DPIAs are effectively controlling information risks across all areas of the Scottish Government.

7.7 3rd Parties and Data Processors

There is a standardised and comprehensive approach to managing relationships with data processors, including the use of standardised contracts which contain suitable language regarding data protection

compliance. However, despite the standard contracts allowing for the Scottish Government to carry out assurance activities in relation to data processors, no such activities have taken place and so the Scottish Government cannot be confident that their data processors are complying with data protection legislation. Were a processor to fail to comply with data protection legislation, this would place the Scottish Government at risk of a breach of Articles 5 (1) (f) and 28 of the UK GDPR.

The Scottish Government should put in place measures that will allow them to gain assurance that data processors are complying with their obligations under data protection law.

7.8 Law Enforcement Processing

The Scottish Government's documented position is that they undertake law enforcement processing (LEP) in a small number of areas. In the course of the audit a number of processing activities were identified which may fall under the heading of LEP, and some interviewees lacked confidence in whether or not they were carrying out LEP, meaning that the Scottish Government may have been carrying out LEP without complying with the requirements of DPA 2018 Part 3. As part of the broader data flow mapping exercise that has been recommended as a result of this audit, the Scottish Government should determine with confidence whether they are carrying out more LEP than they had previously documented.

7.9 Public Inquiries

Due to the different legal routes and circumstances that can result in new inquiries being formed, there is no standard approach to setting up new public inquiries in Scotland. As a result each inquiry is set up differently. The same data protection and information governance questions come up each time, but may be dealt with differently across different inquiries. This has resulted in a failure to learn from each inquiry and adopt best practice, or to identify necessary improvements for the next inquiry.

There is currently a broad piece of work underway, in its early stages, to put in place a more structured framework of support for new inquiries, including guidance, procedures, and standard structures. The Scottish Government should consider enhancing this piece of work with a package of data protection guidance, which could be provided to new inquiries immediately on the chair and secretary being appointed. This will ensure

that they have all the necessary information regarding their responsibilities as a data controller

For this guidance package, the Scottish Government should consider including job descriptions, roles and responsibilities for key data protection staff; templates of necessary documents such as DPIAs, RoPAs, and risk registers; procedural guidance on how to make use of these templates; guidance on the development of transparency information and how to handle information rights; and contact information for relevant experts within the Scottish Government and also within other bodies such as the National Cyber Security Centre, and the ICO's Scottish Regional Office. Having this guidance package in place with ensure that new inquiry chairs have all the necessary information to ensure they set up their inquiries to be fully compliant with data protection legislation. It must be acknowledged that where inquiry chairs are operating as independent data controllers, the Scottish Government does not have responsibility for ensuring that those inquiries comply with data protection legislation, and the provision of the guidance package recommended here would a voluntary effort on the part of the Scottish Government to assist independent inquiries in achieving compliance.

A key point of tension identified during this engagement is around what happens to the personal data held by inquiries after they publish their report and close down. As a result of the lack of a standardised approach to inquiries, the question of who is responsible for the data after an inquiry closes down has been resolved differently on numerous occasions, and no one interviewed could answer with any certainty how it would be resolved on any current or future inquiries, except that someone in the Scottish Government would have to take responsibility for the data.

The Scottish Government should do their best to ensure that this question is answered when an inquiry is set up, with a formal, signed Memorandum of Understanding (MoU) being put in place between the inquiry and themselves agreeing on how personal data will be handled at the close of the inquiry. This should include details of what data will be deleted, and for the data that will be retained there should be a decision of how long it will be retained for and who will have ownership of it as an information asset within the Scottish Government. Attention should also be given to any requirements or guidance from the National Records of Scotland in making these decisions. The Scottish Government should also advise inquiries to reflect the terms of the MoU in their transparency information.

If an inquiry chair is unwilling to set up such an MoU with the Scottish Government regarding the future disposition of personal data collected by the inquiry, then the Scottish Government should put in place

documented plans to the best of their ability. Those plans should account for the fact that the inquiry chair has not agreed any specific actions, and so should remain flexible to accommodate the independence of the inquiry.

In addition, following the conclusion of an inquiry, there is a need to ensure that data subjects can still effectively exercise their rights under Articles 15-21 of the UK GDPR. To be able to do this, data subjects must know where their data is being held, for how long it is being held, and who the correct point of contact is. It is also vital that that point of contact is aware of their responsibilities in this regard, and of the possibility of them being contacted by data subjects.

In order to facilitate this, the Scottish Government could put in place a web page to function as a single source of information about all completed inquiries. This page could list when the report was published; how long the report will remain available; what personal data has been retained; who is now responsible for that personal data; how to contact that person; and links to relevant transparency information for each inquiry.

8. Good Practice

- 51% of the control measures assessed across this audit were rated as having High Assurance, which shows that the auditors found them to be in place and effective at controlling the relevant risks, with no additional advice or recommendations required.
- Many staff working in data protection or information governance related roles across the Scottish Government demonstrated substantial enthusiasm their work.
- All staff are required to undertake annual DP training, and there is a well embedded and effective process in place to ensure that annual refresher training is undertaken on time.
- Significant improvements have been made to governance structures over the last couple of years, following an internal review carried out in 2020/21 and implementation of its recommendations.
- Major projects and programmes can have a data protection specialist from the IADP team embedded within their management team, in order to ensure access to specialist knowledge at all stages of the project lifecycle.

9. Conclusion

It was clear throughout the audit that significant efforts are underway within the Scottish Government to improve their data protection and information governance frameworks, for example with the embedding of specialist data protection resource within project teams. Some of these changes are in their very early stages, but if the Scottish Government is able to follow through on and complete their planned improvements then there will a substantial improvement in their level of compliance with data protection legislation. In addition, some areas of the Scottish Government have clearly invested over the last several years in improving their data protection compliance, with significant lessons that could be shared across the wider Scottish Government.

However, the audit has identified a number of areas where the Scottish Government is either currently in breach of data protection legislation, for example around the inability to demonstrate a compliant RoPA and the failure to always carry out necessary DPIAs prior to beginning the processing of personal data. It is vital that the Scottish Government take action as quickly as possible to control the risks identified within the Urgent and High recommendations provided in the individual exception reports.

10. Next Steps

In line with the ICO's policy on regulating the public sector, engagement with the Scottish Government will continue in order to monitor the implementation of measures to control the risks identified in the course of the audit.

11. Thanks

With thanks for their substantial efforts and work to help make this audit happen effectively:

Stuart Gardner, DPO

Helen Findlay, Head of IADP

The IADP team

Appendix

Priority Ratings

Priorities are assigned as Urgent, High, Medium, or Low, on the basis of the following definitions:

Urgent – An urgent recommendation relates either to a clear breach of data protection legislation, or to an imminent risk of a personal data breach occurring if the issue is not resolved.

High – A high recommendation relates to the serious likelihood of a breach of the legislation or a personal data breach occurring if the issue is not resolved.

Medium – A medium recommendation relates to the realistic possibility of a breach of the legislation or a personal data breach occurring if the issue is not resolved.

Low – A low recommendation relates to the potential for a breach of the legislation or a personal data breach to occur if the issue is not resolved.

The severity of any potential consequent personal data breach is also factored into consideration when assigning a priority rating, including both the sort of data that may be part of the breach and the number of data subjects who could be affected.

Assurance Ratings

Each thematic area was also given an overall assurance rating, based on the following definitions:

High – There is a high level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified only limited scope for improvement in existing arrangements and as such it is not anticipated that significant further action is required to reduce the risk of non-compliance with data protection legislation.

Reasonable – There is a reasonable level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified some scope for improvement in existing arrangements to reduce the risk of non-compliance with data protection legislation.

Limited – There is a limited level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified considerable scope for improvement in existing arrangements to reduce the risk of non-compliance with data protection legislation.

Very Limited - There is a very limited level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified a substantial risk that the objective of data protection compliance will not be achieved. Immediate action is required to improve the control environment.