Public Records (Scotland) Act 2011

Audit Scotland
Accounts Commission for Scotland
Auditor General for Scotland

The Keeper of the Records of Scotland

31st August 2022

Contents

1. Public Records (Scotland) Act 2011

The Public Records (Scotland) Act 2011 (the Act) received Royal assent on 20 April 2011. It is the first new public records legislation in Scotland since 1937 and came fully into force on 1 January 2013. Its primary aim is to promote efficient and accountable record keeping by named Scottish public authorities.

The Act has its origins in *The Historical Abuse Systemic Review: Residential Schools and Children's Homes in Scotland 1950-1995* (The Shaw Report) published in 2007. The Shaw Report recorded how its investigations were hampered by poor record keeping and found that thousands of records had been created, but were then lost due to an inadequate legislative framework and poor records management. Crucially, it demonstrated how former residents of children's homes were denied access to information about their formative years. The Shaw Report demonstrated that management of records in all formats (paper and electronic) is not just a bureaucratic process, but central to good governance and should not be ignored. A follow-up review of public records legislation by the Keeper of the Records of Scotland (the Keeper) found further evidence of poor records management across the public sector. This resulted in the passage of the Act by the Scottish Parliament in March 2011.

The Act requires a named authority to prepare and implement a records management plan (RMP) which must set out proper arrangements for the management of its records. A plan must clearly describe the way the authority cares for the records that it creates, in any format, whilst carrying out its business activities. The RMP must be agreed with the Keeper and regularly reviewed.

2. Executive Summary

This report sets out the findings of the Keeper's assessment of the RMP of Audit Scotland, the Accounts Commission for Scotland and the Auditor General for Scotland by the Public Records (Scotland) Act 2011 Assessment Team following its submission to the Keeper on 29th January 2021.

The assessment considered whether the RMP of Audit Scotland, the Accounts Commission for Scotland and the Auditor General for Scotland was developed with proper regard to the 15 elements of the Keeper's statutory Model Records Management Plan (the Model Plan) under section 8(3) of the Act, and whether in this respect it complies with it and the specific requirements of the Act.

The outcome of the assessment and the Keeper's decision on whether the RMP of Audit Scotland, the Accounts Commission for Scotland and the Auditor General for Scotland complies with the Act can be found under section 7 of this report with relevant recommendations.

3. Authority Background

The post of Auditor General for Scotland was created under the Scotland Act 1998 to help ensure that public money is spent properly, efficiently and effectively. The Auditor General is appointed by the Crown, on the recommendation of the Scottish Parliament. The Auditor General is also the accountable officer for Audit Scotland. He is committed to public services that improve the lives of Scotland's people. The current Auditor General has over 20 years' experience in audit, governance and financial management, and is a qualified accountant and a fellow of the Chartered Institute of Public Finance and Accountancy.

Auditor General | Audit Scotland (audit-scotland.gov.uk)

The Accounts Commission for Scotland is independent of councils and of the Scottish Government and is the public spending watchdog for local government. It holds councils and other local government bodies in Scotland to account and helps them improve

by reporting to the public on their performance. The Controller of Audit is an independent post established by statute, with powers to report directly to the Commission on the audit of local government.

Accounts Commission | Audit Scotland (audit-scotland.gov.uk)

Audit Scotland assists the Auditor General and the Accounts Commission to ensure organisations that spend public money in Scotland use it properly, efficiently and effectively. They give independent assurance to the people of Scotland that public money is spent properly, efficiently and effectively. They audit 223 public bodies and produce a range of local and national reports about the performance and financial management of Scotland's public bodies.

Audit Scotland | Audit Scotland (audit-scotland.gov.uk)

4. Keeper's Assessment Process

The RMP was assessed by the Public Records (Scotland) Act Assessment Team on behalf of the Keeper. Assessors used the checklist elements listed in section 5, to establish whether the RMP of Audit Scotland, the Accounts Commission for Scotland and the Auditor General for Scotland was developed with proper regard to the elements of the Model Plan and is compliant with the Act. The assessment also considered whether there was sufficient supporting evidence of such compliance.

Key:

G	The Keeper agrees this element of an authority's plan.		A	The Keeper agrees this element of an authority's plan as an 'improvement model'. This means that he is convinced of the authority's commitment to closing a gap in provision. He will request that he is updated as work on this element progresses.		R	There is a serious gap in provision for this element with no clear explanation of how this will be addressed. The Keeper may choose to return the RMP on this basis.

5. Model Plan Elements: Checklist

Audit Scotland, Auditor General for Scotland and Accounts Commission for Scotland

N. B. For simplicity, as the plan relates to the records management provision for all three public authorities, the use of 'Audit Scotland' in the assessment below should be taken to refer to that organisation as well as to the Auditor General for Scotland and the Accounts Commission for Scotland.

Element	Present	Evidence	Notes
1. Senior Officer	G	G	Audit Scotland, Auditor General for Scotland and Accounts Commission for Scotland (referred to below as 'Audit Scotland') have identified Diane McGiffen, Chief Operating Officer, as the individual with overall responsibility for records management in the authority. This identification is supported by a *Covering Letter* from Ms McGiffen dated 28th January 2021 and submitted to the Keeper of the Records of Scotland (the Keeper) with the *Records Management Plan* (the *RMP*). Since submission there has been a change of personnel against this element: From August 2022, Vicki Bibby will take on the of Chief Operating Officer. Audit Scotland has committed that a letter to the Keeper of the Records of Scotland will be issued to formally inform him of the appointment. This commitment is welcomed.

			The Keeper has previously indicated that a change in post-holder does not invalidate a records management plan, as long as the post itself does not substantially change. For the purposes of this agreement, the Keeper accepts the role of the Chief Operating Officer, as regards records management, will be the same under Ms Bibby as it was under Ms McGiffen. The identification of the Chief Operating Officer as the individual with overall responsibility for records management in the organisation is also supported in the *Audit Scotland Records Management Policy* (see element 3) section 7. The Chief Operating Officer is also the Senior Information Risk Owner (SIRO) in Audit Scotland. This is confirmed by the *Audit Scotland Information Security Management Policy* section 7 (see element 8). The Chief Operating Officer/SIRO sits on the Knowledge, Information and Technology Governance Group (KITGG) (see under General Comments). In turn, the KITGG supports the SIRO by, among other things, assessing and mitigating information security risks. The Chief Operating Officer is also part of the Incident Management Team responsible for the recovery of records in an emergency (see element 10). The Keeper agrees that Audit Scotland have identified an appropriate individual to this role as required by the Public Records (Scotland) Act 2011 (the Act).
2. Records Manager	**G**	**G**	The Act requires that each authority identifies an individual staff member as holding operational responsibility for records management and has appropriate corporate responsibility, access to resources, and skills. Audit Scotland have identified Gayle Fitzpatrick, Corporate Governance Manager,

			as the individual with the day-to-day responsibility for implementing the *RMP*. This identification is supported by a *Covering Letter* from the Chief Operating Officer (see element 1) dated 28th January 2021 which was submitted to the Keeper in support of the *RMP*. The identification of the Corporate Governance Manager as the individual with overall responsibility for day-to-day records management arrangements for all three authorities is also supported in the *Records Management Policy* section 8. The *Records Management Policy* (see element 3) is 'owned and maintained' by the Corporate Governance Manager. The Keeper has been provided with Audit Scotland's *Corporate Governance Manager Job Description* which specifically notes responsibility for "Managing our legislative obligations and reporting requirements under… the Public Records (Scotland) Act 2011…" The Corporate Governance Manager is the Data Protection Officer for Audit Scotland (see element 9). She is the corporate owner of the authority's *Data Protection Policy*. The Corporate Governance Manager sits on the Knowledge, Information and Technology Governance Group (see under General Comments). The *Information Management Guidance* issued to staff (see element 3) explains that the Corporate Governance Manager will advise on all aspects of records management including around security for example, the three security classifications applied to its public records (see element 8).

			The Corporate Governance Manager undertook a four-day course 'Practitioner Certificate in Scottish Public Sector Records Management' during 2020. The Keeper has been provided with evidence of this training. The Keeper agrees that Audit Scotland have identified an appropriate individual to this role as required by the Act.
3. Policy	**G**	**G**	The Act requires an authority to have an appropriate policy statement on records management. Audit Scotland have a *Records Management Policy* which is publically available at: Records Management Policy (audit-scotland.gov.uk) This is version 08. The Keeper has been provided with documentation showing the Audit Scotland Board approves the *Records Management Policy*. The *Policy* specifically states that it applies to all three authorities covered by the *RMP* (*Policy* section 5). Audit Scotland have also developed *Records Management A guide for staff on managing records* (2017) *and Information Management Guidance* (version 2.1 November 2021). Both of these documents have been provided to the Keeper in evidence. The 2017 document refers throughout to the ishare system that was, at the time of issue, operational in Audit Scotland (see element 4). However, many of the general principles explained in this guidance are still valid and the Keeper welcomes its submission. Audit Scotland have informed the Keeper separately that *Records Management A guide for staff on managing records* (2017) is currently being updated and they will provide a copy once approved.

			Audit Scotland operate an annual *Records Management Compliance Self-Assessment Checklist* which has been supplied to the Keeper (see element 13). This includes a requirement that business areas confirm that "Staff in your business group are aware of Audit Scotland's records management policy and arrangements and their responsibilities under it." (*Checklist* 1.1) The *Records Management Policy* recognises the Public Records (Scotland) Act and the Keeper's Model Plan (*Policy* section 17). The Keeper agrees that Audit Scotland have a 'records management policy statement' as required by the Act.
4. Business Classification	**G**	**G**	The Keeper of the Records of Scotland (the Keeper) expects that the public records of an authority are known and are identified within a structure. At the time of their original submission Audit Scotland arranged their records by business groups. However, they indicated that their Business Classification Scheme was to be rearranged into a 'functional' system. This has now been done. This arrangement has been shared with the Keeper in the form of a PowerPoint presentation. The arrangement must remain a business decision for Audit Scotland, but the Keeper acknowledges that the current thinking in the field would support this change. The advantages of a functional system are identified in the *RMP*: 'to avoid having to restructure the information should business groups change' (*RMP* page 7). Audit Scotland have an *Information Asset Register* (*IAR*) which has been shared in full with the Keeper. It includes retention decisions against record types (see element 5). The *IAR* also shows security classification, whether the record is 'vital'

			(see element 10) and location. This latter field confirms that the corporate records of Audit Scotland exist in both digital and hard-copy format. Prior to 2013 Audit Scotland's public records were held mostly on paper. After 2013 the records were managed in a hybrid of paper and digital systems. However, they are now principally a digital record organisation with legacy paper records managed in greater part through a third-party long-term storage solution. In the case that legacy paper records survive for a particular record type the *IAR* is marked as 'archive'. A limited amount of hard-copy public records are held on site by Audit Scotland. These are records that have current business use and are listed in the *IAR* as being held in 'cabinets'. It is commendable that the *IAR* features all records in all formats. Audit Scotland use Microsoft SharePoint technology as their digital solution. In 2013 This system was referred to internally as 'iShare'. Some of the evidence documents submitted along with the current version of their *RMP* still refer to iShare (for example the *Records Management A guide for staff on managing records* document - see element 3). The Keeper accepts this. Audit Scotland have recognised that migration of records between systems represents a risk. Their *Records Management Policy* notes at section 12.8: "Where records are migrated across changes in technology, the evidence preserved must remain authentic and accurate." The Keeper commends this recognition. However, he is confident that migration from the authority's iShare (structured on SharePoint) to SharePoint Online can be managed without serious harm to the metadata of the record. In January 2020 Audit Scotland finalised the move from iShare to SharePoint Online. This represented a transfer of all organisational records from one system to another. However, at time of submission the authority had not fully adopted the

			M365 records management functionality and are still controlling this locally. The *RMP* (page 9) states: “In March 2020, all Audit Scotland colleagues began working remotely from home due to the Covid-19 pandemic. The significant change in working style also contributed to the decision to delay the enabling of the SharePoint Online records management functionality. Microsoft has recently made some amendments to its Compliance Tool within SharePoint Online. This change has also contributed to the decision to delay enabling the SharePoint records management functionality. Audit Scotland is cautious about turning the functionality on too soon without determining how this will impact on records management.” The Keeper acknowledges that he is being kept up-to-date with progress. For example he has been advised, separately from this submission, that Audit Scotland have appointed a new member of staff (May 2022) who will take forward the implementation of records management in SharePoint and that they are currently exploring options with an external organisation to assist in taking this forward. Audit Scotland go on to state (*RMP* pages 8/9). That they undertake regular file audits of business group SharePoint sites. These file audits provide the Corporate Governance Manager (see element 2) with the ability to review the progress of SharePoint implementation in terms of organisational records management and identify areas for improvement. The Keeper has been provided with a sample of an audit report in evidence. The Keeper has been provided with a screen-shot of the ‘front page’ showing how the records management system appears to staff. Audit Scotland operate an annual *Records Management Compliance Self-Assessment Checklist* which has been supplied to the Keeper (see element 13). This includes a requirement that business areas confirm that " Your business group ensures that electronic information (including e-mails) is held where it is accessible

			to all relevant staff." (*Checklist* 1.4) and "Your business group knows where its records are at all times." (2.3) The Keeper agrees that Audit Scotland retains all its public records in controlled systems which are structured in a clear manner and which can be used by staff to manage public records where appropriate.
5. Retention schedule	**G**	**G**	The Keeper expects an authority to have allocated retention periods to its public records and for those records to be retained and disposed of in accordance with a Retention Schedule. The *Guide for Staff on Managing Records* (see element 3) has a section on the purpose of applying retention decisions to records. The principles are still valid even if references to the iShare system are out-off-date (see element 4 for more on this). Audit Scotland state: "Our Information retention schedule states how long particular types of information should be kept. It is based on legislative requirements, good practice guidance and business needs." (*Archiving Procedure: Guidance for All Staff* section 6). With these principles in mind, the authority has an *Information Asset Register* (*IAR*) which includes retention decisions. This has been provided to the Keeper (see element 4). The *IAR* includes records held digitally, with a third-party storage contactor and physically in-house in cabinets. All formats have retention decisions noted. The Keeper is confident that all record types created and held by Audit Scotland have appropriate retention decisions allocated to them as required. "Business groups across Audit Scotland are responsible for the appropriate retention and disposal of files within their SharePoint sites, including the labelling of files to accurately determine ownership, sensitivity, file type and the current status of the document."

			(*Records Management Policy* - see element 3 - section 14). The Corporate Governance Manager (see element 2) monitors this using regular file audits of business group SharePoint sites (see element 4). The *Information Management Guidance* issued to staff explains the disposal of records against their retention (*Guidance* section 12). The Keeper agrees that Audit Scotland has provided retention decisions for the record types created while pursuing its functions.
6. Destruction Arrangements	**G**	**G**	The Act requires that public records are destroyed in a timely, controlled and secure manner. Audit Scotland acknowledge this. Staff guidance includes a section on 'Disposing of information securely' (*Information Management Guidance* - see element 3 - sections 17 and 18) With this in mind Audit Scotland have the following process in place, to ensure the controlled, secure and irretrievable destruction of public records (For the structure of the records management systems see element 4 above). Digital SharePoint: The majority of the public records of Audit Scotland are managed on the SharePoint system. As such they are subject to the destruction processes of that system. The *RMP* states (page 10) “In July 2013 we started to implement electronic records management through SharePoint technology. Arrangements are in place for managing records, declared in SharePoint, through the life of the record.” Information Asset Owners, supported by the Knowledge, Information and Technology Governance Group (see under General Comments below) are responsible for ensuring relevant destruction takes place when prompted by the Audit Scotland retention schedule (see element 5).

			Physical third party storage: Destruction of the public records held by the third party long-term storage provider is part of the agreement between Audit Scotland and the provider. Staff are provided with guidance on how to transfer hard-copy records to the contractor (*Archiving Procedure: Guidance for All Staff* sections 8 onwards). At the end of the retention period the storage contractor contacts the local Information Asset Owner (IAO). The IAO then selects either to destroy the record or to have it transferred to permanent archive with NRS (see element 7). Evidence of the how destruction operates and the standard of destruction contracted for have been provided to the Keeper in the form of destruction certificates issued by the contractor. Physical in-house: A limited amount of hard-copy public records are held on site by Audit Scotland. These records are in current business use. These are either transferred to the third-party storage contractor (see above) or destroyed by a third-party shredding company. Guidance around arranging the destruction of in-house hard-copy records is provided in the *Information Management Guidance* document (see element 3). Certificates of destruction from this company have been provided as evidence that this arrangement is operational. Hardware: Audit Scotland staff return any device or media, that is no longer in use, to Digital Services for secure disposal. The Keeper has been provided with the Audit Scotland *IT Disposal Policy* (version 2.8 October 2021) Back-Ups: The majority of the Audit Scotland public records are covered by the back-up feature of the SharePoint online system. The *RMP* (page 12) notes that "Servers are backed up with copies stored in our disaster recovery servers". The Keeper can agree that appropriate continuity back-ups are operational to aid record recovery in an emergency. Audit Scotland have explained that: "Once documents are deleted from SPO they are retained for 93 days where we can recover them.

			Microsoft retain for an additional 14 days, but we would need to raise a support call to recover these. Files that are stored in other locations such as MKI and other SQL databases we can recover for up to a year from backup." Audit Scotland operate an annual *Records Management Compliance Self-Assessment Checklist* which has been supplied to the Keeper (see element 13). This includes a requirement that business areas confirm that " Mechanisms and procedures are in place to ensure that unwanted information can be deleted from shared drives and databases." (*Checklist* 2.8), "Your business group keeps a record of what records have been destroyed, when and why." (3.3) and "Before computers are disposed of, their drives are wiped or destroyed as appropriate." (3.6) Audit Scotland operate an annual *Records Management Compliance Self-Assessment Checklist* which has been supplied to the Keeper (see element 13). This includes a requirement that business areas confirm that " Mechanisms and procedures are in place to ensure that unwanted information can be deleted from shared drives and databases." (*Checklist* 2.8), "Your business group keeps a record of what records have been destroyed, when and why." (3.3) and "Before computers are disposed of, their drives are wiped or destroyed as appropriate." (3.6) The Keeper agrees that Audit Scotland has processes in place to irretrievably destroy their records when appropriate.
7. Archiving and Transfer	**A**	**G**	The Act requires that all Scottish public authorities identify a suitable repository for the permanent preservation of any records considered suitable for archiving. A formal arrangement for transfer to that repository must be in place. Audit Scotland recognise this and state: "Archiving is part of our Information Management process and we are all expected to help ensure that our valuable information assets are properly managed and protected throughout their lifecycle."

			(*Archiving Procedure: Guidance for All Staff* section 2). There is some confusion around this element. The Keeper is satisfied that this is due to terminology rather than provision. Audit Scotland use the term 'archive' to signify the long-term storage of paper records when they are no longer being used for immediate business purposes. The first paragraph of the compliance statement against this element (*RMP* page 12) reads "The Auditor General for Scotland, Accounts Commission and Audit Scotland archive their paper records with Haven Products. Haven Products is ISO registered for their document storage, collection, retrieval and confidential shredding." (The use of third party storage contractors is mentioned under elements 4 and 6 above). This is not what the Public Records (Scotland) Act 2011 means when it refers to archiving. The Keeper explains in his Model Plan Model Records Management Plan | National Records of Scotland (nrscotland.gov.uk) That archiving and transfer signifies that "Records that have enduring value are permanently retained and made accessible in accordance with the Keeper's 'Supplementary Guidance on Proper Arrangements for Archiving Public Documents'." Audit Scotland's long-term storage contractor is not a suitable repository for the permanent preservation of public records. Not least because they will store records only as long as they are paid by a client to do so. Under 'archiving' the Act considers the, very limited, selection of public records that will be retained for historical research purpose in perpetuity, potentially long after the creator authority has ceased to exist. That said, the Keeper is aware that Audit Scotland has, in fact, identified a suitable repository for this work, the National Records of Scotland, and has previously transferred records to that repository. The catalogue notes records dating back to 1974 are held by NRS. The archiving arrangement with NRS is recognised in paragraph 4 of the compliance statement against this element.

			Furthermore, staff guidance in the form of Audit Scotland's *Transferring records to the National Records of Scotland* document has been shared with the Keeper as part of this submission. The *Archiving Procedure: Guidance for All Staff* document is, in contrast, principally about the procedure to send hard-copy records to remote storage from where they will be disposed of either by destruction or transfer to NRS. The Keeper agrees, therefore, that the use of an external storage contractor, currently Haven Products, may in some cases be a step in the eventual 'archiving' process. Audit Scotland have made contact with NRS Client Manager to start the process of agreeing a formal Memorandum of Understanding. The Keeper has been provided with an Email between the authority and the NRS confirming this is underway. **The Keeper agrees this element of Audit Scotland's plan under improvement model terms. This means a that he is satisfied that the authority has identified a suitable repository for the permanent preservation of records when appropriate, but has yet to finalise a formal agreement with that repository. As noted above, the Keeper acknowledges that archival transfers have taken place in the past.**
8. Information Security	**G**	**G**	The Act requires that public records are held in accordance with information security compliance requirements. Audit Scotland recognise this and the *Records Management Policy* (see element 3) states: "Records must be securely maintained to prevent unauthorised access, alteration, damage or removal. They must be stored in a secure environment, the degree of security reflecting the sensitivity and importance of the contents." (*Policy* section 12.8). This is repeated in the staff guidance document *Records*

			Management A guide for staff on managing records (also see element 3). To support these aspirations, Audit Scotland have an *Information Security Management Policy* which has been provided to the Keeper. This is version 1.8 dated May 2022. The Keeper has been provided with documentation showing the Audit Scotland Board approves the *Information Security Policy*. The *Information Security Management Policy* commits Audit Scotland to “Treat information security as business critical, whether that be for Audit Scotland information or client data managed by Audit Scotland.” (*Policy* section 4.1.) The *Policy* goes on to require Audit Scotland to "Develop, implement and maintain an Information Security Management System" (*Policy* section 4.11). The structure of the Security Management System is laid out in a hierarchical chart in an appendix to the *Policy*. This chart shows that the *Information Security Management Policy* is supported by a suite of other information security policies and guidance such as their *Clear Desk & Screen Policy*, *Information Acceptable Use Policy* and *Remote Working Policy*. Together with the *Policy*, these supporting documents form the Audit Scotland ‘Information Security Management System’. “Audit Scotland’s Information Security Management system (ISMS) was established in 2016 and re-certification to the standard is subject to 6 monthly audits by a certification body. The last certification was in October 2020 with no areas for improvement and accreditation renewed.” (*RMP* page 13). The Keeper has been provided with a certificate showing compliance with ISO27001 issued by Certification Europe (UK) Ltd. in evidence. The Keeper acknowledges that he has been provided with a suite of information security policies that support the objectives noted above:

			Information Acceptable Use Policy v4.1 April 2022 Backup, replication and retention policy v2.7 January 2022 Clear Work Areas and Screen Policy v1.8 March 2022 Digital Access Control Policy v4.8 January 2022 Physical Security Policy v2.7 March 2022 Remote Working Policy v1.9 April 2022 Supplier Information Security Policy v3.0 June 2022 Working with Personal Devices Policy v1.7 March 2022 A monthly cyber security update is scheduled with the SIRO (see element 1) and a member of the Digital Services Management Team to ensure the latest updates are provided to Senior Management. The *Records Management Policy* (see element 3) commits Audit Scotland to training "to ensure that all staff are aware of their information obligations regarding Data Protection, Data Security and Freedom of Information." (*Records Management Policy* section 16) The *Information Management Guidance* (see element 3) includes considerable supporting guidance on information security including details of the three security classifications applied to its public records. (Guidance section 4). The Audit Scotland staff *Code of Conduct*, which has been supplied to the Keeper, features a section on information security (section 21). Audit Scotland operate an annual *Records Management Compliance Self-Assessment Checklist* which has been supplied to the Keeper (see element 13). This includes a requirement that business areas confirm that "There are procedures in place to restrict access to confidential information." (*Checklist* 1.9)

			The Keeper agrees that Audit Scotland have procedures in place to appropriately ensure the security of their records as required by the Act.
9. Data Protection	**G**	**G**	The Keeper expects a Scottish public authority to manage records involving personal data in compliance with data protection law. Audit Scotland "recognise the seriousness of failing to comply with data protection legislation and the resulting risk to our reputation." (*Data Protection Policy* – see below - section 9) The Audit Scotland *Information Security Management Policy* (see element 8) requires the authority to "Ensure compliance with all relevant data protection regulations and implement privacy by design in all information systems" (*Information Security Policy* section 4.5) Audit Scotland is registered as a data controller with the Information Commissioner's Office (ICO): Information Commissioners - Data protection register - entry details (ico.org.uk) Audit Scotland have appointed a Data Protection Officer. This is the Corporate Governance Manager (see element 2). The Corporate Governance Manager's *Job Description*, which has been provided to the Keeper, confirms this appointment: "Undertaking the statutory role of Data Protection Officer for Audit Scotland, the Accounts Commission and the Auditor General for Scotland". This identification is also confirmed in the *Information Security Management Policy* (see element 8) (section 15) and by the *Data Protection Policy* (section 18). As noted above, Audit Scotland have a *Data Protection Policy*. The current version is 18 (April 2022) which is available online at Data protection policy (audit-scotland.gov.uk). This *Policy* states specifically that it applies to all three authorities

			(*DP Policy* section 6). The Keeper has been provided with documentation showing the Audit Scotland Board approves the *Data Protection Policy*. The *Policy* properly explains the principles of data protection. The *Data Protection Policy* commits Audit Scotland to undertake data protection impact assessments when appropriate (for example *DP Policy* section 9.5). The *Records Management Policy* (see element 3) commits Audit Scotland to training "to ensure that all staff are aware of their information obligations regarding Data Protection, Data Security and Freedom of Information." (*Records Management Policy* section 16) The Audit Scotland staff *Code of Conduct*, which has been supplied to the Keeper, features a section on data protection (section 20). The *Records Management Policy* recognises the Data Protection Act 2018 and General Data Protection Regulation (GDPR) (*Policy* section 17). The Keeper agrees that Audit Scotland have arrangements in place that allow them to properly comply with data protection legislation.
10. Business Continuity and Vital Records	**G**	**G**	The Keeper expects that record recovery, prioritising vital records, is an integral part of the authority's business continuity planning. Audit Scotland have procedures in place to address 'any event which seriously affects business operations, to the detriment of the services that Audit Scotland delivers to its clients' (*Business Continuity Policy* – see below – section 4) The Audit Scotland *Information Security Management Policy* (see element 8) requires the authority to "Produce, maintain and test business continuity plans to

			ensure the availability of its information and information systems" (*Information Security Policy* section 4.2.) To this end, Audit Scotland have a general *Business Continuity Policy* which has been provided to the Keeper. This is version 16 dated April 2022. This *Policy* states specifically that it applies to all three authorities (*Business Continuity Policy* cover sheet).The *Policy* is supported by *Incident Recovery Plans* (IRP). An explanatory document of how IRPs are implemented has also been supplied. The Keeper has been provided with documentation showing the Audit Scotland Board approve the *Business Continuity Policy.* The Keeper agrees that both evidential documents show consideration of the recovery of records in an emergency. For example under 'infrastructure' in the *Policy* and under Digital Services Desk (Plan B) or Electronic Working Papers (Plan L) in the *IRP* Staff are provided with guidance on how the *Policy* and *Plans* operate in a *Introduction to Business Continuity Management in Audit Scotland* document which has also been shared with the Keeper. The *RMP* (page 12) notes that "Servers are backed up with copies stored in our disaster recovery servers". In section 46 of the *Guide for Staff on Managing Records* (see element 3) there is an explanation of this back-up processes. Audit Scotland have provided a separate update on changes in this area since their reviewed RMP was submitted in 2021: "We have a live replica of these systems in our disaster recovery site that is at most 5 minutes behind production. We no longer backup to tape but use a disk-based backup, we are going to be updating this system soon with the additional option to take a backup and store it in cloud storage on Azure."

			Audit Scotland have identified 'vital records' as "…those categories of record which are required by us to carry out our essential core functions in a legally compliant manner" and give examples of what these might be. The authority goes on to establish this principle: "Management of our vital records are an essential part of our Disaster Recovery arrangements and must be kept up to date." (*A Guide for Staff on Managing Records* – see element 3 - sections 44 - 49). The Corporate Governance Manager's (see element 2) *Job Description*, which has been provided to the Keeper, includes the responsibility of "Managing, reviewing and testing our business continuity arrangements to help mitigate business disruptions. Providing specialist knowledge and advice to colleagues on business continuity management." The Keeper agrees that Audit Scotland have an approved and operational business continuity process and that information management and records recovery properly feature in the authority's plans.
11. Audit trail	**A**	**G**	The Keeper expects an authority to have processes in place to track public records in such a way that their location is known and changes recorded. The *Records Management Policy* (see element 3) commits Audit Scotland to ensure that changes and additions to records must be identifiable through audit trails (*Policy* section 12.1). and that "Records must be readily available when needed." (12.3). This is supported in the G*uide for Staff on Managing Records* (section 26). Audit Scotland has now finalised the move from iShare to SharePoint Online (see element 4 above). The new system provides a log of changes and amendments to files which provides a clear audit trail. SharePoint online also offers a powerful search facility for the identification and

			retrieval of records. **However, in order to fully utilise this the authority must be confident that records are named correctly. At the time of Audit Scotland's original submission to the Keeper (2013) the authority had developed an *Information File Naming Convention* which was originally created in 2007 and updated in December 2009. However, currently Audit Scotland state that: "Audit Scotland does not currently have a file naming convention. In guidance to staff we state Filename - this should enable viewers to guess what is in the file without taking time to open and skim the file. Useful information includes a date and description and may include author. We also have an instruction video resource library for colleagues [The Keeper has been provided with a screen-shot of the training module].** **Considering the issue of the consistent naming of public records, Audit Scotland have made the following commitment: "We are currently reviewing our guide for staff on managing records and once updated will provide a copy." The Keeper reminds Audit Scotland that the e-discovery functionality in SharePoint should allow a search at a document level meaning that the record can be located even if 'misfiled'. To fully utilise this functionality the new staff guidance should specifically instruct staff how to name the record not just the container as is done (in the general terms quoted above) currently.** Hard-Copy legacy records can be recalled utilising an 'archive recall process' utilising a catalogue. This has been explained in the *RMP* (page 12). An audit trail of any recall is kept by the 'document storage contractor' company. Audit Scotland operate an annual records management self-assessment checklist for local business areas (see element 13). Two of the 'indicators' that must be addressed by each area are: "Your business group knows how it intends to ensure that its electronic records will remain retrievable, interpretable and accessible for the

			whole of the time for which they are needed" (indicator 1.11) and "Sufficient metadata is captured for electronic records to ensure that the record remains retrievable, interpretable, authentic and accessible over time" (2.9). **The Keeper can agree this element of Audit Scotland's *Records Management Plan* on improvement model terms. This means that he is confident that the authority have understood and properly considered the importance of tracking and identifying their public records. However, he would expect Audit Scotland to issue naming convention instructions to staff to fully utilise the record search facility of their new system (the system will automatically apply version control).**
12. Competency Framework for records management staff	**G**	**G**	The Keeper expects staff creating, or otherwise processing records, to be appropriately trained and supported. There is a commitment in the *RMP* that all staff are aware of our records management practices and are appropriately trained (*RMP* page 21). The Corporate Governance Manager (see element 2) attends national best practice forums. As noted under element 2 above, she also undertook the Practitioner Certificate in Scottish Public Sector Records Management during 2020. The Keeper recognises that this is indicative of the authority allocating resources to appropriate information governance training for its staff. Audit Scotland staff receive 'introduction to records management' training and are staff are provided with guidance on SharePoint. In some cases, for example business continuity, updates can be provided both on SharePoint and through in-house Yammer channels. As evidence of available guidance the Keeper has been provided with two documents: *Records Management A guide for staff on managing records* (2017) *and Information Management Guidance* (2020) (see element 3 for

			more on these). The authority's *Records Management Policy* is available online. The *Data Protection Policy* commits Audit Scotland to ensure mandatory training for all staff (for example *DP Policy* sections 9.6 and 20). Staff training in records management is fully supported by sections 15 and 16 of the Audit Scotland *Records Management Policy* (see element 3). For example a commitment to training "to ensure that all staff are aware of their information obligations regarding Data Protection, Data Security and Freedom of Information." (*Records Management Policy* section 16) In addition to the 'all staff' training the Senior Information Risk Owner (see element 1) and local Information Asset Owners undertake enhanced 'Protecting Information' training. The Audit Scotland *Information Security Management Policy* (see element 8) requires the authority to "Communicate all appropriate information security policies to all employees, contractors, consultants, clients and other stakeholders" (*Information Security Policy* section 4.7) Staff are informed of business continuity arrangements (see element 10) at induction and during and annual Business Continuity Awareness Week. The Keeper has been provided with sight of this business continuity training. Having been provided with training and guidance all staff must complete a 'Fit and Proper' self-assessment form annually. This provides a way for the authority to ensure all staff have been fully briefed on the latest policies and potentially to identify gaps in training. The Keeper has been provided with a copy of this form

			(blank) and acknowledges that it includes sections on information security, data protection and records management. Furthermore, all staff in Audit Scotland are also provided with a *Staff Handbook*. The *RMP* (page 6) states that this *Handbook* includes a records management section including the authority's *Records Management Policy* (see element 3). The Staff Handbook is held on SharePoint and contains 100 documents. A screen-shot has been provided that shows the Records Management Policy section. The Keeper agrees that the individual identified at element 2 has the appropriate responsibilities, resources and skills to implement the records management plan. Furthermore, he also agrees that Audit Scotland consider information governance training for staff as required.
13. Assessment and Review	**G**	**G**	Section 1(5)(i)(a) of the Act says that an authority must keep its RMP under review. This is acknowledged by the IJB (*RMP* page 7). The *RMP* is reviewed annually (*RMP* page 21). Reviewing the implementation of the *RMP* is the responsibility of the Information Governance Manager (see element 2) supported by the Knowledge, Information and Technology Governance Group (KITGG) (see under general comments below). Their *Terms of Reference* explain that the KITGG have the responsibility of "ensuring information and records management governance policies are reviewed at least annually and submitted to Management Team/Board to approve any changes." (ToR section 6) To inform the review, Audit Scotland self-evaluate using a bespoke *Records Management Annual Assurance Checklist* which was introduced in 2014 and which must be completed by local business areas The Keeper acknowledges that he has

			been provided with a copy of the *Checklist*. As well as allowing the Information Governance Manager and KITGG to monitor the progress of *RMP* implementation, the Checklist "will enable IAOs [Information Asset Owners] to assess the adequacy of their business groups' records management systems and procedures and provides recommendations for action to address any gaps." (*Checklist* Introduction). The results of any review are reported to the Management Team/Board for approval of any changes. The SIRO (see element 1) sits on the Management Team. As well as the assurance of an overall *RMP* review, most individual elements have an annual review commitment. The Keeper has received a copy of a board paper *Annual Review of Corporate Governance Policies* written by the Corporate Governance Manager (see element 2). This paper explains the process for regular review of all corporate policies including those relating to records management. The *Records Management Policy* (see element 3) is due to be reviewed by September 2022 The *Digital Disposal Policy* (see element 6) is due to be reviewed by October 2022 The *Information Management Guidance* (see element 3) is due to be reviewed by November 2022 The *Backup, Replication and Retention Policy* and the *Digital Access Control Policy* (see element 8) are due for review by December 2022 The *Archiving Procedure: guidance for all staff* document (see element 7) is due for review by February 2023 The *Clear Work Areas and Screen Policy*, the *Working with Personal Devices Policy*

			and the *Physical Security Policy* (see element 8) are due for review in March 2023 The *Acceptable Use Policy* and the *Remote Working Policy* (see element 8) are due for review by April 2023 The *Information Security Management Policy* (see element 8) is due for review by May 2023 The *Supplier Information Security Policy* (see element 8) is due for review by June 2023 The *Data Subject Access Request Procedure* (see element 9) is due for review by April 2024 The *Audit Scotland Data Protection Policy* (see element 9) is due to be reviewed in April 2023 and the ICO registration in September 2022. Furthermore, the *Data Protection Policy* commits Audit Scotland to "conducting regular testing and reviews of our measures to ensure they remain effective, and act on the results of those tests where they highlight areas for improvement" (*DP Policy* section 9.10). Audit Scotland has recently reviewed its business continuity procedures (see element 10). The RMP explains (page 17): "An internal audit was conducted on our arrangements in June 2020. The Business Continuity Plan has been thoroughly tested, given the review took place during the height of the Covid-19 pandemic. The Internal Auditors reported an audit opinion of substantial assurance for both design and operational effectiveness and there were no recommendations for improvement." The Keeper agrees that Audit Scotland have made a firm commitment to review their *RMP* as required by the Act and have explained who will carry out this review

			and by what methodology. Furthermore, he agrees that supporting policy and guidance documents have appropriate reviews allocated.
14. Shared Information	**G**	**G**	The Keeper expects a Scottish public authority to ensure that information sharing, both within the Authority and with other bodies or individuals, is necessary, lawful and controlled. Audit Scotland make the following statement in their *RMP* (page 22): "The Auditor General for Scotland, Accounts Commission and Audit Scotland are empowered under the Public Finance and Accountability (Scotland) Act 2000 and the Local Government (Scotland) Act 1973 to conduct financial, economy, efficiency and effectiveness examinations on Scottish public bodies. This legislation requires Scottish public bodies to provide us with any information or records to allow us to undertake our work." Audit Scotland provide staff with the following Guidance statement around sharing information: "When you are planning to work with other scrutiny bodies, you must ensure that provision is made in any protocol, agreement, code of practice, memorandum of understanding, etc. of the arrangements for managing the records generated from this joint work. The arrangements should include the ownership of the records, storage, access, destruction and secure sharing of the records especially where the records contain personal information." (*Records Management A guide for staff on managing records* section 52) This seems clear and commendable guidance. The Keeper has been provided with a sample of such an agreement. The Keeper agrees that it contains all that the guidance indicates should be included. The 2020 *Information Management Guidance* (see element 3) also explains the benefits and risks of information sharing (Guidance section 12).

			Audit Scotland operate an annual *Records Management Compliance Self-Assessment Checklist* which has been supplied to the Keeper (see element 13). This includes a requirement that business areas confirm that "If your business group work in partnership with other bodies, the responsibility for and ownership of the records of that partnership is clearly defined." (*Checklist* 1.10) The Keeper agrees that Audit Scotland properly considers records governance when undertaking information sharing programmes.
15. Public records created or held by third parties	**N/A**	**N/A**	**Third Parties:** The Public Records (Scotland) Act 2011 (PRSA) makes it clear that records created by third parties when carrying out the functions of a scheduled authority should be considered 'public records' - PRSA Part 1 3 (1)(b). In the *RMP* (page 23) Audit Scotland have explained their contracting in of services from third-parties, but are quite clear that these third-parties are not carrying out a function of Audit Scotland. The Keeper agrees that Element 15 does not apply to Audit Scotland.

Audit Scotland, Auditor General for Scotland and Accounts Commission for Scotland

N. B. For simplicity, as the plan relates to the records management provision for all three public authorities, the use of 'Audit Scotland' in the assessment below should be taken to refer to that organisation as well as to the Auditor General for Scotland and the Accounts Commission for Scotland.

General Notes on submission:

This assessment is on the *Records Management Plan (2021–26)* (the *RMP*) of the Auditor General for Scotland, Accounts Commission and Audit Scotland (Audit Scotland) as submitted to the Keeper of the Records of Scotland (the Keeper), for his review and agreement, on 27th January 2021. The text of the *RMP* confirms that it applies to all three public authorities.

The *RMP* is publically available at Records Management Plan (audit-scotland.gov.uk)

This is the second formal records management plan received from Audit Scotland by the Keeper. The first was agreed on the 28th November 2013: Draft Keeper's Report (nrscotland.gov.uk)

The *RMP* is supported by a *Covering Letter* of endorsement from the Chief Operational Officer of Audit Scotland (see element 1) and by details of the Audit Scotland Board meeting that approved the *RMP* for submission (27th January 2021): Board Meeting Papers (audit-scotland.gov.uk) (agenda item 15).

The *RMP* is based on the Keeper's, 15 element, Model Plan http://www.nrscotland.gov.uk/record-keeping/public-records-scotland-act-2011/resources/model-records-management-plan.

Audit Scotland make the following statement in their *Records Management Policy* (see element 3): "We recognise that the efficient management of our knowledge, information and records is essential to support our work, to facilitate our governance and management, to manage risk and to comply with our legal obligations under the Act and other legislation as enacted from

time to time." (*Policy* section 2). The Keeper fully agrees this statement.

The authority refers to records as a business 'asset' (for example *Records Management Policy* section 3, *Archiving Procedure: Guidance for All Staff* section 1 or *Information Security Management Policy* section 4.6). This is an important recognition and the Keeper commends it.

Key Group

Audit Scotland operate a Knowledge, Information and Technology Governance Group (KITGG) who are responsible for "keeping records management policy and arrangements robust and up to date".

The Keeper has been provided with the KITGG *Terms of Reference* (October 2019). They meet six times a year and, among other roles, they oversee the annual review of information and records management policies and also review the information risk register.

The Chief Operating Officer/SIRO (see element 1) and the Corporate Governance Manager (see element 2) sit on the Group. The Corporate Governance Manager (see element 2) has a responsibility to Support "the work of Audit Scotland's Knowledge, Information and Governance Group (KITGG) as secretary, providing advice and guidance on information governance issues, including records Management…" (*Corporate Governance Manager Job Description*).

The KITGG oversees the Audit Scotland *Retention Schedule* (see element 5)

The KITGG supports the Senior Information Risk Officer (see element 1) "by ensuring that robust policies, procedures, systems and processes are in place to manage information risks." (*KITGG Terms of Reference* – section 5 supported in the *Information Security Management Policy*). For example: "The Information Security policy is reviewed annually and presented to the Knowledge, Information and Technology Governance Group (KITGG). The KITGG recommend it to the Management Team who in turn recommend it to the Board for approval thereby ensuring oversight and commitment at the highest level for information security." (*RMP* page 13).

The KITGG is responsible for ensuring information security policies are communicated, reviewed and updated in response to changes in risks faced by Audit Scotland, legislation, and internal operational working practices. (*Information Security Management Policy* section 12)

It is the KITGG's role to ensure the *Records Management Policy* (see element 3) "remains relevant, represents good practice and is implemented effectively." (*Records Management Policy* section 9)

Regular updates on data protection are scrutinised by the KITGG who approved the *Data Protection Policy* in 2021 (see element 9).

The KITGG assesses and mitigates information security risks (*Information Security Management Policy* section 11)

This group is clearly of fundamental importance to the records management provision in Audit Scotland. The Keeper thanks the authority for providing details of their work.

6. Keeper's Summary

Elements ***1 -15*** that the Keeper considers should be in a public authority records management plan have been properly considered by Audit Scotland, the Accounts Commission for Scotland and the Auditor General for Scotland. Policies and governance structures are in place to implement the actions required by the plan.

Elements that require development by Audit Scotland, the Accounts Commission for Scotland and the Auditor General for Scotland are as follows:

7. Archiving and Transfer - Formal deposit agreement required

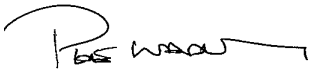
11. Audit Trail - Document naming conventions should be issued to staff

7. Keeper's Determination

Based on the assessment process detailed above, the Keeper **agrees** the RMP of **Audit Scotland, the Accounts Commission for Scotland and the Auditor General for Scotland**.

- The Keeper recommends that Audit Scotland, the Accounts Commission for Scotland and the Auditor General for Scotland should publish its agreed RMP as an example of good practice within the authority and the sector.

This report follows the Keeper's assessment carried out by,



…… ……

Pete Wadley
Public Records Officer

Liz Course
Public Records Officer

8. Endorsement of Report by the Keeper of the Records of Scotland

The report has been examined and is endorsed under the signature of the Keeper of the Records of Scotland as proof of compliance under section 1 of the Public Records (Scotland) Act 2011, and confirms formal agreement by the Keeper of the RMP as submitted by Audit Scotland, the Accounts Commission for Scotland and the Auditor General for Scotland In agreeing this RMP, the Keeper expects Audit Scotland, the Accounts Commission for Scotland and the Auditor General for Scotland to fully implement the agreed RMP and meet its obligations under the Act.

……

Paul Lowe
Keeper of the Records of Scotland