The Public Records (Scotland) Act 2011

Skills Development Scotland

Progress Update Review (PUR) Report by the PRSA Assessment Team

17th March 2021

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 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 recordkeeping 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. Progress Update Review (PUR) Mechanism

Under section 5(1) & (2) of the Act the Keeper may only require a review of an authority's agreed RMP to be undertaken not earlier than five years after the date on which the authority's RMP was last agreed. Regardless of whether an authority has successfully achieved its goals identified in its RMP or continues to work towards them, the minimum period of five years before the Keeper can require a review of a RMP does not allow for continuous progress to be captured and recognised.

The success of the Act to date is attributable to a large degree to meaningful communication between the Keeper, the Assessment Team, and named public authorities. Consultation with Key Contacts has highlighted the desirability of a mechanism to facilitate regular, constructive dialogue between stakeholders and the Assessment Team. Many authorities have themselves recognised that such regular communication is necessary to keep their agreed plans up to date following inevitable organisational change. Following meetings between authorities and the Assessment Team, a reporting mechanism through which progress and local initiatives can be acknowledged and reviewed by the Assessment Team was proposed. Key Contacts have expressed the hope that through submission of regular updates, the momentum generated by the Act can continue to be sustained at all levels within authorities.

The PUR self-assessment review mechanism was developed in collaboration with stakeholders and was formally announced in the Keeper's Annual Report published on 12 August 2016. The completion of the PUR process enables authorities to be credited for the progress they are effecting and to receive constructive advice concerning on-going developments. Engaging with this mechanism will not only maintain the spirit of the Act by encouraging senior management to recognise the need for good records management practices, but will also help authorities comply with their statutory obligation under section 5(1)(a) of the Act to keep their RMP under review.

3. Executive Summary

This Report sets out the findings of the Public Records (Scotland) Act 2011 (the Act) Assessment Team's consideration of the Progress Update template submitted for Skills Development Scotland. The outcome of the assessment and relevant feedback can be found under sections 6 – 8.

4. Authority Background

Skills Development Scotland (SDS) is the national skills body supporting the people and businesses of Scotland to develop and apply their skills. SDS was formed in 2008 as a non-departmental public body, bringing together careers, skills, training and funding services. SDS plays a key role in driving the success of Scotland's economic future, working with partners to:
- Support individuals to reach their potential
- Help make skills work for employers
- Improve the skills and learning system.
- SDS is preparing Scotland's workforce to "maximise opportunities in today's dynamic world".

5. Assessment Process

A PUR submission is evaluated by the Act's Assessment Team. The self-assessment process invites authorities to complete a template and send it to the Assessment Team one year after the date of agreement of its RMP and every year thereafter. The self-assessment template highlights where an authority's plan achieved agreement on an improvement basis and invites updates under those 'Amber' elements. However, it also provides an opportunity for authorities not simply to report on progress against improvements, but to comment on any new initiatives, highlight innovations, or record changes to existing arrangements under those elements that had attracted an initial 'Green' score in their original RMP submission.

The assessment report considers statements made by an authority under the elements of its agreed Plan that included improvement models. It reflects any changes and/or progress made towards achieving full compliance in those areas where agreement under improvement was made in the Keeper's Assessment Report of their RMP. The PUR assessment report also considers statements of further progress made in elements already compliant under the Act.

Engagement with the PUR mechanism for assessment cannot alter the Keeper's Assessment Report of an authority's agreed RMP or any RAG assessment within it. Instead the PUR Final Report records the Assessment Team's evaluation of the submission and its opinion on the progress being made by the authority since agreeing its RMP. The team's assessment provides an informal indication of what marking an authority could expect should it submit a revised RMP to the Keeper under the Act, although such assessment is made without prejudice to the Keeper's right to adopt a different marking at that stage.

Key:

G	The Assessment Team agrees this element of an authority's plan.		A	The Assessment Team agrees this element of an authority's progress update submission as an 'improvement model'. This means that they are convinced of the authority's commitment to closing a gap in provision. They will request that they are 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 Assessment Team may choose to notify the Keeper on this basis.

Progress Update Review (PUR) Template: Skills Development Scotland

Element	Status of elements under agreed Plan 10JUL14	Progress assessment status 23APR19	Progress assessment status 17MAR21	Keeper's Report Comments on Authority's Plan 10JUL14	Self-assessment Update 23APR19	Progress Review Comment 23APR19	Self-assessment Update as submitted by the Authority since 23APR19	Progress Review Comment 17MAR21
1. Senior Officer	G	G	G	Update required on any change	No change on this element, the senior officer remains Laura Barjonas, Head of Corporate Office.	No immediate action required. Update required on any future change.	The senior officer remains Laura Barjonas, although her role is now as Head of IGOR (Information Governance and Organisational Resilience) rather than Head of Corporate Office.	The Keeper's Assessment Team thanks Skills Development Scotland (SDS) for this update which has been noted.
2. Records Manager	G	G	G	Update required on any change	The post and the post-holder have both changed since the submission of the SDS RMP. Kenneth Parker, as the Information Governance Advisor, now has responsibility for records management. Role description for the new post is included as a supporting document for this update.	The Keeper's Assessment Team thanks the authority for the update regarding the changes to both the post and the post-holder. Submitted as supporting evidence is the job description for the post of Information Governance Advisor. This clearly describes the roles of the post, including those relating to records management and compliance with the Public Records (Scotland) Act 2011.	The records manager remains Kenneth Parker, Information Governance Adviser	No immediate action required. Update required on any future change.
3. Policy	G	G	G	The current Policy is aligned with the Records Management Strategy and Improvement Plan which identifies the future actions needed to close gaps in the authority's record management provisions. This Plan is intended to be implemented alongside the move to SharePoint 2010. The Keeper requests that he is kept updated as progress is made in both the Improvement Plan and the project to move to SharePoint 2010.	The RM Policy is being reviewed again, in light of the roll-out of Office 365 and the early lessons learned from that. It will be circulated *ex committee* to the Information Governance Scrutiny and Improvement Group as the first step in the approval process.	The implementation of Office 365 will undoubtedly affect the records management procedures within the authority and it makes perfect sense to update the Records Management Policy to reflect these changes. The Assessment Team commends the authority for regularly reviewing key policy documents, particularly when systems or procedures change. The Assessment Team requests that the updated Records Management	The SDS RM Policy is awaiting final sign off ahead of re-issue; it is planned to be re-published and communicated in November 2020. The updated RM Policy has been simplified to focus on key requirements and to clarify expectations of SDS colleagues for managing information effectively within SDS's rapidly evolving IT and digital environment. It stresses the need for colleagues to ensure that the information they are working with is stored in the right place (with guidance on what that means); is appropriately available to SDS colleagues for the medium to long term; and is managed against the declared retention periods.	In their original submission SDS committed to keeping their information governance policies and guidance documents under review and the Assessment Team acknowledges that this is being done.

					Policy is submitted at the next PUR.	SDS started its roll-out of MS Teams in August 2020. By the end of October all colleagues will be using Teams instead of Skype for calls and chat. The collaboration functionality will begin to be rolled out from November 2020 onwards. The policy will be reviewed again in 2021 to take account of how SDS colleagues need to use MS Teams, for both internal and external collaboration, again emphasising the need for long term access to the information and to apply retention periods when they fall due.	
4. Business Classification	A	A	A	A baseline Business Classification Scheme has been submitted which identifies the main record-creating activities and types of records being created across the organisation. The RMP identifies the need for more work to be done to add further categories of records to the BCS.

Over time the authority intends to impose the BCS upon the structure provided through the shift to using SharePoint 2010 as an EDRMS.

The Keeper can agree this element on an 'improvement model' basis, provided he is supplied with evidence of progress of this project as it continues. | Each major section of the Business Classification Scheme was agreed and signed off by the relevant Head of Service, with the major record types identified for each area. Subsequently, the structure was created within SharePoint 2010 which was the platform for IShare, SDS's EDRMS tool.

During FYs 2017-18 and 2018-19 SDS ran a major business change project to move to Office 365. One aspect of this was the re-working of IShare from its previous SP 2010 platform to work on SP Online. During that transition, the BCS for each area was re-validated and again used as the basis for the file plan within the EDRMS.

One output of the GDPR Readiness Project (see Element 9) was a revised information asset register (IAR) which, in part, provides details of significant record types held outwith the EDRMS. Ensuring that the IAR remains up to date and | The authority's identification of records created in carrying out its business has evolved over time. The Business Classification Scheme (BCS) was used as a structure for records managed within SharePoint 2010 using the IShare platform. Over the last couple of years the authority has moved to Office 365 and SharePoint Online and has amended IShare to reflect this. The BCS has been re-validated and continues to act as the file plan for IShare. The Assessment Team commends the recognition of the importance of imposing a structure on records, irrespective of the system used to create and manage them.

As part of the work to prepare for GDPR the authority revised its Information Asset Register (IAR). The IAR lists records held outwith the EDRMS. Work is ongoing to ensure that the IAR and BCS complement each other and cover the record types created and managed by the authority. The Assessment Team request that at the next PUR they are sent samples of the | Work is underway to simplify the current approach to the BCS. The feedback from the business was that it was too granular and too difficult to read. The new approach no longer incorporates the same depth of detail of the as built EDRMS file plan in the BCS. Instead, it seeks to capture just the major classes of information held under each functional activity as well as the applicable retention period and justification for it. It is anticipated that this will make it easier for information asset owners across SDS to review and amend the BCS for their activities. It should also make it easier for the RM team to make use of the information held there. | The Assessment Team thanks SDS for this update.

If a simplified structure provides SDS with a more useful business tool then it is to be encouraged. Particularly if this leads to better user engagement.

The Keeper is open to whichever system an authority choses to operate as long as it records, at a given point in time, all the public records the business creates and maintains, and explains in which function or service area these records are held. Furthermore, all of the records an authority creates should be recorded within a single structure, even if it is using more than one record system to manage its records.

As long as SDS is pursuing the imposition of this type of structure on their public records, irrespective of the system used to create and manage them, the Keeper should be able to agree it complies with the requirements of his Model Plan and |

					complements the information held within the EDRMS will form a significant piece of work within the business as usual activities of the Information Governance and Data Protection teams.	BCS and IAR as evidence of progress in this area. If this were a formal re-submission it is anticipated that this Element would remain Amber, reflecting the ongoing work in developing a comprehensive classification of all record types. The Assessment Team commends the work undertaken to date and looks forward to hearing about further progress in future PURs.		therefore with PRSA. The Assessment Team looks forward to updates in subsequent PURs. This element remains at Amber while the work explained in the PUR is ongoing. The Assessment Team remind SDS of the importance of appropriate polices, governance and staff training in making this project a success.
5. Retention Schedule	A	A	A	A baseline Retention and Disposal Schedule has been submitted which sets out the actions to be taken against the categories of records created by SDS. The RMP recognises gaps in the retention schedule and throughout 2014-2015 will fill these. Once the Schedule is updated it will be rolled out across the organisation as part of the project to implement SharePoint 2010. The Keeper can agree this element on an 'improvement model' basis, provided he is supplied with evidence of progress as the project continues.	The corporate default of a 4-year retention period followed by deletion has been incorporated into the configuration of the EDRMS – IShare Online. Also included is the capability to apply other values for the retention period if business need requires it. A significant proportion of SDS is working to the default value, while customised values have been applied in other areas (such as Finance and HR). The implementation of the retention periods and automated deletion has been successfully implemented within Ishare Online, which is now hosted on SP Online. While successfully tested at low volumes, a remaining technical challenge is to ensure that the system issues notifications at the end of the retention period at the scale required.	It is clear from the update that a lot of work has been done to standardise and implement retention schedules across the authority. The use of Ishare has allowed the more consistent application of retention decisions and has led to the automated deletion of the vast majority of records on the system. A default retention period of 4 years has been applied to the majority of corporate records, but Finance and HR records have been given alternative retention periods. The Assessment Team would like to remind the authority that records such as the minutes of Board meetings and strategy documents may have longer term archival interest and appropriate retention periods and actions should be applied to these. The authority has also given consideration to records and information shared externally and the need to apply retention decisions. The Assessment Team commends the authority for this	A systematic review of retention periods is currently underway. This will take in details from the Information Asset Register, the existing retention schedule and the as-built retention periods in Ishare Online (the SDS EDRMS). The intention here is in two-parts: to help clarify the appropriate retention periods for some of the information assets and to ensure that there is consistency across SDS. This work should conclude by March 2021. Implementation of the review, depending on the extent of its findings and whether system development is required, may well require two to three to complete. Ishare Online was always intended to have an automated retention function. The initial implementation of this did not work at scale. A revised approach passed UAT in late 2019 but has not yet been activated in the live system, in large part due to resource issues and changes in support contracts. Work is just starting (Oct 2020) to assess what the impact would be of turning the automated retention mechanism on. The process the app manages is: i) Identify which files have exceeded their retention period ii) Notify the information owner and author, to allow them a period of time (42 days) to review the file(s) and decide to retain or delete them iii) If no decision is made after the review period expires the file(s) will be deleted. The potential impact is that some unknown fraction of the files in the EDRMS are beyond their retention period + review	The review of retention decisions is welcome. A retention schedule is a 'living document' and will be subject to continual minor change year on year. However, it is clear from this PUR that a more substantial retention review project is underway in SDS. There is clearly an expectation to have reached a milestone in the project in the next month or two. The Assessment Team looks forward to updates in subsequent PURs. This element remains at Amber while the work explained in the PUR is ongoing.

| | | | | | The move to O365 offers a lot of functionality, with the ability to easily share & co-author material with external partners an obvious potential benefit. The implementation of such external sharing will only be done outside of the EDRMS, so there is an information governance task to ensure that appropriate retention periods are still applied within the SP Online sites being used for the external collaboration.

During FY2017-18 SDS ran a GDPR-Readiness project (see Element 9). One output from that work was a set of retention periods (& justifications) for the structured data held in the various enterprise systems. An interesting piece of work will be done during FY 2019-20 to ensure that the retention periods within the EDRMS, the enterprise systems, the inventory of hardcopy material in off-site storage and the external sharing sites are all consistent.

To support staff in determining which retention period they should be applying for a given record type the IG team are producing both a summary and a full retention schedule. These will be 'live' documents and subject to rolling updates during the work to ensure consistent retention periods. | consideration.

Work to ensure that the retention schedules for records and information stored on Ishare, enterprise systems, in hard copy and also used in sharing sites are all consistent will be undertaken in the following financial year (2019-20). The Assessment Team commends this commitment of time and resources and looks forward to being kept updated on this work in subsequent PURs.

The update describes an initiative to provide staff with a summary retention schedule alongside the full version. This seems to be an effective way to ensure staff uptake and participation in ensuring that retention periods are applied in practice.

If this were a formal re-submission it is anticipated that this Element would remain Amber, reflecting the ongoing work to develop and ensure the consistent application of retention schedules. | period and so would be deleted overnight if the app was enabled. The goal is to have the app enabled before the end of Mar 2021 but that date depends on the scale of remedial work needed to address the impact described. | |

| 6. Destruction Arrangements | G | G | G | The Keeper commends the current destruction arrangements and requests updates on the planned centralisation of destruction contracts and the digitisation of some records. | SDS previously had a Retention and Disposal Policy which detailed the destruction process in place for information in all formats, including electronic records held in IShare. While the advice to staff on this subject remains the same, the policy itself has been subsumed into the RM Policy, rather than continuing as a distinct policy.

Convenience copies of documents are destroyed through one of two routes, depending on their information classification, either sent for recycling in the office waste or placed in 'confidential' waste bins and securely destroyed off-site.

SDS completed the process of selecting a single supplier for its hard copy off-site archiving. DataSpace (Scotland), now part of Cube Datastore, won the contract. The destruction of any of the hardcopy material in store will be carried out through them using Highlander International, which is accredited to EN15713. SDS's internal guidance to staff on this topic is currently being revised to take account of these changes.

For born-digital records held within IShare Online, the destruction arrangements rely on how SharePoint Online manages the deletion of files. At the point of deletion, a file remains recoverable by super-users from the system recycle bins (either local | The Assessment team notes the incorporation of destruction processes in to the Records Management Policy.

The update outlines that paper copies of temporary copies of records are disposed of according to their security classification. This is considered to be best practice.

The authority has selected a single supplier for providing off-site storage of its semi-current hard copy records. Destruction of these records is carried out by the supplier and the authority is in the process of updating staff guidance to reflect these changes. The Assessment Team commends the consolidation of semi-current paper records into one location as this should provide greater control over their management and eventual disposal.

Electronic records held on the IShare Online system are disposed of after 93 days. Other business systems dispose of these records after different periods. This ensures that deleted electronic records are not kept longer than necessary. The Assessment Team thanks the authority for this update. | Convenience copies of documents are destroyed through one of two routes, depending on their protective marking, either sent for recycling in the office waste or placed in 'confidential' waste bins and securely destroyed off-site.

For born-digital records held within IShare Online, the destruction arrangements rely on how SharePoint Online manages the deletion of files. At the point of deletion, a file remains recoverable by super-users from the system recycle bins (either local or site collection) for 93 days. For a further 14 days after that there is the option to request that Microsoft perform a full site collection restore. This is not a viable option in the vast majority of cases so after 93 days the information will be considered to have been destroyed.

The arrangements for information held within the various enterprise systems vary from system to system. Generally, information can be restored from back-up after deletion although the period when that possible varies between systems. This aspect will be explored more fully in the work to ensure that the various retention schedules are consistent (see Element 5).

SDS uses Cube Datastore to hold hardcopy records for the medium to long term. When records are destroyed the process is carried out to EN15713 and the destruction certificates are retained. | The update outlines that paper copies of temporary copies of records are disposed of according to their security classification. This is considered to be best practice.

Thank you for the update on the destruction of digital records managed on IShare. It is important that the information governance team in an authority have confidence how long back-ups are available (FOI and DP responses for example).

See comments under element 3 above around O365 and the imposition of retention and therefore how IShare documents are auto deleted.

The Keeper can agree that line of business systems, what you call enterprise systems, have adequate records management functionality, but it is important that the IG Team in SDS are fully aware of what this functionality is in each case. This includes how records are deleted when appropriate.

As a matter of fact, these line of business systems (from Case Management Systems to vehicle service check sheets) are on the Keeper's radar for further investigation in the coming year. These often sit outside the main records management system explained in an RMP, but are still records created during an activity undertaken as a public authority pursues its |

					or site collection) for 93 days. For a further 14 days after that there is the option to request that Microsoft perform a full site collection restore. This is not a viable option in the vast majority of cases so after 93 days the information will be considered to have been destroyed. The arrangements for information held within the various enterprise systems vary from system to system. Generally, information can be restored from back-up after deletion although the period when that possible varies between systems. This aspect will be explored more fully in the work to ensure that the various retention schedules are consistent (see Element 5).			**statutory functions. This means that they are covered by PRSA. In the future it is likely that the Keeper will require authorities to go into more detail on these systems.** It is noted that SDS ensures that third parties, for example trainers, properly dispose of the records they create when engaging with them. This is to be commended. The Assessment Team also notes the destruction arrangements operational in the third party storage contractor.
7. Archiving and Transfer	**G**	**G**	**G**	SDS are working on identifying records that may be suitable for long-term preservation and have provided a draft list of records. The Keeper would like to be updated should the list be amended as work continues on finalising the retention schedule. Similar to the destruction of records SDS is looking at centralising its approach to the archiving of records. The Keeper requests that he is kept informed of progress towards this. SDS are working towards establishing a Memorandum of Understanding (MoU) with the National Records of Scotland. The Keeper requests that he is provided with a copy of the MoU	SDS has completed a tendering exercise in Summer 2017 to bring all of its hard-copy archiving needs within one contract. The successful company was DataSpace (Scotland), which has since (Summer 2018) become part of Cube Datastore. SDS intends to keep operational records at this facility for physical convenience, rather than long term preservation. SDS has yet to finalise a Memorandum of Understanding (MoU) with the NRS for transfer of archival records. Work on this was put on hold by SDS when a key member of the team went on extended	The authority has selected a single supplier for providing off-site storage of its semi-current hard copy records. This is an appropriate measure and should allow greater control over the management of these records. The Assessment Team look forward to seeing a finalised MoU with NRS for the identification and transfer of archival records in due course. This will need to include the transfer of born digital records and it is positive to see that SDS are aware of their responsibilities in this area.	There is only a little progress to report. SDS received the draft of the MOU from the team at NRS in late 2019. Internal review of it concluded that there were no legal concerns with it. There is a concern that the Controller-Processor relationship defined in it could place a large resource burden on SDS that SDS might not be able to meet. The record set that would be passed for permanent preservation has yet to be agreed. More progress on that is expected once the review of the BCS has been completed.	Thank you for this update. The Keeper fully agreed this element of the SDS RMP in 2014 and no retrograde actions have occurred since that date. The 'green' rating therefore remains. However, you should be aware that, if this were a formal resubmission, it is possible that the Keeper would 'downgrade' this element to Amber as no formal agreement exists between the authority and the archive provider. It is important that you are back in contact with NRS Client Management, particularly as you have

				once it is ready to provide evidence that proper arrangements are in place.	family-leave. SDS has recently re-engaged with the NRS team on this. It is expected that the vast majority of the records deemed to be suitable for permanent preservation with the NRS shall be born digital and that of the material in off-site storage with Cube Datastore the majority are operational records held for audit requirements.		concerns over the controller/processor balance. I have checked and your 'manager' is Laura Gould laura.gould@nrscotland.gov.uk The Assessment Team understands that the review of retention provides an ideal opportunity to fully identify records worthy of permanent preservation by NRS. However, the MoU process could be restarted before/during that selection process.
8. Information Security	G	G	G	The RMP states that information security policies are currently being reviewed. The Keeper commends the regular review of policies and asks that he is provided with updated policies should substantial change occur following these reviews.	Since the 2017 update there have been significant changes in SDS's approach to Cyber Security. A new multi agency (SDS, SE and HIE) Security Council has been established to deliver enhanced Cyber Security practice to all partners. The partners have all also committed to being Scottish Government Cyber Catalysts and becoming exemplars of best Cyber Security practice for the Public Sector. SDS has also been implementing the Scottish Government 'A Cyber Resilience Strategy for Scotland: Public Sector Action Plan 2017-18'. This has involved taking on NCSC Active Cyber Defence measures, sharing intelligence via the Cyber-security Information Sharing Partnership (CISP), and undertaking independent assessment of our Cyber controls. SDS has adopted the ISO 27001 standard as best cyber security	Working collaboratively with appropriate partners is a sensible and effective way to develop further the existing good practice in information security. Cyber security is undoubtedly challenging for all public authorities and working together enables all partners to benefit from shared experience and improvements. The commitment to being public sector Cyber Catalysts along with achieving ISO 27001 demonstrates a strong and solid approach to ensuring the security of digital information, which is currently the main format used by SDS. This is exemplary work and the Assessment Team would welcome the sharing of these skills and experience with other public authorities.	The changes reported in 2019 are now fully embedded, with the Security Council driving changes in cyber security practices across the organisations (SDS, HIE, SE and now SoSE) which SDS EIS (Enterprise Information Systems) supports. The organisational commitment to information security remains strong with the team in EIS being increased in size and having (from November 2020) its own head of service. The Security Operations Centre (SOC) is fully operational, with staff there making use of the monitoring and discovery tools available through Microsoft 365 to better understand how the network environment, how colleagues are using it and where vulnerabilities may lie. SDS has not yet met the accreditation requirements for Cyber Essentials Plus; the external review for Cyber Essentials Plus accreditation (covering EIS, SDS, SE and HIE) is due to take place in November 2020. The work to date towards accreditation has highlighted areas for improvement particularly around business controls and procedures. The first half of 2020 saw a cyber security maturity assessment carried out by an external organisation (likewise covering SDS, SE and HIE). This too highlighted procedural improvements, both within the business and within EIS, that should be made. A senior-level SDS Cybersecurity Working Group has been established (October 2020) to drive implementation of the improvement actions related to Cyber Essentials Plus and the SDS Cyber Maturity Assessment. Once that work has been completed SDS	Thank you for this update. It is encouraging that the information security team has been expanded. The cyber security training for the ARC and Board members was delivered in Dec 2020. For staff training see element 12 below.

					practice and has aligned its policies and procedures to the standard. Senior management are engaged in oversight and governance bodies are in place. A dedicated Cyber Security team sits within our EIS department to provide assurance and incident response. Additionally, SDS are working towards Cyber Essential plus accreditation in 2019. In preparation for GDPR SDS ran a project to ensure that our response to a data breach incident was compliant with the new legislation. A new Information Asset Register has also been established to support GDPR compliance and the role of DPO has been assigned. Going into 2019 the EIS Cyber Security team is being expanded to take on additional responsibility for non-EIS delivered systems and to implement an enhanced Security Operations Centre capability.		will be in a more informed, more robust position as regards its information security posture. Recognising the important role of SDS's strategic leadership in supporting continuing improvements in information security, a training session on cyber security has been commissioned from an external organisation for SDS Audit & Risk Committee and Board members; this is scheduled for December 2020.	
9. Data Protection	**G**	**G**	**G**	Update required on any change	From May 2017 to August 2018, SDS carried out a GDPR readiness and implementation project. Highlights of the project's activities include: complete revision of SDS's information asset register; a double opt-in marketing campaign to achieve GDPR compliance and best practice; an update to our policies, privacy notices, registration	SDS have approached the changes in data protection requirements pro-actively and have clearly undertaken a comprehensive review of all aspects of the business. The range of training described shows a commitment to ensuring that all staff are aware of these legal requirements. These are now embedded in routine working practices which is to be commended. Continuing development	Following the conclusion of the GDPR project in August 2018, activity has transitioned to business-as-usual work, with data protection awareness having increased across the organisation. Processes including data subject access requests (SARs) and data protection impact assessments (DPIAs) have been updated to achieve best practice and ensure that data protection implications are addressed for every project using personal data. Extensive work has been done on data sharing agreements (see Element 14), privacy notices for the major SDS platforms as well as for handling staff data and an updated Cookie Policy has been issued.	As with all other Scottish public authorities Skills Development Scotland have been required to review and update their data protection procedures in light of the 2018 legislation. The Assessment Team acknowledges that the public facing SDS website has been updated appropriately: Privacy	Skills Development Scotland

				forms and contracts; an audit and review of key systems; a GDPR training module with 100% staff completion; tailored training provided to staff in high-priority areas of the business; an agreed approach to updating or creating data sharing agreements for all of SDS's contractors and partners; stronger links with external partners and stakeholders as well as a greater cultural awareness within SDS of the importance of Data Protection. Following the conclusion of the GDPR project in August 2018, activity has transitioned to business-as-usual and post-project work with the aim of achieving best practice across the organisation by 2020. Work in this area will largely focus on data sharing, the ability to perform supply chain compliance checks, the integration and collaboration between key internal systems, further tailored training to key colleagues and an ongoing review of the project outputs.	and improvement is clearly also part of normal business practice for SDS in this area. The proposed future plans show that SDS are aware of the need to review and update practice and policy on an on-going basis. The Assessment Team welcome this attitude and the very thorough approach that has been adopted, and would be interested to hear of further developments in future PURs.	The SDS Information Asset Register and Record of Processing Activity (ROPA) has gone through a full update, ensuring that we know how long personal data is being stored, for what purpose, and where. Given the current climate of leaving the EU and the invalidation of the US Privacy Shield, a strong focus was placed on where personal information is stored, in order to identify any potential cases of having information stored in the United States. Staff training has continued, with all new employees being required to complete a data protection training module, and further updated training is in discussion for next financial year	Continuing development and improvement is clearly also part of normal business practice for SDS in this area (for example on data sharing agreements). In their original submission SDS committed to keeping their information governance policies and guidance documents under review and the Assessment Team acknowledges that this is being done. For staff training see element 12 below.
10. Business Continuity and Vital Records	**G**	**G**	**G**	The Keeper welcomes SDS' intention to review their Business Continuity Plans after each test, to internally audit compliance with each BCP, and to review their business continuity policies and procedures. The Keeper would like to receive updates on these reviews and audits and requests that he is informed should any policies and procedures change.	Some changes and business improvements have occurred since 2014: SDS has adopted 'ClearView' as its business continuity management (BCM) tool. The application supports the entire BCM lifecycle, as identified by industry standards such as ISO 22301: Impact Analysis, Risk Assessment, Plan Development, Plan	SDS has experienced some live incidents which have tested their Business Continuity systems as well as planned exercises. Learning from these is good practice and the SDS has now developed an extensive framework to deal with business continuity arrangements. The use of ISO 22301 to inform the continued development of the SDS business continuity framework demonstrates that the SDS recognises	SDS has experienced a number of additional incidents since the last update, including theCOVID-19 pandemic. The response to this has tested the overall maturity and embedded nature of Business Continuity in SDS and it has continued to show that Business Continuity is viewed as a critical function within SDS. In the past year, there have been a number of exercises and workshops to further embed Business Continuity and Incident Management within SDS including Crisis Management Training which was attended by the majority of SDS Senior Management. This training, held in February and run in conjunction with an	The Keeper originally fully agreed this element of the SDS plan referring to the importance of testing business community arrangements. In 2020 the business continuity arrangements in the Scottish public sector were severally tested by the Covid-19 pandemic. This PUR suggests that this worked well in SDS. The 2019 test, reported on in the PUR, almost certainly

					Maintenance, Plan Approval, Plan Exercising and Incident Management. Additionally, the SDS Business Continuity Framework has been developed to capture all components of our BC arrangements and overall approach. This includes the updated Incident Management Process, with its Gold, Silver and Bronze sub-processes, which identify the actions based on the assessed business impact (High, Medium and Low) of the incident. Within ClearView, each site and business unit has updated its business continuity plan, in which each identify their vital records, and business impact assessment. These include refreshed values for the RTO (recovery time objective) and RPO (recovery point objective) values for SDS's information systems. Business continuity and disaster recovery planning is complemented by a programme of exercises. In 2016, this involved EIS and its major service suppliers. Since then there have been a number of live incidents and/or exercises, including site closures for a variety of reasons, Wannacry cyber-attack, data breach and epidemic, and future ones are planned. The lessons learned from these live incidents/exercises are fed back into the review	the value of these standards in leading good practice. It is particularly helpful to hear that the vital records are being identified at an appropriate level for the needs of SDS. The Assessment Team commend the robust development of business continuity plans and would welcome updates in future PURs.	external consultancy with a wealth of experience in crisis management and included a number of scenarios one of which was pandemic related. This built on the pandemic preparedness work already being undertaken by the Business Continuity Team and proved invaluable when COVID-19 impacted us. Nation-wide scenario testing with responsible staff across the entirety of Scotland was completed in 2019, with each region undertaking a local scenario testing session facilitated and led by the BC Team. This, alongside the creation of the Organisational Resilience Advisory Group comprised of representation from across the business to encourage and embed organisational resilience across the organisations, highlight the commitment that SDS has to business continuity. All Business Continuity plans within SDS are being updated in line with their annual review, with extra consideration given to matters relating to critical functions and role cover in the time of COVID-19. These plans are still held in the business continuity system Clearview, which has been re-procured for an additional four years from March 2020 to ensure consistency and availability of the business continuity plans in SDS.	helped with the 2020 response. For staff training see element 12 below. For review see element 13 below.

					of existing BCPs and are used to inform the evolution of the BC processes.			
11. Audit Trail	A	A	A	SDS recognise that audit trail provision is inconsistent within the organisation and will seek to improve this through implementation of the SharePoint 2010 project. SDS have submitted several draft documents showing their commitment to bridging the gap in audit trail provision. The Keeper can agree this element of the RMP on 'improvement model' terms, provided that he is kept informed on the development of audit trail functionality as the project to implement SharePoint 2010 progresses. Additionally, he will need to see the above draft documents once they have been approved and implemented.	As mentioned under Element 7, SDS has consolidated its archiving arrangements into one contract. Requests for the deposit or retrieval of hard-copy records are made to the Information Governance Team, who then liaise with the supplier until the task is completed. The email chain is retained to provide an audit trail for each transaction. Any audit trail of the work behind the creation of the hardcopy records resides with the teams creating them, rather than within the central IG team. SDS is in the final stages (due for completion in the current financial year) of moving from its older SharePoint teamsites and shared drives to having all its unstructured information in the Microsoft Cloud, principally on OneDrive and IShare Online (SharePoint Online). Both those platforms provide information about the version history of files, giving a clear audit trail of who changed content and when the changes were made.	SDS is working hard towards implementation of an audit trail for its digital records, through the use of an EDRMS. Considerable work has been undertaken on moving unstructured digital files into the EDRMS where they can be managed and subject to an audit trail. There is work still to be done on developing systems to keep track of paper documents but the use of IShare will provide an easier method of tracking changes to documents and ensuring that information can be appropriately audited. At present this Element remains at Amber but there is good progress evident. Once the digital records have all been moved to IShare and equivalent systems and there is a clear system and procedures for tracking paper records then, with supporting evidence, the Assessment Team would expect that this Element would be well on its way to achieving a Green RAG rating.	Work is still ongoing in order to ensure that digital information is stored correctly with an accurate audit trail. The shift from older Sharepoint team sites and shared drives is complete, apart from a few small exceptions that still require Shared Drive access for limited use. These are limited in scale, and the large majority of unstructured information in SDS is stored in IShare Online (a Sharepoint Online site) and OneDrive for Business. Audit trail arrangements for the electronic systems encompass a variety of technical and working solutions. For OneDrive for Business, there is a version history that details any changes that are made to the file, and by whom. This is also present in Sharepoint Online, which also includes a record of the last 90 days of moves, renames and deletions in the native details pane of a document library. For large scale content moves, the Records Management team keeps a manual log of the migrations of files. Both Sharepoint Online and OneDrive for Business. have readily accessible audit trails and, in conjunction with the features accessible by the IT department in the Security and Compliance Center, provide an accurate record of changes, edits and access to information (the latter through the compliance center only). In practice, the Compliance Center tools are only used to investigate a potential breach. All of SDS's hardcopy records are stored at Cube Datastore, an off-site storage facility. Access to these files is limited to the RM Team and, in some instances, accessed by members of the business area that owns the information. Any access to the files is on a case by case basis and managed by the RM Team. Index accession files are kept for new material entering the store and destruction certificates are retained for those items reaching the end of their retention period.	At the time of the last PUR the Assessment Team noted that they required further information about the tracking of hard-copy records. They are happy to report that this has now been provided. For digital records, SDS has now almost entirely moved away from shared drives to a authority-wide electronic solution called IShare. This uses Microsoft 365 functionality. **See element 3 for comments on this transition.** The Assessment Team agree that O365 has a powerful search facility which should greatly improve document tracking. It also imposes version control. However, in order for this element to be graded as 'green' in a formal resubmission the Keeper would require that staff guidance, particularly around the authority naming convention, was provided. At present this Element remains at Amber but there is good progress evident and the Assessment Team would expect that this Element would achieve a Green RAG rating if formally resubmitted.
12. Competency Framework	G	G	G	The Keeper commends efforts by SDS to develop a programme of training through the SDS Academy and to create a Working Group of Records	SDS expects different levels of RM-related competency for three groups of staff: • all staff (who should	Although it is to be expected that SDS would have an excellent understanding of the different levels of skills and competencies required by	Since the last PUR, the framework has been developed further in SDS by defining the RM responsibilities and competencies of a fourth group of colleagues, Information Asset Owners. The four groups of staff which have RM competency expectations	The Keeper expects staff creating, or otherwise processing records, to be appropriately trained and supported.

Management Champions. The Keeper would like to hear further news of these endeavours.

have an awareness of why RM is important to SDS and how good RM practice can help them in their day job as well as being able to use the EDRMS appropriately). This level of competency has been achieved through an e-learning module on RM in the SDS Academy as well as through the training, support & guidance on using IShare Online.

- the Records Management Champions (RMCs) are members of staff from other areas of the organisation who have some local records management responsibilities. Previously, their expected competency was focussed solely on the EDRMS, where they were local super-users and had extra training on the use and features of the system. There is an on-going community of practice for the RMCs and they received enhanced training prior to the roll-out of IShare Online. The expectations of the RMC role are being reviewed as part of an organisation-wide assessment of information-related roles and responsibilities (see Element 13).
- the named Records Manager (Element 2) and Information

staff in relation to their roles, it is nevertheless very encouraging and refreshing to see this articulated clearly. The emphasis on records management training rather than data protection alone is welcome and demonstrates how aware SDS is of its responsibilities.

It is clear that SDS is also aware of the value of measuring itself against standards (as shown in Elements 8 and 9, for example). The development of the RM maturity model is an excellent idea and will enable staff to identify gaps and areas for development The Assessment Team suggest therefore that it may also be helpful to look at the competency framework provided by the Archives and Records Association. This has a number of competencies for records managers in the Process section. https://www.archives.org.uk/cpd/competency-framework.html

This is exemplary work and the Assessment Team would encourage SDS to share their training structure with other public authorities.

are the following:

- Everyone in the organisation, including contractors and temporary staff, is responsible for how SDS manages its information and this is reinforced by policies, guidelines and training..
- The named Records Manager (Element 2) and Information Governance Team are responsible for developing and implementing appropriate RM policies and guidance for SDS as well being subject matter experts on RM, wider information governance topics and the EDRMS. This level of competence has been reached based on previous experience, on-the-job training, self-study and attending relevant CPD, peer and professional networking events, such as those organised by the IRMS
- IShare Supers (hitherto referred to as Records Management Champions) have seen a change in the scope of their role, which has returned to being a role as local super users for the EDRMS, as well as assisting in piloting changes and creating a community of practice internally using Yammer and other tools. They are assisted by guidance written by the Information Governance team.
- The Information Asset Owners (IAOs) are responsible for the relevant retention schedules for their Information Asset, the access requirements for their asset and the application of good records management throughout the asset. Training for Information Asset Owners was piloted with the Information Governance Leadership Group in March, with training to be rolled out to all IAOs in /Q4 2020.

Alongside this work, a Records Management Roles, Responsibilities and Competencies document is being developed to allow the four groups named both to understand the exact expectations of them from SDS as an organisation with regards to Records Management and where to access training and development material to support them to gain the required competencies

Staff training appears to be pursued appropriately in SDS who have consistently updated the Keeper as he requested in his original 2014 agreement.

For example under element 8 SDS report on a training session on cyber security being commissioned from an external organisation and under element 9 the requirement for all new employees to complete a data protection training module. Under element 10 they report on exercises and workshops to further embed Business Continuity and Incident Management within SDS including Crisis Management Training. Again this involved an external consultancy.

It is particularly noted that the use of external training organisations requires a business expense and this is strong evidence that senior managers at SDS consider information governance training appropriately.

The Assessment Team notes that further updated training is in discussion for next financial year.

					Governance Team are responsible for developing and implementing appropriate RM policies and guidance for SDS as well being subject matter experts on RM, wider information governance topics and the EDRMS. This level of competence has been reached based on previous experience, on-the-job training, self-study and attending relevant CPD, peer and professional networking events, such as those organised by the IRMS. SDS mandates that all staff undertake a minimum of 21 hours of CPD each year, which is tracked through the SDS Academy, so there is an organisational commitment to on-going professional development. Element 13 describes the development of an RM maturity model for SDS. One expected outcome from a self-assessment against that model is an understanding of any gaps in the competency of those groups of staff, particularly the IG team. In turn, that will allow a structured development programme to be put in place, working towards an appropriate accreditation.			
13. Assessment and Review	G	G	G	The Keeper welcomes this authority's commitment to regularly review their records management provisions throughout the organisation and audit the	SDS is committed to reviewing progress of on-going work through a variety of approaches. At SDS each service	SDS shows commendable commitment to continuous review and development and has systems in place which encourage this. There is planned and well-	As previously reported, at SDS each service has a work plan which details the intended activities and goals for the year. Progress is reported against these commitments quarterly. For RM, the plan and the on-going reports are reviewed and	It is a requirement of the Public Records (Scotland) Act 2011 that "An authority must— (a) keep its records management plan under review" (PRSA Part

				progress they are making against their Improvement Plan. Should the intended internal audits for measuring compliance with the records management requirements go ahead in 2015-2016 the Keeper would like to receive updates on the outcome of these. Similarly the Keeper would like to be kept informed if the planned inclusion of compliance with records management policies and procedures within their Business Excellence Approach takes place.	has a work plan which details the intended activities and goals for the year. Progress is reported against these commitments quarterly. For RM, the plan and the on-going reports are reviewed and approved by the Head of Service for Corporate Office (accountable officer named in Element 1), the Director of Finance and Corporate Governance and the Senior Director for Enabling Services. A regular, six-monthly update of compliance with statutory obligations, including the PR(S)A, is provided by Corporate Office to SDS's Audit & Risk Committee. At SDS, the Information Governance Scrutiny and Improvement Group (IGSIG, successor to the previously reported & described IGLG) has the remit to examine information governance issues across the whole of SDS, including RM policy and implementation. In addition to quarterly reporting to IGSIG there will be an annual 'deep dive' into the subject, which will include scrutiny of the then current policy. Following a self-assessment against the Audit Scotland Best Value IM Toolkit a continuous improvement action plan (CIAP) for information governance was developed. The remaining actions are due to be completed by the end of the current financial year and	structured assessment and review built into their business as usual processes. There are appropriate working groups and oversight committees at each level of the organisation. The involvement of the Audit & Risk Committee ensures that this is overseen at a strategic level. The use of the Audit Scotland Information Management toolkit to develop a self-assessment is good practice. Using the JISC Records Management Maturity Model is an excellent way to focus on self-assessment and identify future plans. The SDS will be aware that the original maturity model is available on https://www.jisc.ac.uk/guides/records-management/maturity-model This, combined with the internal audit planned for Jan-Feb 2019, will enable the Information Governance Team to plan future development and consolidate much already excellent practice. The use of the Progress Update Review mechanism is very welcome and it is positive to hear that it complements all the other work that is being undertaken in this area. As with Element 12, SDS has a structured approach that has much to commend itself to others, and the Assessment Team would encourage SDS to share its experience with other public authorities.	approved by the Head of Service for Information Governance & Organisational Resilience (IGOR) (accountable officer named in Element 1), the Director of Finance, Information Governance, Resilience and Risk and the Senior Director for Enabling Services. A regular, six-monthly update of compliance with statutory obligations, including the PR(S)A, is provided by the Corporate Governance team to SDS's Audit & Risk Committee. The Information Governance Leadership Group (IGLG) has been reformed, with revised terms of reference and membership. Its remit remains to examine information governance issues across the whole of SDS, including RM policy and implementation. In addition to quarterly reporting to IGLG there will be an annual 'deep dive' into the subject, which will include scrutiny of the then current policy. SDS now has an Office 365 Management Board. This brings together colleagues from across SDS but mainly from IT, business change and information governance, to govern and manage the roll-out of functionality and applications within Microsoft 365. Supporting the work of the board provides the opportunity to test aspects of RM policy and helps ensure that the policy and guidance provided to colleagues is accessible, understandable and sensible. The internal audit of information and records management practices, mentioned in the previous SDS PUR, was conducted in Jan and Feb of 2019. Its output was largely positive and most of the recommended actions from it have been completed. A further audit in this area (including data protection) is planned for early 2021, although the scope of it has still to be set. The opportunity to participate in the PUR process offers a complementary opportunity for reflection. SDS's intention is to provide a PUR every second year, unless invited to re-submit its records management plan in full. This should allow the small team within IGOR time to develop and implement changes between reports. Those activities all focus on review and assessment of the technical aspects of the	1 5.1.a.) The Assessment Team thanks SDS for the update on the expanded review remit of the Information Governance Leadership Group. Also they note that a particular group has been set up whose remit includes the review of the transition to O365 (IShare). These are welcome developments. The Assessment Team note that all Business Continuity plans within SDS are being updated in line with their annual review, with extra consideration given to matters relating to critical functions and role cover in the time of COVID-19 (see also comments under element 10 above). This PUR reconfirms the robust reporting structures in the organisation. The authority's participation in the PUR process in 2017, 2018 and 2020 demonstrates an ongoing commitment to keeping its RMP under review.

<table>
<tr><td></td><td></td><td></td><td></td><td>include reviewing the existing IG-related roles and responsibilities across SDS.

SDS is at the early stages of developing a RM Maturity Model, based upon the one hosted under the Model Plan Guidance for Element 13. The expectation is to finalise that before the end of the financial year then use that self-assessment and the recommendations from the Internal Audit to inform the future work.

There will be an internal audit of records management work conducted in Jan-Feb of 2019. The scope of the audit is to review the policies, procedures and systems in place to ensure the integrity and security of information held by SDS.

The opportunity to participate in the annual PUR process offers a complementary opportunity for reflection.

These review mechanisms concentrate on the detail of policy, either existing or required. The Information Governance team is participating in a number of internal processes which look at service provision, which in turn may well shed light on the impact of existing policies. These processes include

- A *voice of the customer* workshop, to be held in Jan 2019
- Business</td><td></td><td>RM programme. SDS has strong corporate focus on providing good customer service and on continuous improvement. This applies equally to internal customers as to external. In Spring 2020 the Internal Support Service Survey (ISSS) was held, with IGOR scoring highly for the support, advice and guidance it provides on RM and IG.</td><td></td></tr>
</table>

					excellence self-assessment, to be conducted in Feb 2019 • The bi-ennial *Internal Support Service Survey* (ISSS, last ran in 2018) The output from these processes will then be used to inform both the on-going policy work as well as the development of the Corporate Office Continuous Improvement Action Plan for 2019-20.			
14. Shared Information	**G**	**G**	**G**	Update required on any change	SDS shares information extensively with other public and third sector organisations – local authorities and schools; Scottish and Central Government Depts; as well as charities helping citizens in marginalised or disadvantaged groups overcome barriers to employment. The cornerstone of this sharing is the data sharing agreement (DSA). Each one states what information will be shared between the named parties and what the justification for that sharing is. A key piece of work during the GDPR readiness project was the review of the arrangements for data sharing, bringing the register of data sharing agreements up to date while also reviewing the existing and planned data sharing agreements to ensure that the legal basis for the sharing was documented. This work allowed the data flows across SDS and between SDS and partners to be mapped.	SDS have ensured that data sharing has been carefully considered during the challenges of changes to data protection requirements and the introduction of new IT systems. It is evident that this work is planned and implemented sensibly and steadily.	SDS shares information extensively with other public and third sector organisations – local authorities and schools; Scottish and Central Government Depts; as well as charities helping citizens in marginalised or disadvantaged groups overcome barriers to employment. The cornerstone of this sharing is the data sharing agreement (DSA). Each one states what information will be shared between the named parties, the justification and legal basis for that sharing, and clauses ensuring proper security of the information being shared. A template has been created to ensure all DSAs are uniform in the clauses they contain, with the personal information, the purpose and legal basis for processing, and the transfer arrangements being unique to each third party. The process of creating new data sharing agreements sits with the data protection team, ensuring appropriate safeguards are in place for the use, transfer, and destruction of personal information	The Assessment Team thanks SDS for the detailed explanation of the use of Data Sharing Agreements. At the time of the Keeper's original agreement SDS had provided a template Data Sharing Agreement form, guidance for SDS staff and a published privacy statement. It is good that these have been updated, particularly with GDPR/DP2018 in mind. The Keeper agrees that there are still robust measures in place to ensure that information is properly protected when it is being shared between SDS and partner organisations.

| | | | | A process has been developed to guide the creation of any new DSAs, ensuring the appropriate involvement from data protection staff.

The flexibility and improved functionality offered by Office 365 is offering SDS the option of easier collaboration on joint projects with with other public bodies. The information here is more likely to be centred on corporate or project information rather than personal data. Pilot projects for such sharing, using externally-enabled SharePoint sites to replace email communication, are just beginning at the time of writing. The planned governance approach is very much in line with that for the data sharing agreements – to document what is being shared, between which bodies, for what reasons and what the longer retention and disposition arrangements should be. | | | |

7. The Public Records (Scotland) Act Assessment Team's Summary

<u>Version</u>

The progress update submission which has been assessed is the one received by the Assessment Team on 29 October 2020. The progress update was submitted by Kenny Parker, Information Governance Advisor.

The progress update submission makes it clear that it is a submission for **Skills Development Scotland**.

The Assessment Team has reviewed Skills Development Scotland's Progress Update submission and agrees that the proper record management arrangements outlined by the various elements in the authority's plan continue to be properly considered. The Assessment Team commends this authority's efforts to keep its Records Management Plan under review.

<u>General Comments</u>

Skills Development Scotland continues to take its records management obligations seriously and is working to bring all elements into full compliance.

Section 5(2) of the Public Records (Scotland) Act 2011 provides the Keeper of the Records of Scotland (the Keeper) with authority to revisit an agreed plan only after five years has elapsed since the date of agreement. Section 5(6) allows authorities to revise their agreed plan at any time and resubmit this for the Keeper's agreement. The Act does not require authorities to provide regular updates against progress. The Keeper, however, encourages such updates.
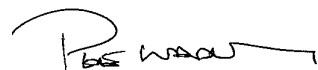
The Keeper cannot change the status of elements formally agreed under a voluntary submission, but he can use such submissions to indicate how he might now regard this status should the authority choose to resubmit its plan under section (5)(6) of the Act.

8. The Public Records (Scotland) Act Assessment Team's Evaluation

Based on the progress update assessment the Assessment Team considers that Skills Development Scotland continue to take their statutory obligations seriously and are working hard to bring all the elements of their records management arrangements into full compliance with the Act and fulfil the Keeper's expectations.

- The Assessment Team recommends authorities consider publishing PUR assessment reports on their websites as an example of continued good practice both within individual authorities and across the sector.

This report follows the Public Records (Scotland) Act Assessment Team's review carried out by,

……………………………………

Pete Wadley
Public Records Officer