The Public Records (Scotland) Act 2011

Skills Development Scotland

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

31st January 2023

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.

6. Progress Update Review (PUR) Template: Skills Development Scotland

Element	Status of elements under agreed Plan 10JUL14	Status of evidence under agreed Plan 10JUL14	Progress review status 17MAR21	Progress review status 31JAN23	Keeper's Report Comments on Authority's Plan 10JUL14	Self-assessment Update 29OCT20	Progress Review Comment 17MAR21	Self-assessment Update as submitted by the Authority since 17MAR21	Progress Review Comment 31JAN23
1. Senior Officer	G	G	G	G	Update required on any 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.	The senior officer remains Laura Barjonas in her role as Head of IGOR (Information Governance and Organisational Resilience).	The Assessment Team thanks you for this confirmation. Update required on any change.
2. Records Manager	G	G	G	G	Update required on any change.	The records manager remains Kenneth Parker, Information Governance Adviser	No immediate action required. Update required on any future change.	The records manager remains Kenneth Parker, Information Governance Adviser	Thank you for confirming there have been no changes to this Element.
3. Policy	G	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.	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	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.	The SDS RM Policy is about to be reviewed for re-issuing; the current issue expires in November 2022. This review will be done alongside the Records Management Competency Framework (see Element 12) and the guidance for colleagues on *what to keep where.* The main points of the policy are expected to remain the same – store information in the right place, manage it against the agreed retention schedule and where	Thank you for this positive update. It is great to hear that the Records Management policy is under review, and that competency framework and RM guidance is being reviewed alongside this.

	🟩	🟩	🟩	🟩	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.	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. 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.		possible & affordable automate that management. Since the last PUR, SDS has rolled out two further phases of MS Teams functionality. SDS colleagues are now using that platform for external collaborations and developmental work within their business areas. While external sharing is governed through a separate policy, which has records management requirements within it, the RM Policy will also include explicit reminders to colleagues that it applies to the information in Teams. Work is being done to see what information can be tracked on how colleagues are using the MS platforms, through the MS Adoption Model which can be visualised in Power BI. This effort is still at an early stage but should allow the RM Team to begin to get an idea of the extent that colleagues are complying with the policy and where to target future training and awareness work.	Thank you also for sharing an update regarding the implementation of new MS Teams functionality and the use of the MS Adoption Model. It sounds like this will hopefully allow for monitoring consistent adherence to policy. The Team look forward to hearing how this progresses in subsequent PURs.
4. Business Classification	A	A	A	G	A baseline Business Classification Scheme has been submitted which identifies 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	The Assessment Team thanks SDS for this update. If a simplified structure provides SDS with a more useful business	The work to simplify the BCS was recommenced in May this year (2022), following a period of resource-limitation, as part of a wider piece of work to revalidate the retention schedule that is in place and to conduct a manual cleanse against that retention	The Assessment Team thanks you for this update which has been noted. If no major delays have

	🟧	🟧	🟧	🟩	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.	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.	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	schedule. Further detail on that work is reported against Element 5 but it, and the BCS update, should be completed by Dec 2022.	taken place since the submission of this PUR, it is assumed that the Business Classification simplification review and update are now complete. To celebrate the progress made, this Element can be turned to Green. This applies to the PURs only and will not change the status of this Element in the Keeper's Agreement. If this was a formal resubmission, upon receipt of evidence of a functional new BCS this Element would likely receive a Green status.

	🟨	🟨	🟨	🟩			able to agree it complies with the requirements of his Model Plan and 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	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	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	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	There is a lot of work being done to update and implement the agreed retention schedules across different platforms. A process of comparing the existing retention schedules within IShare (SDS's EDRMS based in SharePoint Online) with external benchmarks, such as the Scottish Council on Archives Records Retention Schedules (SCARRS) and JISC, is being worked	It is great to hear that efforts have been concentrated on retention scheduling. The implementation of external benchmarks such as SCARRS and JISC is a positive step.

	🟧	🟧	🟧	🟧	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.	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	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.	through, in order to either re-validate the existing retention periods or provide suitable alternatives. Completing this work is an important stepping-stone towards the automated application of the retention periods within IShare. This automation of retention within IShare has been a desired outcome for SDS for some time. Effort to implement this started after the migration to SharePoint Online in 2019 but progress was slow. Work carried out since March 2021 has revealed that the way the retention app has been coded is no longer in line with Microsoft-recommended good practice and as such cannot now be ran within the SDS M365 tenant. The focus of the technical work will now be to either have the retention application re-coded so that is both in line with current MS good practice and as future proof as reasonably practicable or to explore SharePoint retention labels as a potential alternative. There are understood to be undesirable features with the out-of-the-box retention labels (in some circumstances their execution does not leave an audit trail; if a label contains a review process step, the disposition process hangs until the review is completed i.e., if a reviewer does nothing then the file is retained	It is unfortunate that the M365 tenant originally commissioned is not easily modifiable to meet SDS's needs for fully transparent and accountable automated retention decisions, but it is clear from this update that SDS is working towards a solution. This Element will remain at Amber while the work on technical implementation within the two platforms is ongoing. However, it is apparent that SDS is taking steps to ensure that automated retention within IShare (the SharePoint-based EDRMs) will work as desired. The

	🟨	🟨	🟨	🟨		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 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.		indefinitely) so adoption of them would not be straightforward. Whatever the eventual technical implementation there will be a challenging business change process to be gone through to ensure a successful adoption. As access to technical resource to resolve these challenges is proving to be difficult, a manual cleanse of IShare is underway. Retention reports have been produced which include: • The local retention schedule as implemented within IShare • The comparison of that to external benchmarks, as described above, with any areas of significant difference highlighted • A listing, based on the existing retention periods, of those files which have reached the end of their retention period Information Asset Owners are then briefed on the reports relevant to their areas of IShare and are given a period to validate the retention periods or agree changes where there is a need and then to carry out disposition review of the files which are beyond retention. The RM team is providing support to the IAOs to help them understand the report, implement	Assessment Team look forward to being updated on progress in subsequent PURs.

	🟨	🟨	🟨	🟨				any changes to the in-place retention periods (revising the report as required) and to implement the disposition decisions. A pilot of this approach ran successfully over the summer of 2022 and the remaining reports will be issued from October onwards. Completing this work will then mean that the content of the platform will be ‘current’ and that the retention periods will have been re-validated prior to any automation of retention being turned on. Beyond the content held in IShare considerable progress is being made to automate retention within the main line of business systems at SDS. Retention schedules have been agreed for both CSS (Customer Support System) which holds records of interactions with the customers of SDS’s careers information advice and guidance services and FIPS (Financial Information Processing System) which manages payments to the training providers involved with the work-based learning programmes. In both cases the retention schedules have had to take account of operational need, data protection requirements and Scottish Govt’s ask of SDS to produce analyses	

	🟧	🟧	🟧	🟧				of the long-term economic outcomes of citizens using SDS's services. The technical work to implement the agreed schedules within both platforms has begun.	
6. Destruction Arrangements	G	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.	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	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**	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. Since the end of the pandemic restrictions SDS has moved to a hybrid working model, with most colleagues having a working pattern of 1-2 days in the office each week and the others working from home. During the first year of this hybrid working the volumes of material printed will be monitored by one of the senior programme boards. Early feedback suggests that far fewer convenience copies are being created, supporting both good IM practices and SDS's climate change goals. For born-digital records within the SDS M365 tenant, 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	The Assessment Team is grateful for this update on records destruction arrangements. It is evident from this update that SDS has been successful in reducing the need for confidential paper disposal which, as SDS states in its update, is positive in light of both Information Management and environmental sustainability. It is clear that there are still some continuing challenges with the implementation of SharePoint Online (see

	🟩	🟩	🟩	🟩		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.	**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	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 now uses Restore to hold hardcopy records for the medium to long term. When records are destroyed the process is carried out to ISO 9001 (incorporating BS EN15713:2009 and BS7858 standards) and the destruction certificates are retained.	comments under Element 5 above). However, it is also evident that SDS is aware of the main issues posed by the new environment with regard to recoverability of deleted records, whether in the main EDRMs or in one of the authority's line-of-business systems. SDS's continuing use of a third-party storage contractor for the records required for business use medium- to long-term is noted with thanks.

	🟩	🟩	🟩	🟩			undertaken as a public authority pursues its 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	A	G	A	SDS are working on identifying records that may be suitable for long-term preservation and have provided a	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	Thank you for this update. The Keeper fully agreed this element of the SDS RMP in 2014 and no retrograde actions have occurred since	An MOU / Archiving Agreement with the NRS has not yet been finalised, in large part due to other work taking priority over it. Now that the re-validation of the retentions schedule and BCS is well underway and adequately resourced this will be focussed on. Contact has been re-	Thank you for this update. It is clear that work continues to take place in order to formalise the Archiving Agreement with

	🟩	🟨	🟩	🟨	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 once	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.	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 concerns over the controller/process or 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	established with the Client Manager for this and a schedule agreed that should see the initial list of records for permanent preservation agreed by Dec 2022 and the agreement in place early in 2023.	NRS. The Team appreciates this can be a slow process, and commends SDS efforts for continuing to pursue this. The Assessment Team is aware that the rationale of 'no retrograde actions since the Keeper's Agreement' was used in the previous PUR, and the status of this PUR Element retained at Green. However, if this were a formal resubmission, the Keeper would likely 'downgrade' this element to Amber as no formal agreement exists between the authority and the archive provider. The current

	🟩	🟨	🟩	🟨	it is ready to provide evidence that proper arrangements are in place.		permanent preservation by NRS. However, the MoU process could be restarted before/during that selection process.		approach in PUR assessment procedure considers this a minimum standard, so the PUR status has been changed to Amber to reflect this. The Team encourages SDS to continue to prioritise this work, and looks forward to being updated on progress.
8. Information Security	G	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.	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	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.	SDS continues to develop and mature its approach to Cyber Security and has made significant progress in this area, both in technical controls and in the business processes and capabilities needed to respond to and manage an incident. **2021** In 2021 SDS and the partners where all externally assessed and passed the Cyber Essential 'Plus' accreditation. We also expanded the EIS Cyber Security team with the creation of a Security Operation function to enhance monitoring and incident response. **2022**	Thank you for this thorough update on what progress has been made since the submission of the last PUR. By the time this PUR is approved, it is assumed SDS will have obtained its Cyber Essentials Plus recertification. This is not a requirement under PRSA,

	🟩	🟩	🟩	🟩		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.		We are currently working with external assessors on our renewal of Cyber Essential and expect to have Cyber Essentials ‘plus’ by end of September. SDS has also refreshed and updated it ‘IT and System Usage Policy’ to reflect increased use of Cloud services. SDS are now making use of new functionality to control access to Cloud application and have new Data Loss Prevention tools. **2023** As part of a Security Improvement programme, we will be upgrading our Security Operation Centre capability and enhancing our Data Loss Prevention service. An external audit of Cyber Maturity was carried out in 2020. Its recommendations centred on people (roles and responsibilities), processes and also better documentation in line with external cyber security standards (ISO27001). Responding to those led to Cyber Maturity Improvement Project (CMIP) being launched and then implemented over two phases. Phase 1 covered (to Mar 2022): • Operational Support Model) documents produced for the key systems covered (My WoW; App.scot; Agresso Finance/HR);	but indicates commitment to best practice in information security. It is also great to hear of recent focus on monitoring and incident response, as well as the recent IT and Systems Usage Policy review to take into account increased use of Cloud-based information management. Work on access control and data loss prevention is also noted with thanks. Thank you for providing this detailed update on the 2023 Cyber Maturity Improvement Project, stemming from the 2020 external Cyber Maturity Audit. This is a

	🟩	🟩	🟩	🟩		Once that work has been completed SDS 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.		• Data Protection Impact Assessments (DPIAs) undertaken, data risks identified and follow up actions agreed with system owners; • New policies produced (Back Up, Data Resilience & Disaster Recovery/Information Access Control); • Key processes reviewed and improvements identified (leavers process, cyber incident management). • Some collateral benefits also accrued (OSMs/DPIAs done for critical systems not in original scope) Phase 2 (to Mar 2023): • Implementation, testing, exercising and refresh of the improved controls developed in CMIP1 for non-EIS supported systems • Extension of the improved controls and documentation to other SDS critical systems (e.g. IShare, Contact Centre, OSF, Clearview etc) • Developing an outline cyber operating model for SDS across EIS supported and non-EIS supported systems, for implementation as 'business as usual' once CMIP project phase work is completed. In parallel, the Software Governance Group (SGG) was	commendable endeavour, and, alongside other projects described, will undoubtedly solidify SDS's defences against future cyber threats. The 2022 Cyber Security Audit will also assist in keeping SDS on track. The Assessment Team has no concerns over this Element. Update required on any change.

	🟩	🟩	🟩	🟩				established to manage the range of applications and systems in use at SDS. The SGG undertook a detailed self-assessment of effectiveness in early 2022 and identified a number of areas to further strengthen the group’s role and impact. A key recommendation was that the group - renamed as the ‘Digital Assurance Group’ (DAG) - should have governance oversight for SDS’s overall cyber security strategy, operations and performance. Other activities have included work on phishing (raising colleague awareness of the risk, understanding of what to do if they suspect an email is a phishing attack and then testing of that understanding) and reducing risks from use of email have been led by DAG. Both of these will feature in the SDS Cyber Strategy which is due to be published in Oct 2022. Related to this has been work led by DAG on the creation of a master list of business systems in use at SDS, the development of a role description for the business system owner (BSO) for each system and an assessment of how critical each system is to SDS. The master list should be completed in Q3 of the current FY; the Business Continuity team	

								has been working with those known to be in Business Owner roles to assess their system against an agreed framework to determine its criticality. That work will be reviewed by DAG in Q3 to produce a baseline. The role description for the BSOs should be formally approved in the same timeframe. The BC team ran a corporate level cyber incident response scenario session in 2021 (see Element 10), which prompted the purchase and creation of cyber playbooks to help SDS respond to a ransomware attack. The corporate-level playbook is in place as are playbooks for three of the main systems (Aggresso, My World of Work and Apprenticeships.Scot). Playbooks for more of the core systems are planned. These activities will be central to the up-coming external audit of cyber security & maturity, due in Nov 2022.	
9. Data Protection	**G**	**G**	**G**	**G**	Update required on any change.	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	As with all other Scottish public authorities Skills Development Scotland have been required to review and update their data protection procedures in light	The previously established good practice around responding to Data Breaches, managing Subject Access Requests (SARs), assessing risks through Data Protection Impact Assessments (DPIAs) as well as informing colleagues and customers of their rights through Privacy Notices	Thank you for this positive update, and an overview of the DPIA and Privacy Notice review process. That staff training and

	🟩	🟩	🟩	🟩		(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. 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,	of the 2018 legislation. The Assessment Team acknowledges that the public facing SDS website has been updated appropriately: [Privacy | Skills Development Scotland] 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.	continues to be central to how SDS addresses its Data Protection obligations. This good practice also includes appropriate and regularly reviewed staff training and guidance, with all colleagues having to complete mandatory training in Data Protection, Data Breaches and Freedom of Information (FOI), as well as specific training being delivered to particular teams who handle large and/or sensitive datasets The DPIA process retains a strong focus on identifying, assessing and mitigating risks around the processing, sharing, retention and secure storage of personal data. This process is routinely followed for all new business activities (that involve personal information). Privacy Notices are reviewed regularly, with standard practice being reviewing 2 years after creation and annually thereafter. Most are made publicly available on the SDS website's Privacy page. Additionally, SDS's digital services (e.g. apprenticeships.scot) carry the relevant privacy notice on their own sites.	guidance in this area also continues to be regularly reviewed is noted. In conjunction with the steps reported under Element 8, it is clear that SDS understands its responsibilities in the management of information, including adherence to Data Protection and adjacent legislation, and continues to pursue best practice in this area. This Element remains at Green.

	🟩	🟩	🟩	🟩		and further updated training is in discussion for next financial year.	For staff training see element 12 below.		
10. Business Continuity and Vital Records	G	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.	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 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.	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 helped with the 2020 response. For staff training see element 12 below. For review see element 13 below.	As with many public sector organisations since 2020, SDS's main focus for Business Continuity has been on two key areas – COVID-19 response and cyber resilience. Given the vulnerabilities shown by the attack on SEPA, SDS has continued to implement the lessons learned from that incident. Following our last update in March 2021, members of SDS's National Incident Management Team, plus selected senior colleagues from across the business, participated in a 6-part Cyber Incident Management Training course, ran by accredited industry professionals Plan B Consulting, in conjunction with BC Training. As a result of this training, SDS procured a Cyber Incident Playbook, as well as playbooks for key internal systems and a template playbook that could be used internally for other systems. This work was completed by March 2022, with additional internal playbooks for other systems being created throughout 2022. IShare Online, the EDRMS used within SDS, will also have a playbook created for it in 2022.	Thank you for highlighting that SDS's business continuity focus has centred around COVID-19 and cyber resilience. As extensively reported under Element 8, it is clear that SDS has heavily invested in its cyber resilience, including training and guidance. It is also very positive to see that SDS has approached a fellow public authority SEPA to learn from their major incident and to ensure they would be prepared for a similar cyber-attack. The resulting actions (such as ensuring

	🟩	🟩	🟩	🟩		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.		The SDS Board and Audit and Risk Committee members met with the incident manager from SEPA to get further insight into the incident and take some of the key learning points into SDS's approach to Business Continuity. This included such actions as ensuring that the Business Continuity plans and cyber playbooks are not just stored digitally in the business continuity system but are also readily accessible in hardcopy by the BC Team in an SDS office. Processes are being developed to ensure that these convenience hardcopies are kept up to date. As part of the Business Continuity planning process in SDS, each departmental business continuity plan details both the location of all of the dept's vital records and the categories of information held within those vital records. The business continuity plans are stored within the business continuity system, currently Clearview, and are reviewed at least annually; local BC co-ordinators are encouraged to review their BC plan every 6 months and to update it following any major change to their functions or dept. The annual review process for 2022 triggered on the 1st of July, with the majority of departmental plans	guidance is available in hard-copy format and not just digitally) are very welcome. The procedures for the maintenance of SDS's Business Continuity Plans are also noted with thanks. Thank you also for confirming that the second Lessons Learned session on SDS's COVID-19 response has taken place. It is clear that appropriate continuous improvement is taking place in this area, and that SDS continue to be well-placed to meet unexpected events.

	🟩	🟩	🟩	🟩				updated and reapproved by the end of August 2022. As noted in the last Progress Update Review, the COVID-19 incident had provided a severe test of the Business Continuity arrangements in SDS. In order to crystallise the learning points from this, a Lessons Learned session was held in the summer of 2020 focused on the initial phase of response. The Lessons Learned session for the remainder of the COVID-19 Incident is taking place on the 12th of September.	
11. Audit Trail	A	A	A	G	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.	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	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	The biggest change in terms of audit trail for SDS has been the widespread implementation of the Microsoft Teams platform, specifically the file-sharing and collaborative capabilities of this software. This has resulted in the growth of unstructured information being stored in Teams-affiliated SharePoint site, which has become a third main repository alongside IShare (SDS's EDRMS, based on a Sharepoint Online platform) and OneDrive for Business. As Sharepoint sites, the Teams-linked file storage facilities have the same audit trail arrangements as IShare Online, with a version history detailing any changes that were made to the file, when and by whom, as well as a record of	The Assessment Team is grateful for this update on digital records' audit trails which indicates that SDS is acutely aware of the challenges of multiple possible storage locations for records, enabled by the use of MS Teams. This update also indicates, however, that SDS has taken steps to address

	🟧	🟧	🟧	🟩	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.	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	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.	the last 90 days of moves, renames, deletions and edits available via the Details pane in the document library where the files are stored. The features available to the IT department in the Security and Compliance Center are still as described previously, where accurate records of changes, edits and access to files are available. Due to the challenges in having multiple possible avenues for the storing of information, there is a suite of guidance that has been developed by the Records Management Team, in collaboration Office 365 team in SDS's Business Support function, in order to provide help and pointers for staff in terms of what types of information should be stored where – for example, line management files in the manager's OneDrive, long term records in IShare etc.) This, in conjunction with the SDS Document Naming Guidelines and general Records Management advice provided via multiple fora (including a Top Tips OneNote), help encourage correct storage of files. By ensuring that files created by our users are stored in the correct area, with the Version History capabilities and viewable changes via details pane, and the correct naming and file-plan structures, this allows for	this challenge, and that audit trail information continues to be retained. Most significantly, SDS has now developed and implemented staff guidance on save locations and naming conventions, both of which can have a significant positive impact on effective audit trail management. As mentioned in the previous PUR comments, these documents and evidence of their dissemination would be required if this was a formal RMP resubmission; for the PUR process, the Assessment Team is content to upgrade this PUR Element to Green to

	🟧	🟧	🟧	🟩		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.		an easily viewable record of a document's journey. All of SDS's hardcopy records are stored at Restore, 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. As part of the contractual transition from Dataspace Scotland to Restore, the inventory of items stored was reviewed and refreshed. This, in conjunction with the records of accession requests and withdrawal requests made to Restore by SDS, allows the organisation to have a reasonable degree of confidence in knowing where its physical records are stored.	celebrate progress made. That said, the Team reminds SDS that continuous monitoring of adherence to these guidelines should take place to ensure they remain effective. The Team has also noted that SDS continues to use a third-party supplier for the medium-to-long-term storage of hardcopy business records.
12. Competency Framework	G	G	G	G	The Keeper commends efforts by SDS to develop a programme of training through the SDS Academy and to create a Working	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	The Keeper expects staff creating, or otherwise processing records, to be appropriately trained and supported.	The RM Policy sets out SDS's expectations regarding the management of records and it is supported by the Records Management Roles, Responsibilities and Competencies document. This identifies three distinct groups of	Thank you for providing this detailed update on relevant competencies in the practical implementation of the Records Management

	🟩	🟩	🟩	🟩	Group of Records Management Champions. The Keeper would like to hear further news of these endeavours.	competency expectations 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	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.	colleagues with differing responsibilities: • The RM team within IGOR which is responsible for writing policy, process and guidance to help everyone meet the requirements. • Information Asset Owners (IAOs) who ultimately have the responsibility for validating changes to who has access information in their asset and confirming retention schedules; approving file plans and defining what to keep where within their asset; as well making disposition decisions and identifying what might be suitable for permanent preservation. • All colleagues must ensure that they store corporate information in the right place, based on its topic and sensitivity; make sensible use of the version history to capture major changes to content or milestones in the lifecycle; manage that information to the agreed retention periods; share and handle the records appropriately. There are different mechanisms in place to help those groups meet their responsibilities.	plan. SDS has entirely appropriately differentiated between the levels of records management competency required for staff members with different levels of responsibility. It is also clear that SDS continues to ensure these appropriate competencies are being met-through regular and appropriate training provision. Thank you for letting us know that the role of IShare Supers has now been discontinued, and the rationale behind this decision. It sounds like SDS has entirely appropriately considered the role and decided its responsibilities

	🟩	🟩	🟩	🟩		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.	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.	The RM team within IGOR regularly has the opportunity for relevant CPD. In the last year two new members of the team have been enrolled in the RM modules available from PDP; one colleague has successfully concluded the Practitioner Certificate in Scottish Public Sector Records Management; and one colleague has completed 2 advanced SharePoint courses from Leadership Through Data, while another team member is due to undertake LTD's information architecture & M365 course later in the financial year. Additionally, the RM team within IGOR provides on-the-job training for new team members in the in-house processes to support SharePoint users and manage hardcopy records. There is bespoke, in-house training for IAOs that emphasises the RM-relevant aspects of the IAO role by exploring the cost of poor practices in hypothetical scenarios about FOI and DP requests. The team within IGOR also provides support and guidance directly to individual IAOs as and when they request it. Generally, colleagues can make use of a range of procedural guidance on to work within Teams, SharePoint as well as explaining why the guidance is written that way.	would be better realised through the role of IAOs. It is positive to hear that, alongside the Records Management Policy, the Records Management Roles, Responsibilities and Competencies document has now been reviewed and reissued.

	🟩	🟩	🟩	🟩				Awareness of these training opportunities is spread through direct invitation in some cases, through general internal communications channels – weekly updates and Digi? Aye! Newsletters – as well as using Yammer communities and intranet pages. Since the last PUR, the IShare Supers (Records Management Champions as was) role has been retired. This decision was made due to a number of factors such they only rarely had to carry put their role which resulted in an increase in errors; an increase in the size of the central team providing support for colleagues and using the IT ticket system for colleagues to report IShare issues has made it easier for the IShare Support team to take on a heavier workload efficiently. Additionally, some of the other aspects of the IShare Super role – e.g. reviewing retention periods and access permissions – now sit with Information Asset Owners. The Records Management Roles, Responsibilities and Competencies document will be reviewed alongside the RM Policy so that both can be re-issued in Nov-Dec 2022.	

13. Assessment and Review	G	G	G	G	The Keeper welcomes this authority's commitment to regularly review their records management provisions throughout the organisation and audit the 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	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 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	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 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	SDS has a strong commitment to both carrying out the work to deliver on and implement the principles in its Records Management Plan and to periodically review those commitments to ensure that they are still fit for purpose. Corporately, SDS manages its programmes through directorate workplans. Records management work features prominently in the IGOR section of the FIGRR Workplan. The details of which are agreed twice a year between Information Governance Advisor (Element 2) and the Head of Service for IGOR (Element 1). Progress against the actions is reported quarterly and reviewed by the directors. Developing the workplan items involves an informal review of the RMP, and what is needed next. Every 6 months, SDS reports to its Audit and Risk Committee (ARC) on compliance with statutory obligations, including the work done under the RMP and from the PR(S)A (2011). Any policies that are written as part of this work go through extensive scrutiny before being issued in line with SDS's internal policy management and review process.	Thank you for indicating that the RMP review process is managed through Directorate Workplans, and that progress against the Elements is continuing to be measured and reported on a regular basis. As SDS indicates in its update, it is clear that there exists a strong commitment to ensuring the RMP remains fit for purpose and continues to be implemented, and relevant policies are also kept under scrutiny. SDS's regular participation in the PUR process is commended, and the Assessment Team is pleased

	🟩	🟩	🟩	🟩	procedures within their Business Excellence Approach takes place.	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	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.	SDS has committed to participating in the PUR process every two years to provide very useful external expert input to the existing internal processes.	to hear that this is proving a useful tool for SDS.

						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 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.			
14. Shared Information	**G**	**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	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,	The SDS Data Protection Team manages and coordinates the formal sharing of information with external 3rd parties through the establishment of Data Sharing Agreements (DSA) or contracts. Any new or proposed update to a DSA will be reviewed by the SDS Data Protection Team to ensure that Data Protection compliance and good practice is adhered to. Once a new or updated DSA has been approved, any relevant SDS Privacy Notices are reviewed and	The Assessment Team thanks you for this update on how Data Sharing Agreements are continuing to be used, reviewed and managed in SDS. This seems like a reasonable approach to

	🟩	🟩	🟩	🟩		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.	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.	updated if required. A tracker is used to manage the lifecycle of the DSA, which includes the tracking of when each DSA should be reviewed. Where a DSA covers sharing between SDS and multiple partners, such as i) between SDS and the FE and HE colleges or ii) SDS and the Local Authorities, a bespoke tracker is established to be more easily manage the process to have the DSA approved by each organisation and then its lifecycle.	managing shared information.

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

Version

The progress update submission which has been assessed is the one received by the Assessment Team on 28th September 2022. The progress update was submitted by Kenny Parker, Information Governance Advisor, Information Governance & Organisational Resilience (IGOR).

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.

General Comments

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

Iida Saarinen

Iida Saarinen
Public Records Officer