THE NATIONAL ARCHIVES

S46 Practice Study

Information Management Assessment Programme

24.08.2023

Table of Contents

Introduction

Disclaimer

This resource is the output of a study facilitated by TNA. It is a collection of indicative approaches sourced by GKIM practitioners, and is not an official guidance. It is intended to support public record bodies in conducting their assessments and improving their practices, but it is not exhaustive and may not be suitable for all public record bodies.

The revised FOI Act Section 46 Code of Practice (the Code) provides statutory guidance on the keeping, management and destruction of records. The Code is high-level system and format neutral guidance for public sector bodies subject to the FOI Act and/or the Public Records Act. As part of the Information Management Assessment (IMA) toolkit, we have developed the S46 Code Self-Assessment tool (the Self-Assessment) for public sector bodies to assess understanding of their responsibilities and overall compliance with the requirements outlined in Part 2 of the Code: Managing Information and Records.

The Self-Assessment is a diagnostic tool to help public sector bodies measure the strengths and weaknesses of their KIM practices, set improvement targets, and monitor progress.

S46 Practice Study Group

To support the development of the Self-Assessment, a S46 Practice Study Group has been created with participation from Government Knowledge and Information Management (GKIM) practitioners representing various sizes and forms of public sector bodies. The aim of the group was to study the interpretation of the Code's requirements and to identify what 'good' looks like in certain areas. These discussions were captured and summarised in the form of good practice statements.

Good Practices

The good practices published in this document are indicative and based on the conversations and recommendations of participants in the practice study and are not exhaustive. Each example is intended only as a prompt. Different public sector bodies may engage in good practices not captured here and it is valuable to take opportunities to share these with other bodies too. The IMA programme will continue to engage with government to monitor and promote good practice across the sector.

Evidence Types

The Self-Assessment requires participants to identify what evidence types they could provide to support their answers. The evidence type should be available on request for further assessment exercises as part of the IMA programme.

During the Self-Assessment pilot, participating departments defined a wide range of evidence types they could use as proof. The S46 Practice Study analysed these evidence types and synthesised them into a list provided in Annex A of this document.

Use of this resource

Public sector bodies participating in the Self-Assessment are expected to provide examples about their practices and identify evidence types they could use to support their self-evaluated ratings.

Examples in this resource may help point out approaches taken by public sector bodies and benchmark their performance. Without the ability to provide examples of practices and/or point out evidence types it is unlikely that the public sector bodies will meet the requirements.

Summaries of the Code's requirements are listed in the '*Key indicators for an Optimal rating'* box in each section of this document.

Each example, of best practice was recorded in the context of specific questions of the Self-Assessment. You may find that the suggested good practices from one section can be successfully applied in another. The good practice statements are grouped into eleven sections which cover the areas of Part 2 of the Code. Each statement is indexed with an ID corresponding to an assessment question number. The same referencing applies for evidence list in Annex A. Please see the static version of the S46 Self-assessment to look up the corresponding questions.

Monitoring practices

The Self-Assessment will be used by TNA to gather and surface various approaches on 'how' public sector bodies meet with the requirements and what evidence types they can provide to support their answer. Submitted 'other' practices and forms of evidence types will further enrich this resource to support knowledge sharing across the Government Knowledge Information Management community.

Version history

Version number	Publication date	Version changes
1.0	04/07/2023	Original version
1.1	22/08/202324/08/2023	This version • Added Disclaimer to Introduction • Added Version History • Replaced GDPR section and practice statements with Personal Data section

Chapter 1 GOVERNANCE AND CAPABILITIES

Governance

Key indicators for an Optimal rating:

- Having appropriate governance measures and technical capabilities in place to manage information effectively.
- Established information management functions with sufficient seniority within the organisation.
- Maintains a consistent approach to managing information, risk and access.
- Considers the implications for information management during organisational changes, such as restructuring.

Corresponding Assessment Question ID	**Achieve this by:**
5	There is clear responsibility for information and records systems at a senior level.
5	The role of SIRO is held by a senior manager - for example, COO (Chief Operating Officer) - They act at Board level, and the department is aware of their existence and function
5	Document all 'movement' of your information through stages of its lifecycle and use - either in individual instances or by establishing a set of parameters within which your is happy for activity to take place - for example, identifying particular types or locations of information which can be deleted without further examination. These should be accompanied by associated exceptions. Document any destruction decisions, whether ad hoc or systematic - including where certain settings in a platform enable types of users to destroy types of information without further approval.
5	Carry out annual or otherwise *regular* IAO confidence reporting, to help IAOs assess how far staff are following procedures. This contributes to understanding your organisation's compliance maturity by measuring outcomes, and the effectiveness of education and communication.
6, 7	Ensuring that your organisation has written rules on what to keep and when to destroy information to ensure that the organisation maintains a record of its activities.
6	Capture Information Asset Owner approval for destructions.
6	Maintaining formal retention schedules, selection and appraisal policies, and sensitivity review procedures.
6,7	Conduct *regular* reviews of your Retention Schedule - either on a timed basis, or in response to particular changes in STEEP factors that may

Corresponding Assessment Question ID	**Achieve this by:**
	impact your decisions. Ensure the legal bases of your retention schedule is clear.
6,8	Ensuring that your organisation has written rules on access to its information including personal information and other sensitive information.
6,8	Adopt technical controls in systems to avoid inappropriate deletion - for example enabling different levels of system access for different roles in the organisation and using Data Loss Prevention rules to prevent certain activities in some areas of the system. Disposition and how you dispose may be linked to information classification and security clearance of personnel, as well as informing how to destroy information.
6,8	Ensuring relevant policies are published to support transparency, for example: - Publishing Privacy Statement and FOI request process on the public website - Publishing policies relating to user access control and information security
6	Ensuring all colleagues using a system are aware and educated about its capabilities or shortcomings, so that they are clear on what behaviours they need to engage in to achieve good practice themselves.
7	Carrying out *regular* evaluations of the effectiveness of policies and rules throughout your organisation
7	Carrying out *regular* assessments of how well policies and rules are followed by your organisation's staff.
7	Engaging with colleagues to ensure they are familiar with relevant guidance on permanent destruction of information. Approaches to achieving this may include a combination of - tracking traffic in and out of certain key documents or web pages - understanding how those pages are accessed to make it as easy as possible to find them - surveying colleagues to understand their experience and knowledge gaps having used the guidance - reporting on behavioural activity following publication to measure impact of the guidance.
8	Ensuring that your organisation has written rules on access to its information including personal information and other sensitive information. Publishing clear rules and guidance on managing information in accordance with security classification.
7,8	Requiring appropriate security clearance for all staff.
8	Publishing clear rules and guidance on managing information in accordance with security classification.
8	Ensuring that guidance is available on internal web pages, that bespoke advice is available on request via information access team, and that colleagues are aware of how to get access to both.

Corresponding Assessment Question ID	**Achieve this by:**
9	Ensuring that your organisation has a governance or assurance framework that takes account of information risks - for example, inappropriate hoarding and loss of information - and provides for the involvement of senior management
9,10	Record value measures against individual information assets in your asset registers to identify a critical and/or high-value data asset list. You may find it helpful to assign a numerical score derived from risk to and vulnerability of assets, multiplied by the value score to focus attention on a smaller group of the overall assets.
9	DRO/KIM representation on governance boards surrounding major organisational change; Make sure that: - KIM interests are reflected in the considerations of the relevant boards - you have contingency plans for if you aren't consulted, e.g., emergency organisational mergers - consider people moves alongside structural change.
10	Considering the implications of information management during restructuring and other organisational changes, sponsorship of other bodies, and the procurement of services from contractors.
10	Ensuring that contingency plans include sections on minimising service disruption and amending ownership of information during major organisational change, and are approved at the appropriate board level, and reviewed *regularly*. It may be helpful to design this in collaboration with fellow KIM teams in other organisations. This includes readiness plans for Machinery of Government changes.

Organisational Capabilities

Key indicators for an Optimal rating:

- Information management function established with designated manager with day-to-day responsibility for information management.
- Designated manager of sufficient seniority in place to ensure that the authority discharges its responsibilities under the Code, and that the authority is consistent in its approach to managing information, risk, and access.
- Staff is suitably trained to have appropriate information management skills.
- The designated information manager is part of the authority's governance structure and has oversight of information risk;
- Those taking decisions to destroy information on its behalf are authorised to do so by the authority.

Corresponding Assessment Question ID	**Achieve this by:**
12,17	Ensuring that your organisation have an information management function with a designated manager with day-to-day responsibility for information management and responsibility for decisions on access to information.
12	When entering a collaborative relationship, be clear on ownership, documented in an MOU (Memorandum of Understanding), from the outset
13	Ensuring that resources needed to comply with the Code and other statutory obligations are in place.
13	Ensuring awareness of the existence and purpose of the KIM team across the organisation.
14,15	Ensuring that your organisation has staff trained with information management skills.
14,15,16	Complete short, manageable pilots of work you believe needs to be undertaken to establish how much is possible with your current people and resources - the results can form the basis of a business case or risk escalation. Be clear that this is not the same as completing that activity, so that it is clear that the people and resources you have currently would not be sufficient to do so, and why that is.
14,15,16	*Regularly* survey and evaluate staff to ensure you understand their training needs and professional ambitions, and help to manage their development - informally, this may extend to colleagues in other areas of the organisation who are keen to learn new and transferable skills. *The level of skills and expertise needed, and the number of individuals across the organisation will depend upon your organisation's structure, complexity, implementations, and any other unique elements.*

Corresponding Assessment Question ID	**Achieve this by:**
13,14,15	*Regularly* update the risk register and establish risk appetite. The work you commit to as a team should correspond to that level of risk appetite, and you can assess whether you have sufficient people and resources to do that work.
14,15,16	Most organisations will feel they could use more people and resources to achieve better outcomes and recognise that successfully bidding for those is not realistic. Take a bronze, silver, gold approach or similar to categorising work, to identify what is good enough for now, aspirations for the future approach to answering resources questions. For example, identifying if you have enough to do the highest priority work, for now, as agreed within your organisation, having taken a risk-based approach to advocating for the most critical activities.
14,15,16	Be as clear as you can on the high level outcomes you are seeking, and identify where activities are already underway elsewhere in the organisation that may contribute towards achieving those same outcomes - for example, behavioural change activities and training led by HR, or system development and implementation projects led by ICT Delivery Managers - you may be able to nudge closer to the desired outcomes with little input, rather than initiatives of your own.
14,16	Ensuring you have resources and technical capability to enable compliance monitoring.
15,12	Maintain professional skills through training and other continuous professional development.
16	Ensuring that the designated manager [or equivalent] is part of your organisation's governance structure and has oversight of information risk and the ability to raise concerns at the most senior level.
17	Ensuring risk is reportable upwards through the relevant management structure.
17	Record value measures against individual information assets in your asset registers to identify a critical and/or high-value data asset list. You may find it helpful to assign a numerical score derived from risk to and vulnerability of assets, multiplied by the value score to focus attention on a smaller group of the overall assets.
17	Day to day access to registered files is restricted to a specialist team who can grant access to physical or electronic files on a case-by-case basis.
18,16	DRO or equivalent authorises destruction of key corporate records following appraisal by trained staff.
18,16	Ensuring that your organisation make sure that those taking decisions to destroy information on its behalf are authorised to do so.
18	Ensuring that the designated manager has all the resources they need to monitor compliance with the Code and other relevant statutory obligations - in a way that is meaningful and risk aware in your organisation.

KIM Influence

Key indicators for an Optimal rating:

The authority engages with the designated information manager to make sure that their information is managed in conformity with the Code:

- before taking decisions about the design, development, and procurement of IT (Information Technology) systems and applications;
- before the publication scheme is submitted to the ICO;
- before the use and re-use of information;
- before entering cooperative arrangements with other authorities, sponsoring other bodies, acquiring systems originating in another body.

Corresponding Assessment Question ID	**Achieve this by:**
20a	Engaging with the designated manager to ensure that information is managed in conformity with the code before the publication scheme required by section 19 (3) FOIA is submitted to the ICO for approval.
20a	Review should be an ongoing and collaborative process from the outset, not just a one-off at the end before submission.
20a	Publication scheme is signed off by a senior manager, and/or scrutinised by a specialist board.
20a	Making sure that IM/RM principles are embedded in processes - e.g., Privacy by Design - so even if a specific KIM lead isn't on a decision-making board, key KIM considerations are still made.
20a	Ensure that specific training is provided to the relevant people, targeted towards colleagues based on their RACI status.
20a	Clearly and easily available publication scheme both internally and externally.
20a	Address this by having clearly defined roles set up in the organisation/who does what/decision making Tree, including the role of the designated manager. That way relevant individuals in the organisation know who to go to.
20b	Engaging with the designated manager when making decisions about the design, development and procurement of IT systems and applications.
20b	Quality assurance checks
20b	Clear roles and responsibilities.
20b	Address in processes and documentation where information is subject to specific configuration control.

Corresponding Assessment Question ID	**Achieve this by:**
20b	Address copyright explicitly in Data Sharing Agreements.
20b	Achieve this by maintaining continuous review documentation - including contracts, suppliers, and audits.
20c	Engaging with the designated manager to ensure that information is managed in conformity with the code before making organisational changes.
20c	Scheme of delegation, clear decision-making framework
20c	DRO/KIM representation on governance boards surrounding major organisational change; Make sure that: - KIM interests are reflected in the considerations of the relevant boards - you have contingency plans for if you aren't consulted, e.g., emergency organisational mergers - consider people moves alongside structural change.
20c	Achieve this by ensuring that contingency plans include sections on minimising service disruption and amending ownership of information during major organisational change, and are approved at the appropriate board level, and reviewed *regularly*.
20d,20b	Engaging with the designated manager to ensure that information is managed in conformity with the code before the use and re-use of information, including copyright and Crown copyright material.
20d	Address this in training aimed at contract managers, targeting risk management through the life of the contract.
20d	Address this in procurement policies, commercial templates etc.
20d	New supplier forms, 12-month supplier forms, continuous review, risk registers.
20d	Achieve this by establishing the relationship between DRO/KIM and Commercial teams in your organisation.
20e	Engaging with the designated manager to ensure that information is managed in conformity with the code before entering cooperative arrangements with other authorities, sponsoring other bodies, acquiring systems originating in another body and before procuring services from contractors.
20e	Achieve this by building and maintaining strong relationships between DRO/KIM and IT teams, project teams and product owners in operations teams. Take the opportunity in, for example, CAB (Customer Advisory Board) meetings to buy in to other colleagues' work, collaborating with or through project managers, and inputting to risk registers.

Technical Capability

Key indicators for an Optimal rating:

- Tools and systems in place to manage and organize information throughout its lifecycle.
- Tools and systems in place to locate and use information, consistently applied across the authority.
- Backup systems in place to recover from system failures and major disasters.
- Systems in place to ensure that the destruction of information is carried out in line with its sensitivity and is permanent.

Corresponding Assessment Question ID	**Achieve this by:**
22a,22d	Ensuring that systems are in place that can carry out the destruction of information in-line with its sensitivity and is permanent.
22a	Providing guidance on secure destruction of records across different formats, as well as guidance and processes that are suitable for the type of information, considering any sensitivities.
22a	Conducting disposition reviews, with appropriate checks and balances built into any automated destruction processes to ensure their accuracy. These should be built directly based on retention policies, with compliance checks afterwards to check they are applied appropriately.
22a	Ensuring all colleagues using a system are aware and educated about its capabilities or shortcomings, so that they are clear on what behaviours they need to engage in to achieve good practice themselves.
22a	Ensuring your record-bearing systems have automated destruction built-in, or, if not, that you have established an approach to achieving the same outcome via other means.
22a	Using a template for technical capability procurement which includes this as a requirement (where needed) prior to approval for purchase / implementation
22a	Electronic data within IT systems is deleted as per business requirements / policy.
22a	Be able to report on deletions and provide evidence of what has been deleted and why. Approaches to doing this may include technical system reports, disposition review logs, or simply retention schedules which describe the normal parameters for compliant deletion.
22a	Engage and collaborate with ICT colleagues or other system administrators to ensure the appropriate type of full destruction is taking place, taking consideration of any temporary backup which may continue to hold the data.

Corresponding Assessment Question ID	**Achieve this by:**
	This also includes consistent classification and interoperability between systems - for example, linking front end databases with backend repositories, to ensure that documents held as part of a case record are not retained or disassociated from the record when it is deleted from the front-end database.
22a	Ensuring that back-up systems are in place to recover from system failures and major disasters, and that the relevant information is deleted from these at the appropriate time, as well as from the live system.
22a,22b 22c,22d	Consider how your organisation needs to handle portable media, tracking, allocation, acceptable use, obsolescence, audit, and transfer of content.
22a	Tracking, management, monitoring and audit of portable media, to ensure it is used appropriately (only in specific scenarios) and the information stored on it can be deleted as appropriate.
22a	Engaging with colleagues to ensure they are familiar with relevant guidance on permanent destruction of information. Approaches to achieving this may include a combination of - tracking traffic in and out of certain key documents or web pages - understanding how those pages are accessed to make it as easy as possible to find them - surveying colleagues to understand their experience and knowledge gaps having used the guidance - reporting on behavioural activity following publication to measure impact of the guidance.
22b	Ensuring that tools and systems to locate and use information are consistently applied across the authority.
22b	Providing guidance on how to manage information to ensure it is findable.
22b	Address this in technical capability procurement arrangements as being a requirement of any system storing information.
22b	Ensuring that system configuration considers MSCW rated metadata fields, and version control.
22b,22d	Ensuring that tools and systems to locate and use information are consistently applied across the authority, for example mandatory metadata tags to improve findability
22b	Having a data dictionary and data glossary, which also supports interoperability between systems to improve data-driven decision making via federated search.
22b	Take steps to ensure all related content is discoverable consistently regardless of medium - for example, digitizing and indexing physical records and enabling aggregate/federated search so that they can be discovered at the same time as digital records, or ensuring processes which are well communicated to all colleagues.

Corresponding Assessment Question ID	**Achieve this by:**
22b,22c	Make efforts on behalf of your organisation to remain aware of emerging technologies such as machine learning that might help with or otherwise impact the way you manage content.
22b,22c	Staying on top of system updates, contract ownership, and support arrangements, to ensure that critical systems and their contents remain available and complete.
22b	Managing encryption keys so that content does not become inaccessible.
22b	Ensure consistent naming conventions - report on inconsistencies and offer advice, guidance, and audit of content (findability).
22c	Ensuring that tools and systems to manage and organise information throughout its life.
22c	Ensure IAOs are aware of their vital records, their location, and current risk level.
22c	Ensuring you know how Records Management can be achieved across the life cycle in bespoke systems, as well as COTS procured products. That may be by having the capability built into the system or, if not, identifying how the same set of outcomes might be achieved otherwise, in accordance with your organisation's risk appetite.
22c	Maintain an Applications Register, and where applicable link it to your organisation's Contracts Register, Asset Registers etc. This will help ensure any apps you build follow consistent playbooks and are manageable, and that support, maintenance, or customisation arrangements for procured apps are clear and accurate. Safeguard support for key record-bearing systems and complex access databases but ensure levels of maintenance are proportionate based on risk and value, so that you do not exhaust resources on low value assets.
22c	Migration planning at point of procurement.
22c	Provide department wide training on guidance on organising and managing information based on a life-cycle model.
22c	Seek approval for new solutions to deal with legacy data heaps through senior governance boards.
22c.22d	Prevent storage of new information in legacy locations - this both reduces the scale of the backlog in the event of an incident, and the risk that new information is being stored in unsupported or otherwise at-risk locations.
22d,22a	Ensuring that back-up systems are in place to recover from system failures and major disasters.
22d	Follow advice from NCSC (National Cyber Security Centre), for example Cloud security principles, and ensure systems are backed up securely.

Corresponding Assessment Question ID	**Achieve this by:**
22d	Consider apps and systems in disaster recovery plans and be aware of how your content is backed up if you use cloud hosted technologies so you can assess any risks related to the approach.
22d	Identify critical records in your asset registers and include a value assessment of some kind for all assets, based on criticality and risk to the asset, so that you are clear which are the highest priority in the event of an incident.
22d	Achieve this by documenting processes for recovering information in case of a system failure or disaster and ensuring that contingency plans are approved at the appropriate board level and reviewed *regularly*.
22d	Seek approval for new solutions to deal with legacy data heaps through senior governance boards - the less outdated data your organisations hold, the smaller the task of identifying what needs to be recovered in the event of an incident.

Chapter 2 KEEPING, FINDING AND USING INFORMATION

Keeping Information

Key indicators for an Optimal rating:

- Defined how long to keep information.
- Disposal of information is carried out when it is no longer required.
- Can explain why information is no longer held either by reference to a record of its destruction or by reference to the authority's policy.
- The value of information is assessed on a regular basis and understood.

Corresponding Assessment Question ID	**Achieve this by:**
24	Ensuring that your organisation has defined how long to keep information.
25	Ensuring that your organisation can explain why information is no longer held.
25	Record a business justification and IAO (Information Asset Owner) approvals before destroying information.
26	Assessing information to identify its value.
26	Information Management Policy in place which contains retention schedules.
26	Record value measures against individual information assets in your asset registers to identify a critical and/or high-value data asset list. You may find it helpful to assign a numerical score derived from risk to and vulnerability of assets, multiplied by the value score to focus attention on a smaller group of the overall assets.
26	Engaging with colleagues to ensure they are familiar with relevant guidance on permanent destruction of information. Approaches to achieving this may include a combination of - tracking traffic in and out of certain key documents or web pages - understanding how those pages are accessed to make it as easy as possible to find them - surveying colleagues to understand their experience and knowledge gaps having used the guidance - reporting on behavioural activity following publication to measure impact of the guidance.
26	Utilise Features such as email - e-discovery, keywords search, free text search of OCRd content, aggregate search across datasets, records review status and Data Protection features.

Corresponding Assessment Question ID	**Achieve this by:**
26	Within your organisation, agree a definition of regular that works for you, and is compatible with your risk appetite. This may be timebound, or respond to various trigger events, like a change in legislation. Decide an approach that works in response: should assets always be assessed to ascertain its value? Could the information asset register record the asset's value, e.g., based on changing business need? Clearly identify what it is needed on a legal basis, and where exceptions to deletion should be enacted. Include processes to identify records required for permanent preservation.

Metadata

Key indicators for an Optimal rating:

- Collects and retains technical and contextual information about their records to understand their value.
- Metadata kept in a reliable and accessible way for as long as it is required, which will be at least for the life of the records.
- Ability to transfer technical and contextual information to a successor body or archive if selected for permanent preservation.

Corresponding Assessment Question ID	**Achieve this by:**
28a,28b	Ensuring the organisation can transfer technical and contextual information to a successor body or, if selected for permanent preservation, to an archive.
28a	Collecting and keeping all technical information about records in to help you understand their value.
28b	Ensuring consistent application of naming conventions.
28d	Maintaining a dialogue with anybody you are transferring to, not just at the point of transfer, to clarify precisely what is needed at the point of transfer.
28a,28b	Being clear within your organisations on the rationale for why any given metadata element is important - for example: - Compliance checks - Testing and procurement - Migration planning - Establishing UAT criteria - Use of corporate tools and systems in compliance with policy and external standards As well as being clear on these benefits, also understanding how your organisation specifically implements practices that meet its policies, in response to STEEP obligations and changes - the example in this case is knowing what metadata is necessary, why it is necessary, and how it can be preserved/migrated.

Environment

Key indicators for an Optimal rating:

- Holds its information in a suitable environment and manages physical and digital information appropriately to preserve its value.
- Takes action to conserve physical records if there are signs of damage, and digital information is subject to active digital continuity.
- Makes reasonable efforts to recover or preserve damaged or unusable physical records and digital information, including their technical and contextual information, while keeping a record of any actions taken.
- Have suitable tools to identify, locate, and retrieve information as required, while maintaining effective search capabilities and controls to protect sensitive information.

Corresponding Assessment Question ID	**Achieve this by:**
30b	Policy and processes are in place for getting records back, and tests of the process for restoring content have been completed by infrastructure.
30c	Organisation can take action to conserve physical records if there are signs of damage.
30d	Ensuring your organisation makes reasonable efforts to recover contextual information for 'orphaned information' in which they judge to have value, keeping a record of any action taken.
30d	Ensuring your organisation has the appropriate tools to identify, locate and retrieve information when required. If so, does this search capability maintain controls alongside the need to protect sensitive information

Trusting Information

Key indicators for an Optimal rating:

- The organisation has ability to establish when and by whom information was created.
- Policies and processes for information security in place and comply with relevant legislation, guidance, and codes of practice.
- Access and permission controls are applied throughout the life of the information to prevent unauthorized access.
- Technical and organisational measures are in place to prevent accidental loss, destruction, or damage to information.

Corresponding Assessment Question ID	**Achieve this by:**
32a,32c	Ensuring that your organisation can establish when information was created
32a	If receiving information from another body, ensure you have a comprehensive checklist of data elements you will receive, so that there is a process in place which is agreed by both parties ahead of transfer.
32a	Establish scenario-driven approaches to transferring, migrating, and receiving information in bulk, to include for example questions relating to the completeness of the associated metadata. This helps to ensure that the information remains as complete and available/accessible as possible over its lifespan.
32a	Ensure processes are in place to encourage transfer of records from ephemeral repositories to shared volumes - e.g. My Drive to Shared Drive, OneDrive to SharePoint. *(System and collection specific IMA (Information Management Assessment) Modules may make suggestions on how to approach these practically.)*
32b,32c	Ensuring that your organisation can establish who information was created by.

Corresponding Assessment Question ID	**Achieve this by:**
32a,32b	Being clear within your organisations on the rationale for why any given metadata element is important - for example: - Compliance checks - Testing and procurement - Migration planning - Establishing UAT criteria - Use of corporate tools and systems in compliance with policy and external standards As well as being clear on these benefits, also understanding how your organisation specifically implements practices that meet its policies, in response to STEEP obligations and changes - the example in this case is knowing what metadata is necessary, why it is necessary, and how it can be preserved/migrated.
32c	Ensuring that your organisation can apply access and permission controls throughout the life of the information held in to prevent unauthorised or unlawful access.
32d,32c	Ensuring that your organisation has technical and organisational measures to prevent accidental loss, destruction, or damage, to information held in
32d	Ensuring that contingency plans include relevant sections on accidental loss, destruction, or damage to information, and are approved at the appropriate board level, and reviewed *regularly*. It may be helpful to design this in collaboration with fellow KIM (Knowledge & Information Management) teams in other organisations.
32b,32d	Ensuring systems are backed up to databases on a *regular* basis.
32d	Publishing relevant policies.
33	Ensure policies and processes in place for information security that comply with relevant legislation, guidance, and codes of practice. Examples of approaches may include: - Conducting audits against policies. - Conducting interviews with IAOs, and surveying KIM staff survey. - Consulting with external colleagues. - Continuously reviewing your own actions, Mission-critical Objectives and Key Results. - Reviewing efficiency and purpose of approaches.
33,32d	Record value measures against individual information assets in your asset registers to identify a critical and/or high-value data asset list. You may find it helpful to assign a numerical score derived from risk to and vulnerability of assets, multiplied by the value score to focus attention on a smaller group of the overall assets.

Corresponding Assessment Question ID	**Achieve this by:**
33	Using tools and systems that enable your organisation to search the information and identify relevancy.

Personal Data

Personal data was outside the scope of this study and no good practice statements are provided in this document. However, guidance issued by the ICO should be followed on personal data management and GDPR in relation to current business information. Personal data in historical records is covered in Part 3 of the Code, and TNA provides relevant guidance to follow.

Key indicators for an Optimal rating:

Compliant with:

- UK GDPR requirements by destroying personal data when it's no longer needed, except for specific purposes.
- TNA Data Protection and Personal Information guidance and TNA's records collection policy where it relates to personal data in records to be transferred to The National Archives or a place of deposit in accordance with the Public Records Act.

Chapter 3 DISPOSITION AND DESTROYING INFORMATION

Disposition

Key indicators for an Optimal rating:

- Have procedures to decide how to dispose of information that is no longer valuable.
- Disposition decisions are made in line with their policy and the security classification of the information.
- Records of disposition decisions kept and ensures that those taking disposition decisions are properly authorised to do so.

Corresponding Assessment Question ID	**Achieve this by:**
37	Ensuring that your organisation has procedures to decide how to dispose (destroy or transfer to another body/archive) of information that no longer has value.
37	Ensuring disposal in your organisation is signed off by Senior Management, following risk assessment, benchmarking against other organisations, and appropriate consultation internally and externally.
38	Ensuring that your organisation's disposition decisions are in line with the organisation's policy and the security classification of the information.
38	Ensure you can present evidence of Risk assessment on how to carry out destruction, and level of destruction certificate or confirmation needed.
39	Ensuring that your organisation's disposition decisions are recorded.
39	While a retention schedule indicates intent, it does not in itself record actual disposition. It is a useful means of demonstrating what should have happened, but destruction certificates, and associated risk assessments considering whether to keep records for longer than recorded retention periods, show clearer proof.
40	Ensuring that those who take disposition decisions in your organisation are authorised to do so.
40	Address this by ensuring all colleagues using a system are aware and educated about its capabilities or shortcomings, so that they are clear on what behaviours they need to engage in to achieve good practice themselves.

Destroying Information

Key indicators for an Optimal rating:

- Destroys or deletes information that no longer has value.
- Considers the current and potential future value of the information in destruction decisions.
- Makes destruction decisions in accordance with an up-to-date policy that is applied consistently and approved by the authority.
- Has flexible destruction policies that can be adapted to extraordinary circumstances.
- Ensures that staff are aware of the need to destroy ephemeral material on a routine basis.
- Maintains a destruction schedule to identify and destroy information not needed according to the policy.
- Understands that responsibility for decisions to destroy information will remain with the authority in case of authorisation of staff or contractors to destroy information.
- Able to explain why information is no longer held.
- Obtains proof of destruction, such as a certificate, when carried out by a contractor.
- Destroys information using a method appropriate to its sensitivity or security classification.
- Ensures that destruction/deletion is permanent.

Corresponding Assessment Question ID	**Achieve this by:**
42a	Ensuring that destruction decisions consider the current and potential future value of information.
42a,42b,42d	Ensure an exceptions process is in place to meet business or legal needs to retain information for longer than the stated period in the Retention Schedule.
42a	Record value measures against individual information assets in your asset registers to identify a critical and/or high-value data asset list. You may find it helpful to assign a numerical score derived from risk to and vulnerability of assets, multiplied by the value score to focus attention on a smaller group of the overall assets.
42a,42d	Clearly communicate embargoes to minimise the chances of inappropriate deletion, and so that anything that is deleted inappropriately is clearly identifiable as an issue.

Corresponding Assessment Question ID	**Achieve this by:**
42b	Ensuring that destruction decisions in your organisation are carried out in accordance with an up-to-date policy.
42b	Engaging with colleagues to ensure they are familiar with relevant guidance on permanent destruction of information. Approaches to achieving this may include a combination of - tracking traffic in and out of certain key documents or web pages - understanding how those pages are accessed to make it as easy as possible to find them - surveying colleagues to understand their experience and knowledge gaps having used the guidance - reporting on activity following publication to measure impact of the guidance.
42b,42c,42d	Ensure destruction decisions are approved and recorded by the relevant IAO.
42c	Ensuring that that destruction decisions are carried out using a method or process that is applied consistently and that has been approved by the organisation.
42c	*Regularly* review the destruction process to ensure it remains relevant and fit for purpose.
42c, 46	Identify types of information which can be subject to bulk or regular deletions.
42c,46,47,48	Establish rules which give empowered users clear parameters to operate within, so that you do not become overwhelmed with requests to delete. In some scenarios, they can do it themselves. Make sure everyone who is authorised to do it understands what their responsibilities are and how to do it appropriately and successfully.
42c,48	Seek approval for new solutions to deal with legacy data heaps through senior governance boards.
42d	Ensuring that destruction policies are flexible to adapt to the requirements of extraordinary circumstances such as litigation or a public inquiry.
42d	Ensure that destruction reports identify information that is relevant to an ongoing inquiry, so that it can be exempted.
46	Ensuring that staff are aware that there is no need to keep ephemeral material, and that this may be destroyed on a routine basis.
46,47,48	Conduct compliance checks, for example using keyword search, and information assurance reports. Ensure that colleagues understand what ephemeral material is, based on their responses to staff survey, formal enquiries sent to the KIM team, general engagement and observed in system and at desk.
46,47	Conduct compliance checks to understand how discouraged colleagues are from keeping duplicates and ephemeral content. How this works will

Corresponding Assessment Question ID	**Achieve this by:**
	depend on your infrastructure. You might be able to report on levels of content in mailboxes, local shared drives, desktops etc. For example, you may monitor OneDrive account sizes before and after a change campaign to see if there has been a reduction.
46	Automate retention in specific applications wherever possible - for example, Instant Messaging - to reduce the burden on colleagues at desk.
46	Communicate the most appropriate ways of reviewing information to all colleagues.
47	Ensuring that staff are encouraged to delete trivial emails and messages after they have been read.
47	Address this in comms campaigns on reviewing information.
47	Use automated email retention rules meaning staff must actively save information that needs to be kept.
47,48	Run communications and education campaigns on reviewing information.
48	Ensuring staff are discouraged from keeping multiple or personal copies of documents.
48	Ensuring staff are storing corporate information in shared areas and not personal drives.
48	Prevent storage of new information in legacy locations and minimise/limit storage capability in locations identified as ephemeral.
49	Ensuring that your organisation has a destruction schedule to enable identifying and destroying information that is not needed at the appropriate time, as determined by the organisation's policy.
49	Conduct regular reviews of your Retention Schedule - either on a timed basis, or in response to changes in STEEP factors that may impact your decisions. Ensure the legal bases of your retention schedule is clear.
50	Ensuring that staff or contractors are authorised to destroy information, are you are aware that the organisation will remain responsible for decisions to destroy information and for ensuring that they are carried out.
51	Ensuring that your organisation can explain why information is no longer held, either by reference to a record of its destruction or by reference to the organisation's policy.
52,42c	Ensuring that if destruction is carried out by contractors, your organisation has obtained proof of destruction.
53	Ensuring that information is destroyed by a method appropriate to the sensitivity or security classification of the information.
53	Adopt technical controls in systems to avoid inappropriate deletion - for example enabling different levels of system access for different roles in the organisation and using Data Loss Prevention rules to prevent certain activities in some areas of the system. Disposition and how you dispose

Corresponding Assessment Question ID	**Achieve this by:**
	may be linked to information classification and security clearance of personnel, as well as informing how to destroy information.
54	Ensuring that information is destroyed in proportion to its sensitivity and security classification.
55	Ensuring that destruction/deletion is permanent.

Chapter 4 RESPONSIBILITIES WHERE INFORMATION IS SHARED

Key indicators for an Optimal rating:

- Data sharing agreements in place when working with other organisations.
- Agreements cover data protection legislation, and FOIA obligations
- Record management controls, personal data protection and information security requirements specified
- Copyright ownership addressed
- Compliance with relevant legislation ensured.

Corresponding Assessment Question ID	**Achieve this by:**
57	Ensuring that when working jointly with another organisation (authority, body, contractor, a lead or commissioning authority), your organisation has a data sharing agreement in place which sets out responsibilities that ensure information is managed in accordance with the Code throughout its life.
57,58a	Continuous regular monitoring of active contracts, by designated contract managers, managed via contracts register, being careful not to overwhelm individual managers with too many contracts.
57	Making sure information is destroyed or returned at the end of the contract.
58a	Data sharing template agreement with copyright template, copyright disclaimer on website; Copyright Policy.
58a	Ensuring your organisation's data sharing agreement specifies the ownership of any copyright.
58b	Ensuring your organisation's data sharing agreement specifies the obligation to record decisions, particularly in relation to the transfer or destruction of information.
58b	Address this in Commercial branch policy.
58b	Embed the requirement into guidance for creating commercial arrangements which involve data sharing.
58c	Ensuring your organisation's data sharing agreement specifies obligations under copyright, data protection legislation and FOIA.
58d	Ensuring your organisation's data sharing agreement specifies record management controls and any special requirements for the security and handling of personal information.
59	Ensuring that information sharing arrangements enable compliance with the requirements of the PRA or the PRA(NI) where at least one authority is subject to the legislation.

Corresponding Assessment Question ID	**Achieve this by:**
59	Data sharing template accounting for PRA obligations, overarching board for sign off, continuous review, lessons learned. Central log of information sharing agreements.

Chapter 5 MONITORING AND ASSURANCE

Key indicators for an Optimal rating:

- Regularly assess policies and procedures against Code requirements
- Update policies and procedures if necessary
- Include non-compliance risks in the authority's risk management framework
- Engage with information management assurance and audit regimes in their field.

Corresponding Assessment Question ID	**Achieve this by:**
61	Ensuring that your organisation assesses its policies and procedures against the requirements of the Code at regular intervals and updates them if necessary.
61	Record value measures against individual information assets in your asset registers to identify a critical and/or high-value data asset list. You may find it helpful to assign a numerical score derived from risk to and vulnerability of assets, multiplied by the value score to focus attention on a smaller group of the overall assets.
61	Maintain a link between the policy and the risk register - this helps prioritise. Safeguard support for key record-bearing systems and complex access databases but ensure levels of maintenance are proportionate based on risk and value, so that you do not exhaust resources on low value assets.
61	Within your organisation, agree a definition of regular that works for you, and is compatible with your risk appetite. This may be timebound, or respond to various trigger events, like a change in legislation. Decide an approach that works in response: should assets always be assessed to ascertain its value? Could the information asset register record the asset's value, e.g., based on changing business need? Clearly identify what it is needed on a legal basis, and where exceptions to deletion should be enacted. Include processes to identify records required for permanent preservation. Engage with the internal audit function in your organisation to assist.
61	Ensure you have controls in place to manage sharing of information outside of your organisation. This goes beyond data sharing agreements and policies - It may include use of Data Loss Prevention tools to prevent or monitor activities in certain areas of your systems or affording different roles different levels of access across the system.
61	Ensure that what you are asking end users to manage at desk is proportionate to their role - this helps to manage any concern that the activity or outcome it aims to achieve are beyond the resources of the organisation, or disruptive to operational functions. Be clear on whether

Corresponding Assessment Question ID	**Achieve this by:**
	these approaches are permanent, or temporary in lieu of greater automation or similar technical solutions.
61	Proactive checking/make the public aware of any changes if the policy is published online.
62	Ensuring that risks associated with non-compliance are included in your organisations' framework for managing risk.
62	Regularly update the risk register and establish risk appetite. The work you commit to as a team should correspond to that level of risk appetite, and you can assess whether you have sufficient people and resources to do that work.
62	Ensuring that your organisation engages proactively with information management assurance and audit regimes (For example, tools, external assessments, peer reviews and accreditation schemes).
62	Being aware enough of your internal policies and technical capabilities to understand the extent to which you depend on the end user to achieve compliance and working with them to make it as easy as possible for them to achieve successfully.
63	Ensuring that your organisation has a governance or assurance framework that takes account of information risks - for example, inappropriate hoarding and loss of information - and provides for the involvement of senior management.
64	Promoting awareness in your organisation that under FOIA, the Information Commissioner may, with the consent of any public sector body, assess if that authority is following good practice.

Chapter 6 Annex A - Evidence Types

Active monitoring and reporting	42a
Advice from a relevant specialist team	40,58a,b,c,d
Annual or regular reviews - policy, procedure, practice etc.	7,42b,62,63
Annual reports, assessments, and assurance statements	7,61,62,18
Applications Register	22d
Business Continuity Plans	20a,22a,c,d,32a,d
Change control data	25,51,61,33
Classification Scheme and File Plan	10
Code of conduct	18
Contingency planning	55
Contracts and relevant clauses	10,18,20a,32a,42c,50,53,57
Data Asset Register, or equivalent	22d
Destruction certificates and logs	6,18,25,35,37,38,39,40,42a, 51,52,53,55
Destruction or disposition approval, decision, and declaration documentation	18,22d,24,39,40,42a, 42C,52,53
Disposal and/or destruction schedules	6,22d,24,37,39,40, 42a,53
Disposition stubs or equivalent	24,37,39,42a,51
Documentation provided to or deriving from boards - e.g., recommendations to the board, decisions, and minutes from them	5,6,7,35,37
Due diligence forms	18,20a
Examples of engagement with or via specialist groups externally	7
Examples of Privacy by Design	20d,35
Examples of responses to an active inquiry, for example the COVID Inquiry	42d
Examples of well-embedded information management communications	30,32a,47
Governance reports	5,18
Governance structure and scheme of delegation	5,9,12,13,14,15,17,18,20a,c, 32c,33,38,39,40,42d,62
Information and data sharing agreements/registers	57,58a,b,c,d,59
Information Asset Ownership model, policies, processes etc.	5,7,9,12,14,15,17,22c,36, 37,40,62
Information Asset Register	8,9,12,17,22a,c,36

Keep categories or similar retention exception rules	6,24,25,35,37,42a
Meeting minutes	17
Memoranda of Understanding, including templates and guidance	20a,32a,50,57
Organogram	5,12,13,14,15,16,17,18
Ownership of Information Systems	5
Permissions model	8,12
Physical Asset Register, or equivalent - e.g., register of laptops, hard drives, thumb drives that track information-bearing assets	22d
Privacy Impact Assessments	10,13,20a,b,c,d,e,24,35
Privacy Notices	24
Project governance artefacts - for example, PIDs, CABs, User Engagement and Research	20b,22a,d
Recommendations by formal bodies - e.g., ICO, GIAA - and responses	24,35,36,37
Records of Processing Activity (ROPA)	8,36
Regular reporting	9,17
Relevant audits, reports, and recommendations - e.g., on record keeping and information risk	7,14,18,63
Relevant Boards, specialist groups and the design authority	5,9,12,13,15,17, 20a,b,c,d,40,42a,c,53
Relevant case studies - e.g., managing change, influencing user behaviours, working through the pandemic	7,10,14,20a,b,26,48
Relevant decision-making framework, decisions logs etc.	13,39
Relevant documented process or procedure - Appraisal, Destruction, Review, Publication, Procurement etc.	6,8,9,10,12,17,20b,c,d,22c,d, 24,25,30,32a,35,36,37,38,39, 40,42a,b,c,d,46,47,49,50,51, 53, 55,57,59,61
Relevant enquiry log entries	20a,b,c,d,e
Relevant examples of corporate communications	10,30,42d
Relevant governance boards - empowered decision making	20d
Relevant guidance	6,7,8,14,17,20b,22b, 25,28a,b,c,d,30,32a, 36,40,46,47,48,57
Relevant Policy	6,8,10,12,13,16,17,18, 20a,b,c,d,22a,b,c,d,24,25,26, 28a,b,c,d,32a,b,c,d,33,36,37,3 8,39,40,42a,b,c,d,46,47,48,49, 50,51,53,55,61

Relevant records inventories and finding aids	6
Relevant reports	48
Relevant roles and job descriptions, demonstrating how we address the need	5,12,13,14,15,16,17, 18,20e,40,42a,c,57
Relevant staff training and skills frameworks	14,15
Relevant standardized templates	57,58a,b,c,d
Relevant standards embedded in our organisation	32a,b,c,d,33
Relevant training	15,20c,d,22d,32a,36, 39,42a,d,46,47,48, 58a,d,59
Retentions schedules	6,18,24,25,26,37,38,39,40,42a ,48,49,51,53
Retention schedules and associated policy	6,9,16,35,42b,58a
Risk Registers	13,17,20a,37,42a,52, 53,54,55,62
Risk reports	3,37,42a,52,53,54,55
Sample of metadata fields captured in different systems/media	28a,b,c,d
Secure storage specification	36
Service Level Agreements	32a,50
Standard contractual terms	22b
Standard Operating Procedures	12,13,26,32a,b,c,d, 35,55
Standard RM terms in Procurement	22b
Standardized provisions embedded within other documentation - e.g., procurement, Data Sharing Agreements, contracts etc.	10,20a,b,d,e,22c,32a, 50,57,58a,b,c,d,61
System configuration documentation showing relevant functionality - e.g., automated destruction	6,7,9,10,12,18,22a,b,c,d,25,28 a,b,c,d,32a,b,c,d,37,39,40,42b, c,d,48,49,51,55
Terms of Reference	5,9,17
Transfer registers	25,37,39,40
Information Lifecycle Documentation	24
X% of our information is subject to Crown Copyright	20e,58a,b,c,d

Chapter 7 Annex B - Definitions

During the S46 Practice Study conversations, the participants discussed a number of the terms and topics that appeared across the Self-Assessment, which felt hard to interpret by a single definition in the context of their organisation's size, type, function and complexity. The group discussed and agreed on definitions below that would help address the questions with greater consistency.

Definitions provided by the group should be used along with the Glossary of the S46 Code of Practice.

Designated Manager

The role of the designated manager will depend on the size and functions of the authority. In Government Departments the designated manager is the Departmental Record Officer (DRO) and in Northern Ireland the Information Manager (IM). Detailed information on these roles is provided at Annex C of the Code.

Governance

Governance, for the purposes of the IMA toolkit, is defined as the structures in place within public sector bodies that govern corporate activities.

Regular Review

The groups all concluded similarly that 'Regular' should have a temporal element, but also reflect something happening in response to a particular event. For example, regular could be interpreted as 'After no more than every 6/12/18/24 month [as agreed within your organisation] or following one of a recognised group of triggers, such as updates to fundamental legislation'.

Within your organisation, agree a definition of regular that works for you, and is compatible with your risk appetite. This may be timebound, or respond to various trigger events, like a change in legislation.

Senior Leadership

S46 Study Group: ‘Across the groups, the terms 'Senior' and 'Senior Leader' were generally interpreted in terms of the level of accountability held by the individual, for the purposes of supporting compliance with the theme described in the question.

While there was no single definition, interpretations included a Senior Leader as someone who:

- Is positioned at executive or other senior decision-making level.
- Can influence organisational decisions and direction.
- Can act as a point of consistent and ongoing representation.
- Has a high level of accountability in the organisation.

- Has broad contextual knowledge of the organisation, and insight into the organisation's structure and governance.
- Has the ability to consult subject matter experts and make considered recommendations and decisions.
- Can advocate for information and records management issues to other senior stakeholders both internally and externally, for example concerning restructures, resourcing, and procurement.
- Has access to the organisation's risk register and is able to contextualise risks escalated to them.

The Study group agreed that:

- A senior leadership position would typically include senior roles that have strategic oversight, responsibility for decision making and are accountable for performance, such as SIRO, DRO, Directors, Assistant Directors.
- Senior roles are often based in the top tier of the organisation, such as the executive, board, governors or oversight/steering committee.
- The level of the senior leader depends on the specific organisation in question.