Managing NDA Information Requirements

Version:4.0

Date:April 2019

Doc No: IMP06

Document Outline

This document sets out a series of requirements that custodians of NDA information and records are expected to consider and, where applicable, to implement measures that ensure the requirements are adequately addressed. Further information on this topic may be obtained from the NDA.

CONTENTS

EXECUTIVE SUMMARY

Creating confidence in the 'quality' of information recorded many years ago by unknown operators and by unfamiliar means, is difficult to achieve. Clarity and transparency is very important enabling the user to understand how and why the information was created in the first place. But it also has to be fit for the purpose for which it was intended, it has to be error free, based on valid assumptions, clearly and concisely recorded. It is human nature to question the reliability of any historical data and information – maintaining a complex set of information over several decades and then expecting the custodian to actually use it when making critical decisions should not be underestimated. A well-constructed and robust system for managing the technical and contextual content of the information is thereby essential if reliability, confidence and trust are to be ensured.

The Nuclear Decommissioning Authority and its Site Licence Companies and subsidiaries are responsible for managing the majority of low, intermediate and high level radioactive waste in the United Kingdom. Whilst the wastes vary, the management objective is common – safe storage and, ultimately, disposal. The information produced over the decades to support this objective must be properly and responsibly managed. Failure to do so may compromise the industry's long term capability to achieve safe storage and disposal. Enabling knowledge creation and transfer from one generation of workers to the next is essential. Furthermore, maintaining access to the information and providing the means for workers to understand and assimilate it is a high priority that cannot be addressed 'later'.

CHAPTER 1 - PRELIMINARIES

1.1 Introduction

The Nuclear Decommissioning Authority (NDA) has produced a Policy [1] that outlines the need to manage information that is created, stored and disposed of on its sites. The object of this document is to define a set of requirements, based on this policy, which can be used to inform local management strategies such that they are consistent and comprehensive. It needs to be read in conjunction with the good practice guidance published by the UK regulators and the International Atomic Energy Agency (IAEA)[1].

To support the main objectives of the NDA, significant volumes (in paper, microform and electronic forms) of information is produced and stored. Some of this information (for example, that relating to staff working in a radioactive environment) is critical to safe and effective operations and may need to be retained for many years.

This document has been written for all teams and those responsible for information and records management within the whole NDA estate (which include the NDA headquarters, its subsidiaries and its Site Licence Companies). The requirements are relevant to all management teams and Information and Records Managers. It applies to all NDA information assets, not just those relating to radioactive waste.

[1] www.iaea.org

1.2 Aim

The aim of this document is to set down a series of requirements, based on the experience of practitioners and accepted good practice, which are critical in the success of the management of information relating to the operation and management of NDA sites. Implementing those requirements that apply to local operations is vital for developing a common system for information and records management on NDA sites. However, it is also applicable to organisations that intend to use NDA facilities to fulfil their own radioactive waste (and other) management responsibilities.

A common, structured and visible information management system will have a positive effect on knowledge preservation inter-generational transfer.

1.3 Scope

This is an NDA-produced document but the principles and practices on which the requirements are based are common across the entire UK nuclear industry. Some of the requirements may also be applicable to other organisations who may also wish to consider the benefits of adopting the requirements set out in this document.

Many of the requirements will apply to information relating to all forms and categories of information – after all, the focus is on long term management of information in support of knowledge creation, preservation and transfer. However, some of the requirements may not be applicable to particular information where the need for long term knowledge is less critical or information where its long term hazard potential may require the adoption of even greater controls for knowledge preservation and transfer.

1.4 Who Should Read this Document

Anyone with a responsibility for records, information or knowledge management need to have an understanding of the range of requirements and implications of implementing them, particularly the effect on human and financial resources. Appendix 1 contains a summary of the requirements.

Records, information and knowledge managers are the group of professionals most likely to be charged with the implementation of the requirements contained in this document.

1.5 The Need for a Document for Managing Information

The principal aim of the NDA's Policy for managing information is to ensure that the management of information is planned, resourced and executed so that it is fit for purpose both now and in the future. Some processes performed by organisations in the NDA family will take many years to complete and it is vital that important information is managed so that these activities can proceed at the appropriate time.

There is also an ethical dimension to the management of information - the industry has many responsibilities to society. Failure to manage information relating to radioactive materials now will undoubtedly increase the burden placed on future generations.

1.6 Records Management

This document is about the management of 'information'. Information can be managed in many forms, and can also be referred to as 'document' or 'record'. Records and archives management principles are used widely within this document. In the records and archives field, a 'Record' is recorded information that has enduring value. 'Enduring value' is anything that is evidence of what has been done, or of how a particular decision was reached. An 'Archive' is information that is no longer required for operational business purposes, but has historical value.

Records and archives can be electronic or physical. In both cases they can be in any format, and on any computer system or physical medium.

One of the principles of records management is that each record has a retention requirement. The retention time for a particular record will depend upon legal, regulatory or business requirements. Within the nuclear industry, there are a number of regulators, including the regional environment agencies and the Office for Nuclear Regulation. The NDA has made available a Records Retention Schedule with advice on retention periods. This advice is based on information from the regulators, from national legislation and from knowledge of business requirements within the industry.

Non-operational NDA information will be retained in the archive facility known as Nucleus (the Nuclear and Caithness Archive).

1.7 Security classification scheme

All information has an intrinsic value and thus needs an appropriate level of protection. The security classification of information will depend upon the sensitivity of that information, in terms of the likely impact of its compromise, loss or misuse.

Information must be marked with the appropriate security marking in line with the Government Security Classification Policy April 2014[2] [19] and the ONR Classification Policy 2017 [as amended] [20].

Information transferred to Nucleus (the Nuclear and Caithness Archive) must be marked with an appropriate security classification. The organisation's IAO (Information Asset Owner) is responsible for deciding the appropriate security classification prior to transfer.

Where legacy information (created or being processed pre 2015) is not marked this will be logged by Nucleus as OFFICIAL:HISTORICAL. The IAO will be asked to review the security marking should Nucleus receive a request for this documentation. Following the review, the security classification marking will be updated in the Archive Management System (AMS) by Nucleus (the Nuclear and Caithness Archive).

Information created or being processed since 2015 onwards and for all vital records that are not marked will be treated as OFFICIAL by Nucleus (the Nuclear and Caithness Archive) unless

[2] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/251480/Government-Security-Classifications-April-2014.pdf

instructed otherwise.

Where a security classification marking has been altered on a document and there is no evidence of a second review of the re-classification then the document should be treated in line with the highest classification marking on the document.

The transfer of security controlled documents needs to be managed in a specific way. Nucleus (the Nuclear and Caithness Archive) must be contacted prior to the transfer of any security controlled documents.

1.8 Context

This document needs to be read in conjunction with two other documents, both of which have been published by UK regulators.

The first, jointly published by Health & Safety Executive (HSE), Environment Agency (EA) and Scottish Environment Protection Agency (SEPA) in February 2010, is called "Managing information and records relating to radioactive waste in the United Kingdom" [2]. It is Part 3d of "The management of higher activity radioactive waste on nuclear licensed sites". This guidance document sets out the expectations of the named regulators in terms of the management of radioactive waste related information on UK nuclear licensed sites.

The second was republished by the Office for Nuclear Regulation (HSE) in March 2013 under the title "Nuclear Safety Technical Assessment Guide – Licensee management of records", Revision 4 NS-TAST-GD-033 [3]. The purpose of this document is to provide generic guidance to advise and inform ONR inspectors when exercising professional regulatory judgment on the adequacy of a licensee's records management arrangements made under Licence Condition (LC) 6.

This document complements these two guides and great care has been taken to avoid conflicts between all three. Many of the requirements set out in this document arise as a result of specific regulatory expectations but they are more generally focussed on good management practices. Whereas, the regulators' guidance is intended to apply to a nuclear site as a licensed entity, this document approaches the management of NDA information from a 'UK perspective' where numerous stakeholders each play a role in the civil nuclear industry. Thus, there are several references to the importance of establishing shared goals, promoting effective communications and the clear transition of responsibility.

CHAPTER 2 - GENERIC REQUIREMENTS FOR THE MANAGEMENT OF INFORMATION

2.1 Developing an Information Management Policy

2.1.1 Requirement

Organisations must develop corporate policies for managing information

2.1.2 Reason

The management of information must be coordinated, comprehensive and integrated into existing business practices. Visibility of need and clarity of purpose is required to ensure actions can be planned and the resource implications understood. These are best served if the SLC or subsidiary has a clear policy in place that works in conjunction with other information management and business planning policies.

2.1.3 Implementation

A concise and clear written statement expressing the organisation's policy for the management of information is the recommended way of attracting the attention of those with a key role. The way in which the policy is expressed and delivered to staff will depend on the organisation's preferences. However, it needs to be sustained as a core corporate position.

This document identifies a number of requirements and provides recommendations on how the requirement may be met. The policy needs to use these requirements, and experience gained from within the organisation and possibly elsewhere, to formulate an approach. The actual processes for undertaking elements of the policy are likely to be described in much greater detail in local procedures. Where some procedures already exist, these **must** be amended to meet the requirements in this document.

Organisations in the NDA family must ensure the information management system is both capable of meeting the requirements of the local policy and has the means for routinely monitoring performance and making any necessary improvements.

In its publication "*Managing Digital Records Without an Electronic Record Management System*" [5], The National Archives (TNA) states that "system management rules are a set of explicit instructions to users on the organisation's preferred means for managing corporate information. These include direction on appropriate capture, access management and disposal of all information irrespective of format or storage media". It goes on to suggest the system management rules should include:

- Appropriate means of capturing electronic information into the filing structure;
- Clear definitions on what information should be captured into the filing structure and what may be held in a personal drive;
- Specific criteria for the application and management of access controls;
- Specific criteria for the disposal of all information with explicit reference to the organisations disposal policy.

2.2 Appointments, Responsibilities and Roles

2.2.1 Requirement

Organisations must ensure that suitably qualified and experienced people are appointed to key information and knowledge management roles and that those appointed understand their duties

2.2.2 Reason

The Government has taken examples of good practice and mandated that certain appointments are to be made within its departments to protect information from risk of loss. The management of information by organisations within the NDA family will involve many people over the years and all of them must be made aware of their individual roles and responsibilities and how they can contribute to the protection of information. Where possible, job or role descriptions must contain clear references to information management and steps taken to ensure these people receive the necessary training and guidance to be competent in their roles.

2.2.3 Implementation

Government has defined three roles [6] that focus on information risk management. All government organisations and Non-Departmental Public Bodies (NDPB), such as the NDA, must appoint staff to undertake these roles. These roles, or their operational equivalents, must be taken up by the Site Licence Companies (SLCs) and NDA subsidiaries:

- **Accounting Officer (AO)** – the AO has overall responsibility for ensuring information risks are assessed and mitigated to an acceptable programme at Board level. The specific risks to information need to be considered when defining AO accountabilities.
- **Senior Information Risk Owner (SIRO)** – the SIRO is a mandatory appointment in government departments and NDPBs. The appointee will normally hold an executive position and be familiar with all types of information risk. The risks associated with information can be significant and the SIRO must be aware of these and have the authority to take action to protect the information.
- **Information Asset Owner (IAO)** – the IAO is a mandatory appointment in government departments and NDPBs. The appointee is responsible for understanding what information is held within their part of the organisation, what is added and removed, how information is moved, who has access and why and for providing assurance to the SIRO. Information will be created in different parts of the organisation and in different forms over many years. The IAO has an important role in collating and protecting these information sources. In larger organisations it is possible that several IAOs will be appointed.

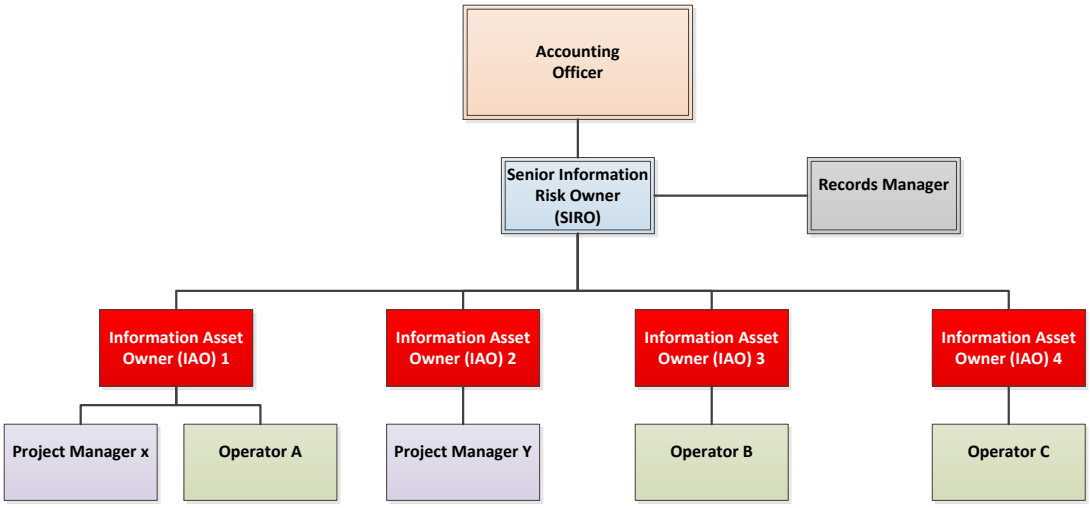
The AO, SIRO and IAO focus on the protection of information once it has been created. However, there are others within the organisation that are likely to have a role in overseeing the creation of information and the systems in which it is kept, such as:

- **Project Manager (PM)** – a PM, or equivalent, will often be appointed to oversee specific activities and deliver specific objectives. The PM needs to be aware of what information must be created and ensure there is a system in place for capturing it.
- **Records Manager (RM**) – most organisations appoint a RM who has overall responsibility for record creation, indexing, cataloguing, storage, review and destruction.

The RM must be informed of the need to protect the records of the organisation. The RM will also play a key role in ensuring that those who need to have access to the information whilst it is under the control of the organisation have the appropriate access. The RM may also advise on appropriate archiving procedures. The RM will work closely with the IAO(s) to control the formal transfer of records to other custodians.

- **Operators** – these are staff and/or contractors that may be required to create and store information related to the various processes undertaken. They will be required to implement information and record management procedures and seek expert advice where necessary.

There is no defined organisational structure relating to these positions but the following figure illustrates the hierarchy of key positions. In reality, an organisation's structure may be simpler than this. It is important that external stakeholders have a clear point of contact for obtaining information that they require.



In its Information Governance Strategy 2013 [7], NDA stresses the need for effective Knowledge Management within the SLCs:

- "Preserving the knowledge required in order to fulfil the NDA's core mission, that this knowledge is available to be reused across the Estate in a timely and cost effective manner and that learning is continuously captured and made accessible, both now and for future stakeholders;
- It must also ensure that key understanding of the sites themselves, the equipment used and the general environment is available throughout the decommissioning operations and that this knowledge is also preserved and used."

Managing information to the high standard necessary requires a specific set of skills. Teams responsible for the management of processes may not have the technical knowledge required to create and manage information such that it is sustainable over the long term. Senior managers

must consider the need for obtaining these specialist skills, if they do not already exist in their organisation.

The National Archives, in close collaboration with the Government, has developed the "Government Knowledge and Information Management (KIM) Professional Skills Framework" (developed Spring 2016).

7 different GKIM Professional Skills Frameworks are identified:

1) GKIM Skills Framework Overarching
2) GKIM Skills Framework Information Architecture Role
3) GKIM Skills Framework Information Management Role
4) GKIM Skills Framework Information Rights Role
5) GKIM Skills Framework Knowledge Management Role
6) GKIM Skills Framework Library Management Role
7) GKIM Skills Framework Records Management Role

These skills are relevant irrespective of the information being managed. Managers appointing staff to information management roles must ensure they are properly equipped with the necessary skills. The requirements detailed here must be used as a basis for determining how those competencies can be developed.

Government Knowledge and Information Management (KIM) Professional Skills Framework requirements are provided in Appendix 7.

2.3 Application of Quality Management System Principles

2.3.1 Requirement

Organisations must be able to demonstrate that they can implement a proportionate level of control in their information and records management activities, consistent with the principles set out in a recognised management system standard such as BS/EN/ISO 9001 [8]

2.3.2 Reason

The extended timescale over which the processing of some radioactive materials takes place means that the long-term management of information is particularly important. Complete and accurate information will increase confidence in the operation and management of processes, particularly as successive generations take on responsibility for their management. Informed decisions based on information provided by clearly competent workers, well managed processes and comprehensive and accessible information – is the foundation of responsible radioactive materials management.

Note that 'blind' adherence to the BS EN ISO 9001 Quality Management standard [8] is unlikely to be sufficient to address the demands of the management of information over the long term.

2.3.3 Implementation

The application of quality management system principles apply to each element of the information management system. The information management system must incorporate effective controls to collect data, create information and subsequently manage all these activities. It must address the following, as a minimum:

People

- clearly assigned and documented roles and responsibilities;
- provision of training to ensure competency in the creation, maintenance and retention of fit for purpose information;
- maintenance of training information;
- development of a culture that regards knowledge sharing and information management a benefit;
- identification and sharing of good practice with the means to implement improvements, where justified.

Processes

- provision of written procedures that ensure information is created, stored, reviewed and retained in an accessible form;
- controls are put in place to ensure all relevant activities are documented;
- methodology statements describing the operation of processes are written and consistently documented;
- controls are put in place to safeguard the integrity of information and prevent unauthorised alteration or amendment;
- retention times are clearly defined so that important information remains accessible for as long as necessary and until the withdrawal of institutional control from disposal facilities.

Tools

- computer codes are regularly reviewed and checked for accuracy and consistency;
- measuring equipment is regularly tested and calibrated, with this calibration information retained for future reference;
- internal audits are routinely conducted to ensure policy and procedures are implemented;
- peer reviews are carried out to ensure information is clearly and properly documented;
- periodic reviews are carried out to ensure documents and data are updated in a timely manner.

It is not a requirement that the organisation is formally certificated against BS EN ISO 9001. However, it is expected that the organisation's managers can demonstrate that they are in control of management practices in critical areas – and this includes long term information management. Independent evidence of compliance with BS EN ISO 9001 offers one way of demonstrating appropriate and proportional management control.

2.4 Information Risk Management

2.4.1 Requirement

The threat of unplanned degradation, alteration and loss of information must be identified and action taken to minimise the risks as far as practicable

2.4.2 Reason

Certain information produced by organisations is extremely valuable and thus needs to be maintained in a form that is accessible to other users. Organisations have a duty to protect all important information, to take action to prevent its loss and to maintain access. The costs (in terms of financial cost, radiological dose to workers and environmental impact) of 'reproducing' lost information should not be underestimated.

2.4.3 Implementation

An important part of information management is the prevention of unreasonable risk. One of the most obvious threats is that of the information becoming lost - through unplanned destruction, an inability to find the right information at the right time, unapproved alteration or inaccessibility caused by the way it has been created and managed. The consequences of information loss could be significant and so it is necessary to put in place measures that reduce these risks.

Information is needed to create knowledge and its loss will lead to the inability to make informed decisions. For example, if specialist knowledge about the particular nuclear materials and processes being handled is not available, the wellbeing of society and the environment might be put at serious risk.

Requirement 2.2 (see above) recommends that a SIRO and an IAO need to be appointed. Both these people have a critical role to play in the management of information risk. For example, the SIRO periodically ensures that an information risk assessment is carried out that will include consideration of the following:

- the clarity of the organisation's message on information management:
    - where has the need been explicitly defined?
    - how has the need been articulated to staff?
    - what actions are taken to ensure staff understands the message?

- clarity of the relevance of information to the organisation:
    - is there a record of what information is held?
    - is there a record of the security, sensitivity and importance of the information?
    - how management systems are to support information risk management?
    - recognition by staff of the importance of the information to the business (and in the longer term, societal) need?

- the assessment of all information threats:
    - has an information risk assessment process been developed?

  - have the threats been defined?
  - has the likelihood of each threat been determined to identify the degree of risk?
  - where is this information held and who is responsible for it?

- plans for managing information risk:
  - have mitigating actions been agreed?
  - is there a clear plan in place with action owners defined?
  - do the plans reflect the roles of the supply chain and customers?
  - is there a process for assessing the implementation of the plan?

- staff roles and responsibilities for managing information risk:
  - has all staff been informed of their responsibilities and potential impact?
  - do staff have a route for raising concerns or 'near misses'?
  - is there is a culture of information risk management?
  - do staff understand the consequences of poor risk management?

- organisation core skills and capabilities for managing information risk:
  - has a Senior Information Risk Owner been appointed?
  - does the organisation have the infrastructure to manage information?
  - is information management seen as a core skill?

- organisational culture for the management of information:
  - is information risk management undertaken as a matter of course?
  - is information risk given adequate priority and resources?

There are a number of 'generic risks' that must be addressed through the risk assessment and mitigation process. These include:

- the absence of clear and comprehensive oversight of information risk management and the resources and skills necessary for its control;
- the failure of new business processes to take into account information risk;
- lack of understanding of information to be created, retained, secured, deleted and preserved at a sufficiently early stage in the management system design;
- destruction of critical information, failure to retain or inability to find when needed;
- the recording of inaccurate information and allowing this to be propagated;
- technical obsolescence rendering vital digital information to become inaccessible;
- failure to allow information to be made accessible to the right people at the right times;
- absence of appropriate metadata.

Information contained in digital format is particularly at risk of loss, especially in the long term. The National Archives (TNA) has provided guidance under the Government's Digital Continuity

Project [9] on how to manage digitally-based information and the actions required mitigating the threat of information loss. Those responsible for the management of information must familiarise themselves with this guidance and implement plans to reduce the risk of loss of digital information.

The potential for information loss within the UK nuclear industry is significant. There are some specific threats that have been identified and these must be addressed in a coordinated way.

1. Specific Threat	2. Potential Risk	3. Mitigating Action
Organisational change	The civil nuclear industry has experienced many organisational changes over the last 60 years. Each change increases the risk of information being lost, relevance and importance becomes unclear and conflicts emerge in the management strategies	○ Create a record of industry organisational changes ○ Create local and national information management policies
Transfer of responsibility	Information residing in a site-based store or archive can be 'forgotten' and the opportunity for a formal handover of responsibility is not taken	○ Create local and national information management policies ○ Agreed procedure for handover of information
Breaking the link	Personnel with the necessary insight and experience to interpret the information are moved or otherwise become detached from the information	○ Assign information to an IAO ○ Ensure that IAOs are aware of requirements for 'interpreting' information
Orphaned information	Information does not exist in isolation - it will always be part of a larger information set. When responsibilities change, information can be transferred without consideration of the impact on the entire information set. This can lead to orphaned information whose relevance and provenance become uncertain	○ Create local and national information management policies ○ Identify and document the links between various information sets ○ Maintain links between information series
Decommissioning of Sites	Records are moved into off-site storage to make way for decommissioning programme	○ Ensure accurate indexing of records and an effective means of tracking ○ Ensure contracts contain adequate safeguards for records protection

Information risk management is a very important activity that will affect any organisation handling information. The loss of information can have a significant impact on operations both now and in the future and must, therefore, be explicitly addressed.

2.5 Metadata

2.5.1 Requirement

All information must have associated metadata

2.5.2 Reason

Metadata is a vital part of any information, without which there is an increased risk of the information being unusable. It is particularly important that the right metadata is created for digital information but it is also very important for hard-copy information. When the information becomes separated from its creators, the metadata can help validate the information and enable the reader to determine its credibility and the level of confidence that can be placed regarding its fitness for purpose.

2.5.3 Implementation

When digital information is created, some of the metadata is generally produced automatically by the computer application. This metadata can then be used subsequently by a computer to find the file and enable the software programme to convert the contents from binary code to a human readable form. Most of this metadata is not visible to the user, although it might be possible to add visible information, such as keywords. When hard copy information is created, the metadata is more likely to be created and recorded 'by hand'.

In all cases, metadata is associated with a 'piece of information'. The identification of what constitutes a 'piece of information' is an important part of the management of information. The makeup of a 'piece of information' will depend upon the particular type of information being managed. For example, in an Accounts Payable process, a 'piece of information' could be a whole year's file of invoices received, or alternatively it could be an individual invoice. In a project file, it could be the whole project file, or it could be a particular report or set of results. The choice of the makeup should depend upon long-term access requirements; such that the resource required to create and manage the metadata is proportionate to the ease of accessing a particular piece of information.

The National Archives defines [5] metadata as follows:

- data that describes the context, content and structure of all records and folders within a file system. In a file system this is essentially user-generated and 'passive' in that it can rarely be used for active management of the records. By contrast, metadata in an EDRMS (electronic records management system) is more functional, often system-generated, extensive and linked tightly to system processes.

There are a number of 'metadata standards' including one published by the UK Government for public records [10].

Metadata for records created or being processed since 2015

The NDA has decided to adopt the following definition of metadata as detailed in the table on the following page. The table describes the required metadata for all information created or being processed since 2015 onwards and for all vital records. This metadata is based on established standards as referenced in Appendix 4 of this document. NB. This table is subject to further review.

Metadata requirements for legacy records produced prior to 2015

There is a relaxation of mandatory requirements for legacy records which have a disposition of "Archive" produced prior to 2015

The minimum metadata required for legacy records is:

- Title
- Source of Data
- Security Classification

It is possible that older information will include incomplete metadata. In these cases, the minimum legacy metadata applies as detailed above. It must be remembered that the absence of metadata increases the risk of loss of the information content therefore where legacy records do have more than the minimum legacy metadata recorded this must be retained with the records.

Specific metadata is required for security controlled documents. Contact should be made with Nucleus (the Nuclear and Caithness Archive) with regard to the metadata requirements prior to transfer.

Metadata in Legacy Datasets

For any legacy metadata dataset to be accessioned to the Archive Management System (AMS), each field in the legacy database must be mapped to the most appropriate field as detailed in IMP06 metadata table. This mapping should be performed by Restore and submitted to the Nucleus End User Group (NEUG) for approval, for assurance that Restores interpretation is correct by the owning site. Any data fields that cannot be mapped directly to IMP06 through this process must be concatenated together along with their descriptors into a catch-all "Additional Information" field, so no legacy data is lost.

The following characters should be avoided in Titles and metadata fields ; / ? : @ = &" < > # % { } | \ ^ ~ [ ] `

Metadata Field	Explanation	Mandatory for pre 2015 records	Mandatory for records 2015 onwards	Default	Repeatable	Controlled	Example
Title	From title page or archive designation - in full with sub-title. Description if not named on the work.	Y	Y		Y	N	Final Letter of Compliance Bradwell IEX Medical records Leavers 1989-1990 A-L Cut-away model of Oldbury power station
Source of record	Where did this record come from? Who transferred it to the archive? "Fonds"	Y	Y	Source	N	Auth	Site name or site name followed by plant if need to be more specific NDAAL to maintain list of Fonds to include 'see' and 'see also' references: Magnox - SEE - Magnox Ltd Magnox Ltd. - SEE ALSO Magnox Electric Ltd. Magnox North Ltd Magnox South Ltd
Classification	Current or previous Security Classification	Y	Y	Official	Y	N	O, O-S, S, TS, Codeword etc.
NDA Archive Number	Nucleus Record ID Number	Y	Y	Applied by Archive	N	Y Unique	012345
Date of Deposit	Date of Deposit at Nucleus	Y	Y	Applied by Archive	N	N	2017-08-28
NDAAL Barcode	NDAAL use	Y	Y	Applied by Archive			Store/rack/press/shelf Disk/folder/file
Location	Location of Physical item	Y	Y	Applied by Archive	Y	N	Wick, Manchester
Disposition Action	Action to be taken on the Disposition Date	Y	Y		Y	N	REVIEW DESTROY – If no review is required prior to destruction Disposition action should be state Destroy.
Disposition Date	Date on which Disposition Action needs to take place	Y	Y				2020-02-20
Record Identifier	Local (original) identifier of document or doc package (may relate to finding aid)	Y	Y		Y	N	Box AA123 MIMP/ILW/BRA/FLOC.doc Magnox PRS 123
Version/ Issue/ Edition	Rev.1 , 3rd Ed., Issue 2, Ver. 2.3 etc.	N	Y	1	N	N	Rev. 2.1
Author	Author, Creator, Authoriser, Reviewer, Approver etc. with designation,	N	Y	Source	Y	N	Smith, Freda Jones, Edna Sellafield Ltd if individual Author not know If author not known default to using Source of Record or Publisher
IAO	Responsibility for future actions (role not name)	N	Y	Source	N	Y	Waste Operations Director, Magnox NDA Archives director
Language (if not English)		N	Y	Eng	N	Y	ISO 639-2 code

Date of Publication/ Production	From document or embedded metadata	N	Y		Y	N	2015-01-22 Where no day is known default to last day of month
Record Retention Schedule (RRS)	Reason for the record being kept – could be to a reference to the specific requirement in the RRS or to a legal/regulatory or business reason	N	Y		y	N	Companies House Act 1985, Line 445 RRS 2017
TNA Reference	Unique ID reference given by TNA when record is stored within TNA or is transferred to TNA	N	N		Y	N	AB12-548B, AB400-654
Subject/ keywords	anything that might assist 'unknown' item discovery	N	N		Y	N	Staff Personnel files: Care, Carter, Case, Cassin. Letter of Compliance, LOC, FLOC, ILOC, ILW, DCICs, 9B34c
Description/role	Form of the information	N	N		Y	N	Engineering Advice Note … Box of personnel records Site Shift Log Waste Acceptance Criteria. Package Record Schedule Engineering Drawings
Publisher	Company responsible for production/commission	N	N	Source	Y	Auth	Magnox Ltd Radioactive Waste Management Ltd Golders Ltd
Format/ composition	Digital/Paper/film	N	N		Y	N	PDF/A 35mm microfiche aperture card acetate film e-mail .msg file
Coverage (Spatial/Geo)	Site/region etc	N	N		Y	Y	Sellafield, Dounreay, Welsh Sites
Access Controls	Restrictions on access, to include Vital/Public Record detail	N	N		Y	N	Any restrictions on use. Closed. Public record
Coverage Start Date	For records that cover temporal data	N	N		Y	N	1978 April 1986
Coverage End Date	For records that cover temporal data	N	N		Y	N	1982 June 1987
Physical description (Extent, condition, physical size)	Number of boxes, number of files (in number of boxes), size of drawing, extent of, duration, size of file etc. Physical condition if not perfect	N	N		Y	N	63 pages. Box of 7 files. 24 X 1.1 cuft boxes 16mm film reel, 144ft, 4 minutes 128Kb Original smoke damaged and missing cover page Artefact: 500cm, A3, A4
Reference point	Page/table reference	N	N		Y		"Page 23, Table 7 ", "Chapter 13", "Issue 42, page 34"

Relation to other item	List of other record identifiers associated to this record	N	N		Y		MIMP/ILW/BRA/FLOC.doc Magnox PRS 123 01253487 Waste Package Records - Package Records Schedule (PRS) reference
Dependency	tools needed to access etc.	N	N		Y	N	Mind-reader ™ software required to display
Scale	of map, drawing, model etc.	N	N		Y	N	1:24, 1:25000
Processing Information	Converted from / to	N	N		Y	N	Digitised from paper by Restore Ltd 2012 following QP123 (see http://ndaal.doi/QP123)

When creating digital information, the system may be able to automatically create the metadata needed for computer applications to retrieve and display the digital contents. The structure and content of automatically created metadata is not normally within the control of general users. Electronic document management systems often include the facility to set up a template where additional information about the file can be recorded – for example, key words or phrases, content descriptions. Where possible, the requirement to complete the metadata should be enforced. A properly constructed and populated set of 'descriptive' metadata will add considerable value to the information and contribute to its long term value.

The relevant information owner must liaise with the Records Manager and the IT provider to ensure that all staff understand the importance of creating accurate metadata. The challenge of creating accurate metadata for existing and archived information is significant. It may not be possible to establish metadata for all information on grounds of both practicality and knowledge. However, it is possible to document the legacy metadata content for records which have a disposition of "Archive" or retention of 10 years or more. To do nothing is not a sustainable position as this represents a high-risk strategy.

2.6 Physical access

2.6.1 Requirement

Actions must be taken to ensure information remains physically accessible to those who need it and for as long as it is needed to perform relevant management activities

2.6.2 Reason

The UK's radioactive materials management activities will result in the creation of a large amount of information. Retention periods, locations and custodians will vary but if the content of this information contributes to operational management, there must first be a system that enables a potential user to locate and gain actual physical access to the information required.

2.6.3 Implementation

Ensuring physical access to information is clearly important. If physical access is not possible because the existence of specific information is not known, or it cannot be found within a collection or cannot be physically (or digitally) extracted in such a way that the information content can be accessed, then the original objective that demanded its creation cannot be achieved. Poor control of information is unacceptable.

Physical access to information relies on knowledge, including its:

- existence
- location

- owner
- custodian
- form
- access restrictions

Access often fails because the owner or current custodian forgets, or is not aware, of the existence of the information. A simple measure that can mitigate this risk is the production of an Information Asset Register (IAR) containing basic information about all information sets. An EDRMS will aid the production of this register for the period it is used to manage the information. This may have to be supplemented by a manually produced register for older information or those that take a non-document form, such as photographs, drawings, physical samples. It is the responsibility of the information owner to ensure all information under their supervision is included in the register. Responsibility for the production and maintenance of the register(s) may be assigned to an organisation's Records Manager.

The NDA's Records and Information Advisor is responsible for the maintenance of the NDA Record Retention Schedule. This schedule provides a generic framework for record retention requirements within the NDA Estate.

Any suggestions for additions, deletions, amendments or queries should be forwarded to the NDA's Record and Information Advisor by email to Infogovernance@nda.gov.uk

There may be issues with access to information created 'behind the barrier', as they may have been contaminated by radiation. There are two methods for ensuring access to this information:

- de-contamination (with an appropriate certificate attached);
- scanning 'behind the barrier' (using the controls specified in 2.15.3) and transferring the information electronically to an appropriate store 'outside the barrier'.

There are many similarities between the management of metadata and the IAR and the functions could well be combined.

The requirement for an information asset register must be considered along with the appropriate storage requirements (see 2.9) as both access and storage is clearly related.

2.7 Information Access

2.7.1 Requirement

Actions must be taken to ensure that information remains accessible to those who need it and for as long as it is needed

2.7.2 Reason

Information can often be complex because it has been created by a number of individuals and/or organisations in different ways. Special measures are therefore needed to ensure the information can be found, interpreted and understood for as long as deemed necessary. Failure to access important information may severely compromise future operations.

2.7.3 Implementation

The previous requirement (2.6) referred to physical access to the information. This requirement focuses on the importance of ensuring the required information can be extracted and used by the reader. In very simple terms, information is accessed in three stages:

- 'retrieval' of the data from the storage media;
- 'conversion' of the data into recognisable symbols;
- 'interpretation' of the symbols to produce meaningful information.

Together, the originator, information asset owner, Records Manager and others must ensure that the information is managed in a way that will not preclude its accessibility at a later date. Hard copy-based information (paper, film) is generally easier to access at any time. Access to digital information (such as local hard disc, CD, DVD, server) may be more complex as there is an absolute reliance on computer technology – particularly the supplier of the software needed to read the digitised information. The pace of change in digital technology and tools adds a further degree of complexity to the challenge.

Great care must be taken when selecting storage media and format (see 2.8) - the deciding factor will be the assured access to information over a defined period of time. For information residing in an archive, digital media needs to be carefully managed as the threat of the loss of access is particularly high unless a rigorous management regime is implemented. Appendix 2 contains a list of International and British Standards relevant to the selection of storage media and information management strategies.

The Records Manager must establish a process whereby information can be regularly assessed for accessibility and threats identified. This is particularly important for digital information, and all information stored in archives. Where storage media such as CD / DVD is used, media in use must be assessed at regular intervals for degradation and damage and for loss or corruption of stored information. Where there is a heightened threat (such as when one piece of media fails), remedial action must be immediately taken for all potentially affected information. With some media types (such as CD/DVD), loss can be total and with little warning (catastrophic loss). Records Managers must therefore consider the need to hold duplicate sets of information on different media. Where information is classed as 'vital records' (see 2.14), the requirement for duplicate storage media of different types is fundamental to good records management.

Strict controls must be implemented to ensure that important information is not altered without proper authorisation. Any change to information that could impact on conclusions drawn from that information, particularly archived information, must be recorded. Physical access to information must be restricted for this reason. Additional care needs to be exercised for digital information – particularly that information residing on a storage device accessible to many people (for example a network server). Some additional measures can be taken to protect digital information. For

example, a spreadsheet could be converted from the original application format (for example, a Microsoft Excel) to portable document format (PDF/A 1b) – a simple action that would prevent accidental alteration of data and improve access for users who do not use the originating application. It is general accepted by archivists that PDFA is a stable digital format and suitable for long term storage.

The Information Asset Owner (IAO) must decide the appropriate retention period (using guidance from the NDA Record Retention Schedule as appropriate). This date should be recorded as the Disposition Date. If the IAO wishes to review the records prior to their destruction the Disposition Action for the records must be recorded as Review. Where the IAO is happy for the records to be destroyed on the Disposition Date by Nucleus (the Nuclear and Caithness Archives) without a review the Disposition Action for the record should be recorded as Destroy.

If a retention period cannot be determined, this fact must be recorded and a review date (Disposition Date) included. The Disposition Action must be recorded as Review. There must be a documented procedure for the review of information – including those with open ended retention. In this case, there must be a process for the migration of the information onto replacement storage media, if necessary.

Where information needs to be retained past the retention period, due to a legal hold being in place, it is the responsibility of the Records Manager to inform Nucleus (the Nuclear and Caithness Archives) so appropriate action can be taken to ensure information covered by the hold is not destroyed. The Records Manager must inform Nucleus (the Nuclear and Caithness Archives) once the Legal Hold has been removed.

2.8 Selecting the Appropriate Storage Media and Format

2.8.1 Requirement

> The appropriate media and format must be used for storing information, ensuring that integrity can be maintained and the information accessed at any time

2.8.2 Reason

The risk of information loss can be dramatically increased if the storage media used is not appropriate for the management system adopted. There is no 'ideal' media suitable for all forms of information. A number of 'management factors' must be considered when selecting the appropriate storage media. An effective management system will result in the identification of the optimum media.

For digital information, choosing an appropriate storage format will reduce the risk of issues with the availability of software that will display the information in an acceptable manner, over an appropriate time. An appropriate choice of format will also reduce the need for or frequency of format migration processes which update formats to more modern equivalents.

2.8.3 Implementation

Storage media

Selecting an appropriate storage media is critical for mitigating one of the main causes of information loss. Selection must be based on a clearly defined process that takes into account, as a minimum, the following factors:

- quantity of information to be stored;
- type and form of the information to be stored;
- length of time the information is to be retained;
- intended frequency of the reviews of stored information;
- proposed frequency and process for migrating information onto replacement media;
- maximum time allowable to locate and access information;
- maximum time allowable to find specific information;
- the acceptable level of technical sophistication in information storage;
- the acceptable level of technical sophistication in information retrieval;
- proposed method of transferring information to another custodian;
- cost of purchasing media and supporting technology;
- cost of maintaining storage media, information and supporting technology;
- proposed storage facility conditions and management regime;
- anticipation of the information access restrictions that may affect a future custodian.

Storage media must be selected by a process that considers all of these factors. It must not be made simply on the basis of cost or convenience and it must take into account that the media for 'in use' information may be different to that for archived information. Appendix 3 contains a comparison of some of these factors against commonly used media.

For waste package records (as an example), once the waste package has been produced and placed into interim or long term storage (in some cases prior to disposal), it may be possible to discard a proportion of the numerical (quantitative) data that has been created, resulting in a higher proportion of descriptive (qualitative) information. With the waste package in storage, it is unlikely the package record will need to be accessed on a frequent basis. Whatever is the long term fate of the waste package, the associated information will be needed to enable the waste packages to be transferred to alternative storage or disposal facilities, so access to the information remains an imperative. Based on the factors above, the use of paper or film-based media in addition to the digital information may represent a lower risk to information loss. This would result in a very robust and well-resourced management system where information can be frequently reviewed and, where appropriate, migrated onto new storage media.

The environment in which information is stored is one of the crucial factors that will influence the storage media selected. Information storage is considered further in section 2.9. However, there are a number of British and International Standards that define the characteristics of appropriate storage media (Appendix 2).

Two types of hard-copy media are in common use in the United Kingdom. These are paper and photographic film. Some countries have developed specialist media, such as silica carbide tiles (Japan), but these are not currently under serious consideration in the UK.

There are various grades and qualities of paper. Long term paper-based information must utilise papers that are commonly referred to as 'archive paper'. Recycled paper must not be used for long term storage unless:

- its components can be confirmed;
- there is evidence that its performance is equivalent to archive quality paper;
- the management system ensures the media is checked frequently and the information transferred when signs of degradation are observed.

Only paper that complies with relevant International Standards (or their current equivalents) must be used for long term storage of information. Appendix 2 lists the principal standards for paper.

Photographic media is a good alternative to paper. The advantage with photographic film is that it has the potential to store more information than paper as the image size is reduced, and it requires relatively simple technology to recover the information. It is also relatively durable if it is stored in conditions similar to those required for paper. Where photographic film (for example, microfiche, microform, aperture cards) is used, its processing and storage must comply with relevant British and International Standards (or their equivalents) – as listed in Appendix 2.

The preferred size for microforms of paper originals is 16mm. Typically this is produced at 24x reduction as this permits a standard A4 page to be captured across the width of the film. 35mm microfilm (in the form of aperture cards or as roll film) is typically used for drawings that can be up to A0 in size.

There is a wide range of digital storage media. These can be categorised as magnetic, optical and solid state.

Some information might be stored on removable magnetic media – such as floppy disks, dismountable hard disks (for example, the 'Winchester Disk'), magnetic tape and USB drives. The risk of information loss when using these media for long term storage is very high and they must not be used, under any circumstances, for this purpose. Where legacy information is held on these media, it must be transferred to a more suitable media as soon as possible.

Optical media in common use include the Compact Disk (CD) and Digital Versatile Disk (DVD). These disks are generally regarded as useful as transportable storage media (along with the use of USB drives). CDs became commercially available in 1982 but they tended to be used primarily for

audio recordings. DVD technology followed in 1995 and they were seen to provide a greater range of capabilities, being used for both audio and data storage. DVDs also have a much higher storage capacity than CDs.

CDs and DVDs re suitable only for short term storage of data. The market for specialised media (for archive material, for example) is extremely limited, so care must be taken when purchasing these media with longer term storage in mind. There is currently no International Standard for the production of high quality 'archive grade CD/DVDs. There are some international standards that relate to the testing of CD/DVDs for long term integrity and durability and these are listed in Appendix 2.

The only transportable solid state digital storage in common use is the so-called USB drive (memory stick). This media is relatively robust although catastrophic failure is not unknown. Memory sticks are not considered sufficiently mainstream for the long term storage of information and are thus not recommended for this purpose. As these devices are easy to misplace, it is highly recommended that any information stored on this media is encrypted and the access keys kept separate from the media. Some USB drives come equipped with encryption software, such that information is 'auto-encrypted' during the storage operation.

Computer network servers are used extensively in the management of information in the UK and they are often regarded as the storage device of choice. The information stored on network servers must be regularly backed up - this is a good way of mitigating loss as a result of a hardware fault. It is preferable that server storage is used in preference to transportable media for the storage of information. When combined with fault tolerant systems (such as the use of RAID technology), 24/7 operation using mirrored systems and suitable information and records management software (EDRMS solutions), a highly efficient document archiving solution can be configured. Where high volumes of low access rate information is stored, the use of a hierarchical storage system (based on on-line, near-line and off-line storage) can reduce the cost of digital storage.

The speed of change of digital technology – both hardware and software - means that a strategy of technology migration must be developed. This strategy must include the following elements:

- technology watch activities which identifies technology trends;
- review of existing technology, including error monitoring and operational costs;
- planned migration (hardware and software) prior to a significant increase in errors / costs;
- responsibilities for ensuring continued operations.

Data loss from digital storage systems can be catastrophic in that the whole content of the storage device can be made instantly and completely irretrievable. Suitable business continuity plans (sometimes called disaster recovery plans) must be in place and tested at regular intervals. These plans must be based on the availability of up-to-date backup media.

There is a further risk to digital storage – the presence of software viruses. All digital media must be scrupulously checked for the presence of virus that may 'contaminate' host systems and other storage devices. This could become an increasingly serious issue where digital data is transferred or

shared with others. Hence all digital storage systems must be regularly checked for viruses using up-to-date software. Similarly, all data received for storage must be checked for viruses prior to them being stored.

In summary, information that must remain accessible in the short term only can be placed on digital storage devices as long as they are stored correctly and they are regularly monitored and, where necessary, the information is regularly migrated. Paper or photographic film can also be used for medium and long term storage; however appropriate storage conditions and inspections need to be in place to ensure their usability.

Storage format
The selection of an appropriate storage format will result in the reduction or elimination of issues with software obsolescence. Selection must be based on a clearly defined process that takes into account, as a minimum, the following factors:

- format of the original digital document;
- type and form of the information to be stored;
- length of time the information is to be retained;
- intended frequency of the reviews of stored information;
- anticipated longevity and cost of appropriate information retrieval software;
- ease of conversion (if required) to alternative formats;
- storage file size.

Where long term access is required, a digital format suitable for archival purposes must be selected. For text based documents, the PDF/A format (BS ISO 19005) is approved for this purpose.

In addition to text based documents, where graphical, audio and/or video content is involved, appropriate standards for their production and storage should be employed. Different standards may be appropriate for the primary content of the documents than for secondary or supporting content. Typical formats that should be used for documents with non-text based content include JPEG and MPEG. Use of any of these formats, allied to the appropriate management of the storage conditions, will ensure that the record can be maintained for any duration. Where storage in other formats is anticipated, reference must be made to the Records Management team at the NDA for approval prior to their use.

Compression of electronic documents (for example the used of .zip files) must be avoided where long term retention is required, as the availability of decompression software cannot be guaranteed over the long term. There are internationally agreed compression methods for image files (and especially colour image files – such as JPEG) which can be used with care. For PDF files, the use of 'FLATE' compression is included in the generic file format specification; however such files do not conform to the PDF/A specification.

File naming conventions
File naming conventions relate to both physical and electronic information. For physical files, it relates to the information recorded on the front of paper files or on the package containing the microform. In the case of electronic files, it relates to the name of the file chosen.

When choosing file names, there are three principles to be followed:
the name must be meaningful to those who may need access to the information;
the name must be structured to allow sorting and searching;
the name must contain as much (but not too much) detail as possible.

When choosing file names:

- do not use abbreviations;
- use only letters, numbers and spaces (i.e. no punctuation);
- dates must be in the format YYYYMMDD;
- company name – use the full name (no abbreviation) and do not include 'Ltd.' etc.;
- persons name – use surname followed by forename and do not include Mr., Mrs. etc.;
- include a status indicator such as DRAFT where appropriate;
- add a version number where appropriate.

2.9 Storage

2.9.1 Requirement

> Information must be stored and maintained in such a way that its physical integrity is preserved and the information is accessible until a decision is made that it must be destroyed

2.9.2 Reason

The environment in which information is stored and the procedures used when handling them are critical to maintaining their physical integrity of the storage media. An assessment of all information needs to be made to determine the likely outcome on the long term safety of operations, human health or the environment if it were to be lost or unintentionally destroyed. If the outcome is unacceptable, an authentic copy of the information must be made using different storage media and the information stored under different conditions to minimise the effect of systematic failure. Where information is classified by the organisation as 'vital', then the storage requirements described in 2.14 needs to be implemented.

NOTE: Where media conversion processes are implemented (and particularly where paper to electronic conversion is implemented), appropriate mechanisms (see 2.15) must be employed to

ensure that no significant loss of information (including metadata) occurs.

2.9.3 Implementation

Media used for the storage of information must be actively managed. All storage media will degrade over time and if this goes unchecked, there will be a point at which the contents of the information will be lost or impossible to retrieve, either totally or in part. If this happens the objective to inform others will have failed.

There are a number of environmental and physical factors that will affect the durability of the storage media. The main features are listed below together with the media particularly affected and measures that must be used to reduce the unwanted effect of the feature on the media.

Factor	Media particularly affected by this factor	Measures that could be used to reduce the detrimental effect on storage media
Temperature	Paper Microform Network server	Storage facility location Temperature controlled storage facility Controlled access to avoid sharp changes in temperature
Relative humidity	Paper Microform Magnetic Network server	Storage facility location Humidity controlled storage facility Controlled access to avoid sharp changes in humidity
Exposure to light	Paper Microform	Restricted access to storage facility Use of non-routinely accessed areas Control of artificial light sources Absence of natural light
Gaseous contamination	Paper Microform	Storage facility location Control of incoming and recycled air Gas scrubbers Inert shelf / racking coatings
Particulate contamination	Optical Magnetic Network server	Storage facility location Control of incoming and recycled air Particulate sieves
Fluid contamination	All	Controlled use of equipment employing liquids and fluids Ensuring hands are free of creams and lotions
Vermin	Paper Microform Some magnetic (tape)	Controlled access Building integrity Traps
Fungal growths	Paper Microform Some magnetic (tape)	Storage facility location Control of incoming air and recycling Racking design to promote air circulation
Magnetic fields	Magnetic Solid state Network server	Storage facility location Storage facility design Storage facility construction materials Restriction on use of certain electrical devices

Ionising radiation	Microform Magnetic Solid state Network server	Storage facility location Storage facility design Storage facility construction materials Restriction on presence of radioactive materials
Fire	All	Heat and smoke detection systems Zonal fire suppression systems Storage units/cabinets
Handling	All	Procedures to minimise personnel access Protective clothing and equipment Use of suitable packaging

Paper
A significant amount of information that is placed in archives will be paper-based. Inadequate preparation of this information and poor storage conditions will have a detrimental effect on the integrity of the paper. The Transfers of Records for Permanent Preservation to the NDA Archive Facility Procedure should be followed when preparing records to send to Nucleus. Reference should also be made to NUC PRO 0044 Nucleus User Guide.

Archive design, construction and operation are very important for information preservation and security. Further information on this aspect of information storage can be found in the BSI publication PD5454 [14] and BS EN 16893, due May 2018.

NOTE: Nucleus will operate in accordance with these requirements.

Microform
The optimum method for storing microforms will depend on the precise nature of the material, the format and their intended use. However, microform must always be stored under the appropriate conditions in accordance with BS 1153 [12].

Magnetic media, optical & solid state
Air conditioning and dehumidifying equipment will often be necessary to maintain the recommended storage conditions for magnetic media but care needs to be exercised as there can be problems with static electricity in low humidity conditions. This can be a particular problem where solid state storage media are used.

Atmospheric impurities can adversely affect the magnetic particles on tape. In addition to corrosion caused by excess moisture, some volatile chemicals can reduce tape lifetime by attacking the binder and the polyester substrate. It follows, therefore, that the atmosphere in the storage area must be kept as clean as possible.

Finally, the presence of magnetic fields created by large magnets or electronic equipment has the potential to alter the orientation of iron particles on the tape thereby deleting or indirectly altering the stored information. Magnetic media must therefore be stored in cabinets that eliminate this particular risk.

Network servers

The storage location itself must be suitably secured depending on the perceived risk and the sensitivity of the information. Security procedures must be established such that not only is the integrity of the information preserved, but that unauthorised changes, amendments and deletions are controlled. The International Standard ISO/IEC 27001 [13] specifies requirements for establishing, implementing, maintaining and continually improving an information security management system. Implementation (and formal certification where appropriate) of this International Standard enables the demonstration of good information security management.

2.10 Information Asset Registers

2.10.1 Requirement

A register (IAR) of all information held must be maintained and regularly published

2.10.2 Reason

It is essential to establish a list of all information held, particularly where these are widely dispersed throughout the organisation. An Information Asset Register (IAR) is a tool for organising and managing an organisation's information assets, and the risks associated with them. The IAR provides a high level overview of what information is owned, available and maintained. The IAR also includes any links between information assets, their owners (IAOs), their business requirements and technical dependencies.

An IAR that is well maintained will help ensure that:

- information can be found;
- the type of information is defined;
- information content is described;
- importance and value of the information is clearly identified;
- links between information sets stored in different locations is made visible;
- a means exists to identify information gaps.

If the existence of particular information is unknown, or is of questionable provenance, it is unlikely the information will receive the attention it requires and its value in the long term will be significantly reduced.

2.10.3 Implementation

Operational records

For information, and particularly that information with a very long retention period or containing information that is classified as 'vital records', a high standard of cataloguing is required. It is likely that the Records Manager will have ultimate responsibility for creating and maintaining an IAR, often with assistance from those responsible for business processes. The IAO will have responsibilities for ensuring that the Records Manager is aware of the existence of the business processes and for

supplying information about them. The IAR must list and briefly summarise the contents of information. It must also contain a brief description of the information, its location, information asset owner and retention requirements.

When new / amended business processes are being designed / implemented, the requirement for – and thus the creation of – information relating to the processes must be determined. The existing IAR must then be examined to determine whether additional entries in the register need to be made.

Information remains active for as long as there is an expectation that the contents will be needed for day-to-day operations. Information can and should be made semi-active once day-to-day access is no longer required. This needs to be a formal process which must incorporate specific controls. Where information has been made semi-active or inactive, provision to transfer it to Nucleus (the Nuclear and Caithness Archives) must be put in place.

Archive records
An archive description must be recorded for each piece of information transferred to an archive for long term preservation.

Archived information can be particularly vulnerable if insufficient or inaccurate information is maintained - there are risks arising from 'out of sight, out of mind'. Given the long-time scales involved in the management of some information, many of them will be transferred to archives and may remain there for many decades.

It is vital that appropriate 'archival descriptions' are produced. The International Council on Archives' Standard for Archival Descriptions [11] should be used as a starting point for the development of an information archives description. Much of the information required for an archival description can be obtained from the metadata supplied with the information (see 2.5.3).

A listing containing a brief summary of the contents of information in use is a very helpful aid in its management. A description (see 2.5.3) must be provided for every document transferred to Nucleus (the Nuclear and Caithness Archives) for long term preservation. It is eminently good management to create the descriptions as soon as possible and at the time when the originator and contributors are on hand to give advice. Postponing this activity to a later time when knowledge about the information has diminished increases the risk of inaccuracies and places a far higher burden on the current custodian or archivist.

2.11 Review, Retention and Disposition

2.11.1 Requirement

There must be a process implemented for the routine review of any information created in support of the processes undertaken. The review is concluded by a decision to either retain the information 'as is', transfer the information to alternate storage media, transfer to archives or destroy

2.11.2 Reason

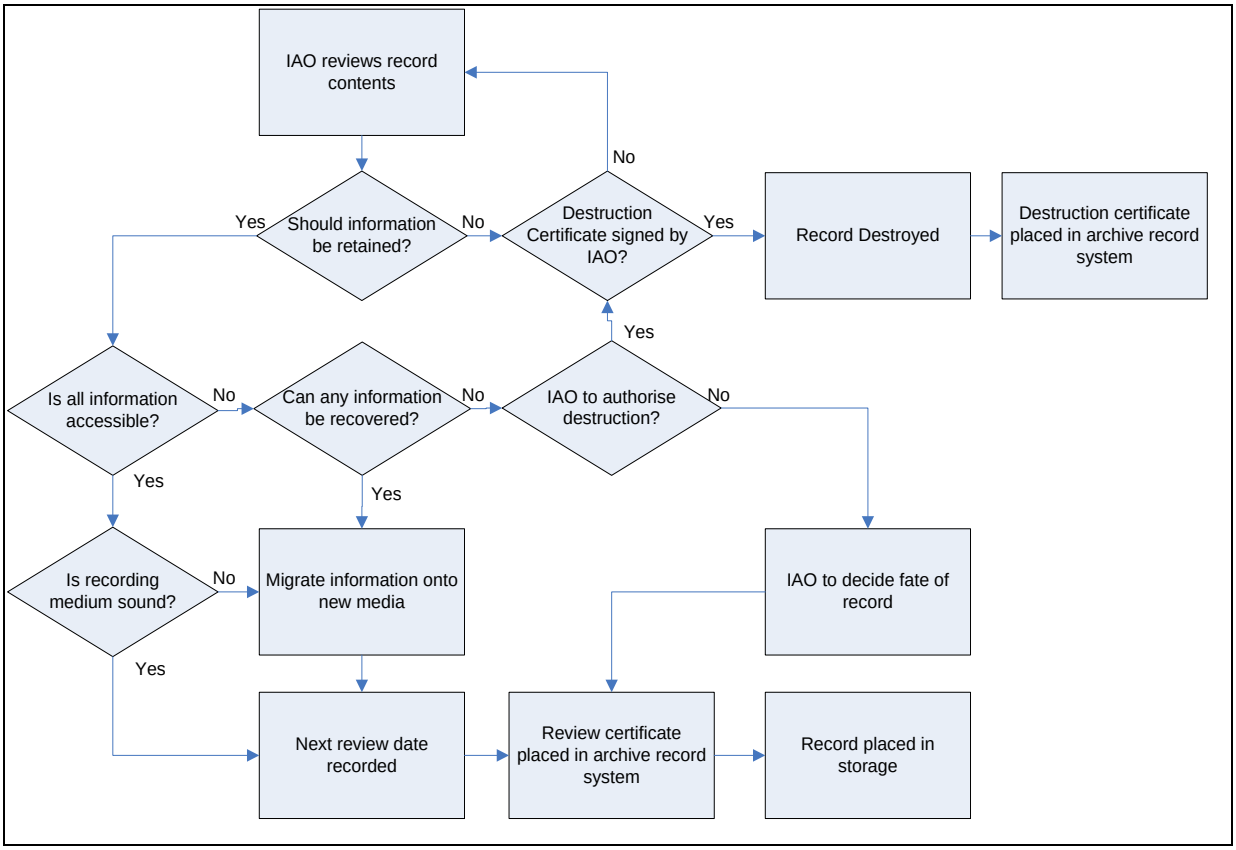
Reviewing stored information is a fundamental part of records management. Some information will have a finite period of usefulness after which it may become of historical interest only. Information must be clearly marked if it has been superseded or no longer relevant and removed from active use. This must be done in a systematic, controlled and visible way. The review process also fulfils other important roles such as gaining assurance that the information remains accessible and that the storage media is sound and will remain so until the next review. Efficient and effective records management will not require that all information is retained 'forever' but disposition must be controlled and the outcome recorded.

2.11.3 Implementation

All information must be clearly linked to the NDA Record Retention Schedule. This will determine whether the information must be retained until a certain time or event has elapsed and if a disposition date has been agreed. The absence of a retention period (which is recorded in the organisations retention policy) could devalue the information. The flow diagram below shows a typical review process that includes a review of disposition date, information accessibility and media condition. The result of the review must always be recorded.

The information asset owner is responsible for ensuring the information review is undertaken. A number of criteria must be considered when deciding on the fate of the information. These criteria must include (but are not limited to):

- the type of information - see below for information types;
- the relevance of the information to current activities;
- the likelihood that the information will be needed to support future activities or enable decisions to be made;
- the present and future risks that will be incurred if the information is lost or destroyed;
- the potential costs if the information has to be re-established;
- the contribution the information makes to the overall knowledge base of the organisation, or elsewhere in the NDA estate.



The reviewer must always bear in mind that some information may have little apparent value at the current time or in the immediate future but that it may gain in significance at later stages of its lifecycle. There is also a need to consider the potential for requests for information by those not directly involved in the day-to-day operations, such as site stakeholder groups, special interest groups, local planning authorities, regulators, contractors and governments.

When the retention period has expired or the disposition date reached, the information asset owner is responsible for reviewing the information and to advise the Records Manager on the course of action, which will be one of:

- retention of the information for a further period and the recommendation of a new review date;
- transfer to another owner (such as Nucleus);
- destruction of the information.

The Records Manager is responsible for carrying out the post-review request, as follows:

- If the information is to be retained, the Records Manager must record the date of review and the name and affiliation of the person undertaking the review. As a minimum, this information must be included in the IAR. In addition, the Records Manager must consider the need for making any changes to the information content that will preserve accessibility or to transfer to

replacement storage media;

- If the information is to be transferred to another owner, the Records Manager must ensure the change is recorded and that the receiving owner formally accepts responsibility.
- If the information is to be destroyed, the Records Manager must record the outcome of the review and formally record the destruction.

The following information must be retained, as a minimum:

- subject;
- title;
- creator – person and affiliation;
- information identifier;
- date of creation;
- brief description of coverage/scope of information;
- reason for destruction.

It is recognised that the prospect of reviewing all existing information is daunting. However, all new information from 2015 must be included in a review programme and existing information added based on their perceived importance.

2.12 Fit for Purpose Information

2.12.1 Requirement

Information must be created and recorded in such a way that it is capable of supporting the need for which it was intended

2.12.2 Reason

Information must be created and recorded in such a way that it is able to contribute to the activity for which it was intended. If information is produced at the wrong time, in the wrong format, is not of the required accuracy or precision, is not accessible or lacks credibility and provenance, then there is little point in devoting resources to its management. Information that has the desired characteristics and can support a specific activity is termed ‘fit for purpose’.

2.12.3 Implementation

This requirement, on first inspection, appears to state the obvious – why would information that is not fit for purpose be created in the first place? Information that is not fit for purpose may arise as the result of a number of reasons. For example, poor planning, a lack of attention to detail or a failure to anticipate future needs. The benefits of good information management planning cannot be over-

estimated. Chapter 3 of this document is devoted to this topic.

The actions of creating information must only be undertaken to address a specific need. It is incumbent on the related process owner to know, or at least anticipate, this need and to clearly state it within the information. Defining the need for which the information has been created is important information that will help a subsequent reader decide on its appropriateness.

The creator must consider the following factors when creating and storing fit for purpose information:

4. Factor	5. Considerations	6. Examples
Intended use	Why is this information being created? What are the anticipated uses of this information? What could the information be used for? Is this information needed to support other information sources? What must this information not be used for?	To support a safety case. To inform a safety committee To enable nuclear materials to be moved in the future To provide an estimate of future requirements arising from a specific activity
Corroborating evidence	Is other information needed to lend credibility or confidence? Is other information needed in order to interpret this information?	For example, inclusion of a specification in the information See below further guidance on information
Format	In what way must the information be presented?	Photograph, spreadsheet, graph, technical report
Accessibility	What can be done to ensure the information is accessible for as long as the information is to be retained?	Information presented in a non-proprietary format
Assumptions	Have any assumptions been made when deriving the information that may impose conditions on its subsequent use?	Based on a specific scenario or model
Skills	What skills or experience does the reader need to interpret and use the information?	A detailed understanding of nuclear physics Ability to 'read' a weld X-ray

During the early stages of, for example, a particular programme, a wide range of information will be produced to meet a variety of purposes. As the programme enters its latter stages, an increase in emphasis is likely to be placed on information relating to compliance with disposability or long term storage.

Where possible, information should have a clearly defined purpose and be provided in such a way that it can fulfil this purpose. Information 'fitness for purpose' will be influenced, and in some cases determined, by the following criteria:

- Origin – is the source of the information reliable and appropriate?
- Accuracy – what is the level of accuracy? Is it appropriate?
- Precision – what is the level of precision? Is it appropriate?

- Timeliness – has the information/data been provided at the right time?
- Form – is the information/data presented in an appropriate way?
- Cost – what is the cost, in the long term, of producing the information?

Continuous critical assessment to confirm the need for creating certain information is more likely to reduce the amount of unnecessary and superfluous information than measures taken to reduce the mass of information at a later date. Destruction of stored information carries a greater risk of accidental information loss than intelligent production. However, all information must be periodically reviewed and the information fitness for purpose can be assessed at this time.

2.13 Information Management after End of Retention

2.13.1 Requirement

Organisations must implement processes for reviewing information to ensure that retained information is accessible or is transferred to an organisation responsible for its preservation

2.13.2 Reason

A clearly defined system must be put in place to ensure important information is retained and accessible. A certain amount of information may be of value even after its retention period has been concluded. For example, historians or researchers may be grateful for the retention of some information.

Decisions about the fate of information must be made in consultation with regulators, the appropriate Government departments and agencies and any organisation responsible for national records and archives. Such decisions have been documented in the NDA's Records Retention Policy, where a requirement to 'Review at the end of the retention period' determines whether this action is required.

2.13.3 Implementation

Records Managers must implement a system for reviewing and, where appropriate, retaining or transferring information once it has reached the end of its retention period. Records Managers must use the NDA's Records Retention Schedule to determine whether particular information needs to be reviewed.

It is anticipated that Nucleus (the Nuclear and Caithness Archives) will have an increasingly influential role in overseeing, at the very least, this integrated approach to the long term management of information. In the meantime, systems must be developed, in close cooperation, to ensure that the appropriate information is retained.

It is expected that some consolidation of the information will be undertaken. There will be a number of reasons for consolidating information, including:

- cost of retaining information;

- the need for appropriate facilities to store the information;
- the likelihood that there is unnecessarily duplicated information in existence;
- there being no known requirement to retain this information separately.

Where appropriate, information must be prepared for long-term retention. This may mean transferring information onto more appropriate media and re-locating information.

Where information is to be transferred to Nucleus (the Nuclear and Caithness Archives) a number of actions need to be undertaken to ensure that a managed transfer is achieved. The following actions need to be completed prior to a transfer:

- ensure that the appropriate metadata (see 2.5.3) is transferred along with the information;
- where vital records (see 2.14) are involved, ensure that the required copies are transferred to the relevant locations;
- where paper / microform records are transferred, ensure that a 'Letter of assurance' that confirms that the records are not contaminated is also transferred;
- ensure that an appropriate manifest of records is also transferred.

Those responsible for preparing records for transfer to Nucleus should reference NUC PRO 0044 Nucleus User Guide and the Transfers of Records for Permanent Preservation to the NDA Archive Facility Procedure which sets out requirements prior to transfer.

2.14 Vital Records

2.14.1 Requirement

Vital records are those that, regardless of storage media, are essential to the organisation in order to continue with its business-critical functions

2.14.2 Reason

Within the nuclear decommissioning industry, it is widely agreed that the term 'vital record' is applied to information relating to radioactive materials, their quantities, characteristics, properties, location and containment. This is justified by the nature of the materials involved. The loss, for example, of information relating to the contents of a particular drum of radioactive materials could result in the need to re-characterise the contents of the drum which could prove very costly, both in monetary terms and in a loss of confidence in the industry and could result in exposure to radiation.

Other information could be classified as vital records, should the industry agree that the appropriate controls are necessary for their management.

2.14.3 Implementation

Creation

Organisations responsible for the management of radioactive materials (and other processes where information has been classified as 'vital') must ensure that the appropriate information is being created, and that its content is accurate and verifiable.

Management

Within 1 month of creation or amendment of information that has been classified as a vital record, the following requirements must have been completed:

- At least 3 copies of all vital records must be retained; the information content of each copy must be identical;
- Each copy must be stored at a different location, and each location must be physically remote from each of the other locations (such that an incident of any kind at one location will not affect either of the other locations);
- At least one copy must be stored in an electronic format. Non-electronic copies could be as follows:
    - In paper format, where archival paper compliant with ISO 11108[3] is used. The paper must be stored in facilities compliant with the BSI publication PD5454 [14];
    - In microform format (e.g. microfilm, microfiche) that has been created and stored in compliance with BS 1153[4];
    - In any other format approved by the NDA.
- Where at least one copy is retained in an electronic format, then the format must be one where long term access to its authenticated information content is assured. The PDF/A format (BS ISO 19005) is approved for this purpose (see 2.8.3).

Procedures for the creation of copies of vital records need to be such that the information content is preserved and the authenticity of the copy can be demonstrated. Copies of vital records can be created during the following processes:

- Moving an electronic copy from one storage media to another;
- Converting an electronic copy into another format;
- Converting (usually by scanning) a paper document into an electronic and/or microform form;
- Copying a paper document to another paper document.

Destruction

[3] ISO 11108:1996 *Information and documentation -- Archival paper -- Requirements for permanence and durability*

[4] BS 1153:1992 *Recommendations for processing and storage of silver-gelatine-type microfilm*

Vital records must only be destroyed and/or moved to a long term archiving store in compliance with the NDA's Record Retention Schedule, unless otherwise agreed with the NDA.

2.15 Media Conversion Projects

2.15.1 Requirement

Information (including metadata) needs to be safeguarded, especially where storage media is changed

2.15.2 Reason

From time-to-time, perhaps as a cost saving exercise or to guard against media degradation, the media upon which information is stored will need to be changed. Examples of such 'media migration' are from paper to electronic (using scanning technology) or from CD to network server (using electronic transfer tools).

Media migration projects must only be undertaken where an objective is the destruction of the original media. In these circumstances, the information on the new media needs to be authentic and its integrity needs to be able to be demonstrated.

Before commencing media migration projects Nucleus should be contacted to check requirements as outlined in their specification documentation.

The NDA has a mandate to build a collection of records relating to the development of the UK's nuclear energy programme. This goes hand-in-hand with the statutory obligation to manage public records and make them available to the public and the nuclear community. There are significant quantities of paper based information concerned with the history, development and decommissioning of the UK's civil nuclear industry since the 1940s. As it can be difficult to give access to these materials, the NDA sees digitisation as a way to maximise the use of these materials, and thus encourages the current custodians of these materials to engage in such a programme.

2.15.3 Implementation

All media conversion projects (including the conversion of paper based documents to electronic images) must be demonstrably compliant with BS 10008:2014 [18]. This requires a number of processes to be in place, including;

- project plan for the media migration;
- appropriate technology and procedures to be in place;
- required level of documentation of the migration process;
- suitable audit trails and metadata to enable demonstration of compliance;
- sign-off by the information asset owner of the process.

Should a digitisation programme be demonstrably compliant with BS 10008, then there is the

possibility of approving a policy for the destruction of the paper originals, once the quality and security of the electronic images has been confirmed. Where document scanning is implemented, unless otherwise agreed, electronic images must be stored in PDF/A(1b) format. The implementation of Optical Character Recognition (OCR) techniques within the PDF/A (1b) is required, such that document content can be automatically searched.

CHAPTER 3 - MANAGING EXISTING INFORMATION

3.1 Understanding the Scale of the Challenge

3.1.1 Requirement

Organisations must adopt a management approach that enables them to understand the scope, content and volume of information retained

3.1.2 Reason

The UK civil nuclear industry has been creating information for over sixty years. In some of these instances, this information will not be separately and appropriately catalogued. Information has been managed to a range of standards, using a variety of approaches. There is a wide range of storage media in use, a lack of suitable long term storage facilities and a mass of superfluous information. The risk of losing information is high and must be mitigated. Existing information must be managed consistently to ensure valuable information remains accessible. However, we must accept that there is a limit to what can be done to older information to improve fitness for purpose.

Organisations must establish a programme for reviewing existing information, identifying those that contain important information and determining the need to adopt more stringent approaches to ensure the information remains accessible over the long term.

3.1.3 Implementation

For some organisations, it may be necessary to launch a ‘one-off’ project to identify all information held. This has the potential to be a significant undertaking for which additional resources may be required over and above those normally allocated to day-to-day records management.

Old information (circa pre-1980) will be largely paper-based and there may even be a significant amount of information recorded on photographic film (microform). Much of this information will not have been created to the standard we would expect today and the storage media (especially paper) may have started to degrade (fading, yellowing, tearing). It needs to be remembered that a high proportion of this information will contain important content (plant operation details, construction and manufacturing records, radioactive material accumulation) that will be needed to manage radioactive materials in the latter stages of their lifecycle, for example.

Ironically, information created between about 1980 and 2000 could be some of the most vulnerable in terms of information loss. It was at this time that new and high volume digital storage media, such as 5¼" and then 3½" ‘floppy’ disks, were widely used. But due to their physical frailties and the increasing difficulty in sourcing disk drives, there is a particular priority to review and migrate the information stored on these vulnerable types of media. In many cases, the need to migrate this information will be greater than that which is 30 or 40 years old and stored on paper and microforms.

The risk of loss of the content contained in old information is in general greater, because the current custodian and information asset owner may be unfamiliar with it. The time and energy required to review old information and make an informed decision on their fate does sometimes result in high risk strategies being adopted – this can range from deliberate destruction of the information to its transfer to a store where they become someone else's problem (out of sight, out of mind). Those responsible for information management (such as the SIRO) must be aware of the risks associated with old information and ensure that they are reviewed prior to a decision being made on their future.

The first step in managing existing information is to determine the size of the challenge. The organisation must have a clear understanding of the number, location, form and type of the information for which it is responsible. It is expected that such a project would be led by the Records Manager. The following steps are suggested:

- identify the information – confirm location, responsible persons, type;
- asset register – unless it already exists and can be relied upon it will be necessary to produce a comprehensive and complete list of the information with the assistance of current custodians;
- media check – confirm the storage media used, assess vulnerabilities, assess existing damage, check there are means for access to the information content;
- storage arrangements – check suitability of storage arrangements and that they are consistent with the storage media used;
- access – confirm arrangement for physical access to the information;
- costs – determine the likely costs (financial and time) of reviewing and, where applicable, preparing important information for a further period of retention.

The management approach to existing information will, initially, be different to that used for new information. However, the aim should be to align the management of all information with an emphasis on fitness for purpose, clear ownership and accessibility.

The review of existing information is clearly of great importance, given the penalties if important information is lost due to neglect. An example of a generic approach to the review of information is illustrated below. The principal challenge for those managing existing information is making an informed judgement of the value, relevance and significance of each piece of information, especially when it is not possible to consult the originator. Experience tells us that the standard of old information varies and, generally, the older they are the more difficult they are to review - particularly if the purpose of the information is not clear or it cannot be directly linked to a specific process.

3.2 Managing Short, Medium and Long Term Information

3.2.1 Requirement

The approach adopted for the management of existing information must take into account the fact that some information will have a longer retention period than others

3.2.2 Reason

Frequently, reference is made to 'long term' information. Whilst some information needs to be retained for a long time to support, for example, a variety of radioactive materials processing management activities and decisions, not all of it will have to be retained for the 'long term'. Some information need only be retained for a relatively short period of time, after which they can be discarded and destroyed. The management approach must help Records Managers decide how long each piece of information needs to be retained.

3.2.3 Implementation

The resources needed to retain information in an accessible form must not be underestimated. If information is to be retained for many decades, the resource commitment could be considerable. Not only are the logistics going to be demanding, so too is the transfer of knowledge needed to undertake a meaningful review of the information. Treating all information as having an identical retention period is unsustainable and it is possible that some important information will be lost if an unsustainable system breaks down. When developing an approach to the management of existing information, organisations must consider how the Records Manager will be guided to determine the appropriate retention period.

There are no universally accepted time periods that define 'short', 'medium' and 'long term'. However, to enable the development of an appropriate management approach, the following time periods should be taken as indicative:

- short term – up to five years;
- medium term – five to thirty years;
- long term – in excess of thirty years.

Sometimes, legislation will provide a clear requirement for the retention of information which is different to the 'operational' needs. For example, site licence condition 6 (LC6) requires some information be 'preserved' for a period of 30 years, reflecting the requirements of the Nuclear Installations Act 1965 (NIA65). In some instances, conflicting legal / regulatory requirements will exist. In this case, an appropriate records management approach will need to ensure the longer of the retention periods is adhered to.

In order to advise on the requirements for retention periods, the NDA has developed and published their NDA Record Retention Schedule. This schedule was developed with input from the Records Managers and other records professionals of the SLCs and subsidiaries. For each record, a trigger and retention period is defined, with the trigger defining when the retention period starts. The action to be taken at the end of the retention period (such as 'destroy' or 'transfer to Nucleus (the Nuclear and Caithness Archives) is defined. To help all participants to understand where this information is derived from, a reference to existing legislation / regulation is given for each subdivision, along with a note of the retention periods from that legislation / regulation where stated. The Schedule also states

which information is:

- to be treated as 'vital records' (see 2.14);
- required for demonstrating compliance with the Nuclear Site Licence Conditions (NSLC);
- required for the Compensation Scheme for Radiation Linked Diseases (CSRLD);
- required for demonstrating compliance with the environmental regulations.

SLCs and subsidiaries are required by the NDA to comply with the minimum retention periods stated in the Schedule. The Records Manager is responsible for ensuring the retention periods are implemented. In most cases it may be difficult to predict future needs so they must be deduced as far as possible. The Records Manager must also consider the likelihood that information is linked to another SLC or subsidiary and that information may be 'mutually supporting'. Where this is the case, the link must either be retained or the Records Manager must be satisfied that destruction of information will not compromise other information.

Information retained only for the short term is unlikely to result in significant storage challenges although some digital media might be vulnerable after about five years. The volume of information created may contribute to more practical challenges.

Information retained for the medium term should be located in a dedicated and purpose designed store or archive. Ideally, a duplicate set of information should be produced if the information is to be frequently accessed – this will reduce general 'wear and tear'. Duplicate sets of information should be stored in different locations and preferably using different storage media.

Information retained for the longer term should be transferred to Nucleus (the Nuclear and Caithness Archives) here it will be stored in an environment which ensures the integrity of the storage media. Access to this information is restricted where appropriate. However, it will still be necessary to periodically check the information and to review the information content. Placing information into archives does not relieve the custodian of its management necessarily.

Actions necessary to manage existing information include:

Short and Medium Term Information

- produce an information asset register (IAR);
- develop and implement a management plan for the preservation of all information;
- identify information where there is a risk of information loss and implement corrective actions.

Long Term Information

- produce an information asset register (IAR);
- develop and implement a management plan for the preservation of all information;
- identify information where there is a risk of information loss and implement corrective

actions;

- review information storage arrangements and confirm conditions meet these defined minimum standards;
- ensure the ability to access information is retained for as long as necessary;
- identify source of funding for records management and ensure the commitment is recognised in long term plans;
- ensure effective processes in place to formally transfer responsibility of long term information to Nucleus (the Nuclear and Caithness Archives).

The range and quantity of information means that it is impossible to describe a single generic approach that will suit all needs. What is important, however, is that the management approach takes into account the inequality of information and their information content - anticipated longevity is one factor that must be considered.

3.3 Reviewing Existing Information

3.3.1 Requirement

Existing information must be reviewed and the conclusions used to inform the management plan

3.3.2 Reason

All information (or, at the very least, a representative sample) must be routinely reviewed. The ongoing need to retain the information must be assessed – particularly where more recent information is available.

Reviewing existing information is essential to:

- maintain knowledge of the information;
- ensure the information remains accessible;
- consolidate information where possible;
- remove information that is no longer required to support current or future operations.

3.3.3 Implementation

The approach is broadly the same for each information type with the possible exception that the retention of some of the information may be necessary to assist in the transfer of knowledge and

other strategic requirements. It is likely that some information will be retained longer than other information as it is needed to aid interpretation and because it has a 'social value' outside routine operations.

An approach for the review of existing information must be developed locally. Most organisations will have an established records management system which must include information reviews. The complexity of the information and the potential for very long retention times may mean that a variation to the normal information review approach is adopted.

Information held must be reviewed to determine whether:

- the type and quantity of information is accurately recorded;
- the scope of information held is relevant to the operations undertaken by considering:
    - is it of purely historical interest only?
    - is it needed to manage the operations in their current form?
    - will it be needed when transferring it to another custodian?
    - will it be needed to support further processing (including treatment or re-packaging)?
    - will it be needed to manage the disposal processes?
- there is a clear purpose for the information;
- the information is complete:
    - all elements are clearly documented:
    - metadata;
    - assumptions, uncertainties, estimates, models;
    - links to other sources.
    - gaps in the information are identified
- the information is fit for the intended purpose;
- there are any access requirements or restrictions;
- there are any emerging threats that may result in information loss;
- likely costs of migrating the information to an alternative media;
- information has been superseded by more recent or fit for purpose information.

Routine information review is a critical part of information management. It must not be regarded as an 'optional extra' when the resources allow.

3.4 Controlled Migration of Information

3.4.1 Requirement

> The migration of important information must take place only using an approved process that includes appropriate controls

3.4.2 Reason

Information retained for a long period of time may have to be migrated onto alternative storage media so that it remains accessible. For example:

- there may be a need to retain more than one copy of the information;
- there is potential or actual degradation of the existing storage media;
- to reduce the threat of information loss;
- to improve information accessibility, particularly over the medium and long term.

Migration must be carried out as part of a planned and controlled process. This process will include testing access to the new information. A separate audit log must be kept within the records management system giving details of the migration.

3.4.3 Implementation

The term 'controlled migration' is used to distinguish the formal process of migration from simple duplication. Controlled migration will result in the creation of new information that contains identical information to its source. The process is to be used where the need to maintain access to information is expected to exceed the useful lifetime of the storage media.

A controlled migration process must include the following steps:

- confirm how long the information must remain accessible;
- determine the need for, and frequency of, access to the information;
- select a media that is compatible with the information to be stored and is cost effective;
- manage the replacement media;
- similarly, ensure the knowledge and infrastructure is in place to enable recovery of the information - this is particularly important for digital media;
- ensure all equipment used is clean, free from contamination and has been tested;
- retain the source information until the migrated information has been tested and proven to

be accessible in all respects;

- take action to update links to other information sources – this is particularly important in digital information management systems;
- create a migration log or an addition made to the information metadata;
- formal acceptance of the migrated information by the appropriate IAO.

Specific actions for the most commonly used storage media, paper and digital, must include:

- For paper-based information:
  - ensure raw materials are compliant with recognised manufacturing standards – this includes the paper, additional filing materials and inks (see Appendix 2 for current standards);
  - handle raw materials and equipment with care and preferably using lint-free gloves to avoid contamination;
  - if photocopying equipment is used, ensure the equipment is clean and all traces of chemical agents, oils and fluids are removed from surfaces that are likely to come into contact with the paper;
  - if a printer is to be used to transfer the information from a digital source, ensure the printer is clean and all traces of chemical agents, oils and fluids are removed from surfaces that are likely to come into contact with the paper;
  - conduct operations in a clean and pollution-free environment;
  - after printing/copying, test adhesion of the ink on the paper by rubbing a finger across the information;
  - ensure the text, drawings, images are clear and there is no loss of detail or perceptible reduction in resolution;
  - ensure every document is complete and no pages are missing;
  - ensure the information is re-assembled in the same way as the source.

- For digital-based information:
  - ensure raw materials are compliant with recognised manufacturing standards (Appendix 2) – this includes the storage media itself and any other materials used to mark or label the media (if applicable);
  - handle raw materials and equipment with care and preferably using lint-free gloves to avoid contamination;

- conduct operations in a clean and pollution-free environment;
- ensure the text, drawings, images are clear and there is no loss of detail or perceptible reduction in resolution;
- ensure any imbedded macros or algorithms continue to work, if this is the intention;
- ensure every document is complete and no pages are missing;
- ensure the information is re-assembled in the same way as the original.

For other information, for example that stored on microforms, the same principles of controlled migration apply. Testing migrated information will be very similar to that performed on paper-based information.

3.5 Managing the Volume

3.5.1 Requirement

Organisations must develop and implement a procedure for managing the volume of information

3.5.2 Reason

Retaining all information for an indefinite time is neither practical, affordable or desirable. Finding a particular piece of information will become increasingly difficult and the task of reviewing information will soon become overwhelming. It is inevitable that as it becomes more difficult to find a piece of information, confidence in its provenance and fitness for purpose will ensure the entire information management system falls into disrepute. Custodians of information must therefore implement a procedure that controls the volume of information held.

3.5.3 Implementation

One of the greatest challenges after sixty years of operation is managing the volume of information being stored. Doing nothing is not an acceptable approach as there are high risks of information devaluation and loss. The volume of information must be managed and a staged approach should be considered. The following stages provide a starting point for developing a procedure:

- Stage 1 - register
- Stage 2 - review
- Stage 3 - consolidate
- Stage 4 - condense
- Stage 5 - compact
- Stage 6 - migrate

- Stage 7 - dispose

The volume of information can only be managed if the extent, scope, provenance and location of all the information are known. Previously in this document, reference has been made to the importance of having an IAR (see 2.6.3). The significance and value of the information is such that an unmanaged programme of volume reduction could result in an increased risk of information loss. Reference to the IAR must be part of any volume reduction programme.

Section 3.3 explains the importance of the information review process. When implemented, the review process is likely to identify information that is no longer required or that has been superseded. All records management systems must incorporate information review processes.

The next stage must be to consolidate information. The objective of this stage is to bring together all similarly themed information and reduce unnecessary duplication. This stage requires not only knowledge of the subject matter, but also the scope, content, ownership and location of the information itself. If information is to be brought together into, say, a single information set it is important to know what can be left out and what must be retained to maintain fitness for purpose. Metadata plays an important role in 'signposting' consolidated information.

The fourth stage is to condense as much of the information as possible. Again, knowledge of the subject matter is important. The objective of this stage is to reduce the volume by removing any information that is superfluous, of unknown provenance, dubious quality and fitness for purpose.

The next stage is to identify opportunities where information might be compacted. This stage is particularly relevant to digitally-based information where it is quite common to use software applications that 'zip' files. The technique is certainly proven but there is a risk that data will be lost if the complex algorithms that allow compacted data to be 'unzipped' are not retained. It should be noted that there is a small risk of corruption when zipping and migrating digital information. Any corruption of the algorithms may render the entire file inaccessible. The risk is such that compaction is not recommended for information of significant importance.

Stage 6 is the migration of information onto higher capacity media. In most cases, migration will only be considered practicable for digital information. DVDs and solid state memory now offer high storage volumes that were not available just a few years ago. The majority of electronic information will be stored on magnetic 'spinning disk' media (the NDA preferred option), which itself is increasing in capacity and reducing in terms of cost per Gb. However, as the volume increases, so does the risk of loss of significant amounts of information. It is possible to use migration as a technique for hard-copy based information but these are less common. Typically, an increase in information volume is the result of size reduction. For example, the Japanese nuclear industry has developed a process where it is possible to scan and laser etch up to 12 A4 pages of text onto a silica carbide plate measuring $10cm^2$. This technique is unlikely to be adopted in the UK in the near future.

The last stage in a process for reducing the volume of information is its disposition. This must only be considered after completing a review of the information concerned and when all the previous stages have been undertaken or are impractical. Only information that is of no future value should be destroyed. A record of all information destroyed must be made and retained in accordance with a defined retention policy.

In summary, the management of existing information is a significant undertaking and it may take many years to review, collate, condense, migrate and store this information to an acceptable standard. However, non-intervention is not an option and is unlikely to be cost-effective in the long term. Organisations must retain sufficient resources to manage information and resist the apparent financial benefits of arbitrarily reducing the quantity of information or the staff responsible for their oversight. Information is an asset that must be safeguarded for as long as it is likely to be needed, which could be for many decades or indeed centuries.

3.6 Storage

3.6.1 Requirement

Information must be stored in appropriate locations, depending upon their age, retention period, storage media type and access requirements

3.6.2 Reason

Retaining all information for an indefinite time on the operational site is neither practical, affordable or desirable, particularly bearing in mind the process of decommissioning. Deciding upon a suitable location for storage will depend upon a number of factors, including:

- Retention period;
- Age of information;
- Media type;
- Access requirements;
- Cost of storage;
- Required security arrangements.

The objective must be to store information in a secure location where appropriate access is guaranteed and at a minimum cost.

3.6.3 Implementation

Information can be classified according to the following generic types, based on access requirements:

- Active – required for quick access and so stored in an operational environment;
- Semi-active – required on a less frequent basis to active information and where access times are less critical. These are frequently stored 'on-site' in an information store;
- Inactive – required to be stored but are not required 'on-site' for access purposes (sometimes these are called 'archived information');

- Historical – no longer within their retention period, but important for historical, social and/or research purposes.

Typically, SLCs store physical information in operational areas, in on-site information stores or under third party contracts off-site. Nucleus (the Nuclear and Caithness Archives) is now operational and the following procedures must be adopted:

- Active – stored on-site in operational areas or in on-site information stores;
- Semi-active and inactive information not required 'on-site' must be transferred to Nucleus (the Nuclear and Caithness Archives) This information may remain under the management of the relevant SLC or subsidiary;
- Historical information must be transferred to Nucleus (the Nuclear and Caithness Archives) and stored in compliance with the archives Retention Schedule. This information is transferred to the full responsibility of the archive. N.B. NDA governance records, selected for permanent preservation will be transferred to The National Archives (TNA), Kew

Where information is held in an electronic form, often they are stored on local systems (such as stand-alone PC's), network servers or physical media (CD/DVD or other mass storage devices). For effective management, and to reduce operational costs for SLCs, an 'electronic archive' will also be made available based on an Electronic Records and Document Management System (EDRMS). This must be used in the same manner as the physical archive for the storage of semi-active and inactive information.

CHAPTER 4 - MANAGING NEW INFORMATION

4.1 Planning for Information Creation

4.1.1 Requirement

Information management is a planned activity and opportunities to create and manage information must be identified early in the process design

4.1.2 Reason

Opportunities for obtaining the information needed to manage operations in the future may be limited and costly. In the same way that other elements of a major project are considered in detail in advance of implementation, information creation and management must be planned. The consequence of poor information management planning can include increased costs when having to undertake additional work at a later date to create missing or inaccurate information.

4.1.3 Implementation

Information management is a planned activity that must be considered in the early stages of project planning. The responsibility for highlighting the need to plan for information management will generally rest with the Project Manager.

An information management plan must be produced, ideally, in advance of the operation of any process. This will help identify opportunities for creating information well in advance of the event and ensure the necessary resources are in place. Clearly, it would be unreasonable to expect all information creation opportunities to be identified in advance, so the Project Manager would regularly update the plan as the project progresses.

The information management plan must contain the following, as a minimum:

- the process identifier;
- the information to be collected;
- method to be used to obtain the information (for example, measurement, estimate, fingerprint sample);
- the optimum time to collect the information;
- the person/group responsible for collecting and managing the information;
- file naming conventions;
- the storage media and format.

Where the information capture process is likely to be complex or costly, procedures must be written and referenced in the information capture plan. Information management procedures will:

- contribute to information consistency;
- help identify risks, constraints, costs, resource requirements;
- provide a reliable reference and, potentially, other information;
- help assess quality assurance features.

The Project Manager, in consultation with others, must make the first attempt at listing the information needs before operations start.

CHAPTER 5 - TRANSFER OF INFORMATION MANAGEMENT RESPONSIBILITIES

5.1 Transferring Responsibilities

5.1.1 Requirement

> A system must be established and implemented to control the formal handover of information and transfer of responsibility for their ongoing management

5.1.2 Reason

A process and the information about it must not be separated. This does not mean that the information needs to be physically co-located with the process, but that the relevance of the association must be clearly understood and appreciated. During every phase of the process lifecycle, the information must be physically transferred to its new custodian.

For example, where the processing and disposal of radioactive waste is involved, it is expected that the organisation operating the processing and disposal facility will be responsible for the management of information about the waste. Once the waste has been successfully disposed of, any remaining information is expected to be transferred to Nucleus (the Nuclear and Caithness Archives)

5.1.3 Implementation

One of the greatest threats to information loss occurs when a transfer of responsibility for that information takes place. A recipient may not be aware of the significance or importance of the information and therefore not implement a sufficiently robust management approach which offers the appropriate protection.

The primary responsibility for ensuring the right information is created and managed and that the information is accessible will be with the custodian of the process. The exception to this is the management of some information which is a combined responsibility for all stakeholders.

Continuing the example from 5.1.2, when radioactive materials are transferred to another custodian; it is the responsibility of the consignor to establish a system whereby the information is transferred. The recipient must work closely with the consignor to ensure all appropriate information is transferred accurately and it continues to be accessible after the transfer.

APPENDIX 1 – List of Requirements

Req No.	Requirement
2.1	Organisations must develop corporate policies for managing information
2.2	Organisations must ensure that suitably qualified and experienced people are appointed to key information and knowledge management roles and that those appointed understand their duties
2.3	Organisations must be able to demonstrate that they can implement a proportionate level of control in their information and records management activities, consistent with the principles set out in a recognised management system standard such as BS/EN/ISO 9001 [9]
2.4	The threat of unplanned degradation, alteration and loss of information must be identified and action taken to minimise the risks as far as practicable
2.5	All information must have associated metadata
2.6	Actions must be taken to ensure information remains physically accessible to those who need it and for as long as it is needed to perform relevant management activities
2.7	Actions must be taken to ensure that information remains accessible to those who need it and for as long as it is needed
2.8	The appropriate media and format must be used for storing information, ensuring that integrity can be maintained and the information accessed at any time
2.9	Information must be stored and maintained in such a way that its physical integrity is preserved and the information is accessible until a decision is made that it must be destroyed
2.10	A register (IAR) of all information held must be maintained and regularly published
2.11	There must be a process implemented for the routine review of any information created in support of the processes undertaken. The review is concluded by a decision to either retain the information 'as is', transfer the information to alternate storage media, transfer to archives or destroy
2.12	Information must be created and recorded in such a way that it is capable of supporting the need for which it was intended
2.13	Organisations must implement processes for reviewing information to ensure that retained information is accessible or is transferred to an organisation responsible for its preservation
2.14	Vital records are those that, regardless of storage media, are essential to the organisation in order to continue with its business-critical functions
2.15	Information (including metadata) needs to be safeguarded, especially where storage media is changed

Req No.	Requirement
3.1	Organisations must adopt a management approach that enables them to understand the scope, content and volume of information retained
3.2	The approach adopted for the management of existing information must take into account the fact that some information will have a longer retention period than others
3.3	Existing information must be reviewed and the conclusions used to inform the management plan
3.4	The migration of important information must take place only using an approved process that includes appropriate controls
3.5	Organisations must develop and implement a procedure for managing the volume of information
3.6	Information must be stored in appropriate locations, depending upon their age, retention period, storage media type and access requirements
4.1	Information management is a planned activity and opportunities to create and manage information must be identified early in the process design
5.1	A system must be established and implemented to control the formal handover of information and transfer of responsibility for their ongoing management

APPENDIX 2 – Storage Media Manufacturing and Storage Standards

The following is a list of International and British Standards relevant to the selection of storage media and information management strategies. These Standards should be implemented where applicable.

Paper

- BS EN ISO 9706:2000 Paper for documents – Requirements for permanence
- BS ISO 11108:1996 Archival paper – Requirements for performance and durability
- BS ISO 11798:1999 Information and documentation – Permanence and durability of writing, printing and copying on paper – Requirements and test methods

Film

- BS 1153:1992 Recommendations for the processing and storage of silver-gelatine-type microfilm

CD/DVD Testing for Long Term Integrity

- ISO 10995:2011 Information technology – Digitally recorded media for information interchange and storage – Test method for the estimation of the archival lifetime of optical media
- ISO 29121:2013 Information technology – Digitally recorded media for information interchange and storage – Data migration method for DVD-R, DVD-RW, DVD-RAM, +R, and +RW discs

Storage of Media

- ANSI/PIMA IT9.23:1998 American National Standard for Imaging Materials – Polyester base magnetic tape – Storage practices
- ANSI/PIMA IT9.25:1998 American National Standard for Imaging Materials – Optical disk media – Storage
- ISO 18921:2008 Imaging materials – Compact disks (CD-ROM) – Method for estimating the life expectancy based on the effects of temperature and relative humidity
- ISO 18925:2013 Imaging materials – Optical disc media – Storage practices

APPENDIX 3 – Information Risks and Information Access Comparisons

7. Recording Medium	Comparative Information Capacity[3]	Risk of Information Loss[4]	Comparative Ease of Locating Specific Information[5]	Comparative Ease of Accessing Information[6]	Typical Review Frequency[7] Needed to Confirm Accessibility	Typical Information Migration Frequency[8]	8. Comparative Risk Resulting from Technology Change
Office Paper[1]	Low	Medium	Difficult	Medium	10 years	<50 years	Very Low
Archive Paper	Low	Medium	Difficult	Medium	10 years	<100 years	Very Low
Photographic Film	Medium	Medium	Difficult	Medium	10 years	100+ years	Low
Solid Substrate[2]	Medium	Medium	Difficult	Medium	10 years	1000 years	Low
Magnetic Disk	Medium	High	Easy	Difficult	5 years	5 – 10 years	Very High
CD/DVD	High	High	Easy	Difficult	5 years	10 years	Very High
Network Server	Very High	Medium	Very Easy	Difficult	5 years	10 -20 years	High

Low Risk/Positive Outcome Medium Risk/Manageable High Risk/Undesirable

1. 'Office Paper' is very often a product of recycling and may therefore contain materials that will shorten its useful lifetime
2. For example laser etched silicon carbide tiles
3. A rough comparison of the amount of information that can be stored on one entity, i.e. one page, one disc
4. This is the relative risk of not being able to find specific information. The risk can be significantly reduced if the records management system incorporates a regularly updated and comprehensive information asset register
5. An indicative measure of how easy it might be to find a piece of information. Hard copy information requires a person to read the text and find, by sight, the required information. Digital information can often be accessed by an application that can search for defined text or patterns, making the search fast and accurate.
6. An inactive measure of how easy it is to assimilate the information. For hard copy based information the reader would have to be familiar with the language used. For digital information the software application has to locate the information, read the binary digits, convert the bits into human readable symbols and then display the symbols. Clearly, for digital information there are vulnerabilities in the information coding, the storage media, the hardware used with the storage media and the software used to read the information.
7. This is an indicative frequency that the information should be examined and retrieval (and conversion, where necessary) of the information is tested

This is an indicative frequency for transferring information to a replacement system to avoid information loss resulting from format / media degradation

APPENDIX 4 – References and Bibliography

A4.1 References

1 NDA Policy on radioactive waste information management – LL12105309 (accessed 12th August 2014)

2 Regulators' Joint Guidance on managing radioactive waste records and information – February 2010 http://www.hse.gov.uk/nuclear/wastemanage/rwm-part3d.pdf *(accessed May 2017)*

3 Technical Assessment Guide - Licensee management of records NS-TAST-GD-033 – Revision 4 http://www.onr.org.uk/operational/tech_asst_guides/ns-tast-gd-033.pdf *(accessed 12th August 2014)*

4 IAEA Publications - http://www-pub.iaea.org/MTCD/publications/publications.asp *(accessed 12th August 2014)*

5 Managing Digital Records Without an Electronic Record Management System – The National Archives 2010 http://www.nationalarchives.gov.uk/documents/managing-electronic-records-without-an-erms-publication-edition.pdf *(accessed 12th August 2014)*

6 Guidance on Mandatory Roles (AO, SIRO, IAO) – The Cabinet Office October 2013 http://webarchive.nationalarchives.gov.uk/20130128101412/http://www.cabinetoffice.gov.uk/media/45149/mandatory_roles.pdf *(accessed 19th August 2014)*

7 NDA Information Governance Strategy 2013 – http://www.nda.gov.uk/publication/information-governance-strategy-february-2013/ *(accessed 12th August 2014)*

8 BS EN ISO 9001:2015 Quality management systems — Requirements

9 The National Archives Guidance http://www.nationalarchives.gov.uk/recordsmanagement/dc-about.htm *(accessed 12th August 2014)*

10 e-Government Metadata Standard — Cabinet Office — Version 3.1 29 August 2006 http://www.nationalarchives.gov.uk/documents/information-management/egms-metadata-standard.pdf *(accessed 12th August 2014)*

11 ISAD(G): General International Standard Archival Description, International Council on Archives, Second Edition, ISBN 0-9696035-5-X, 2000

12 BS 1153:1992 Recommendations for processing and storage of silver-gelatine-type microfilm

13 BS ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems - Requirements

14 BSI PD 5454:2012 Guide for the storage and exhibition of archival materials

15 WPS/850 Waste Package Data and Information Recording Requirements: Explanatory Material and Guidance

16 Radioactive Waste Management Glossary, International Atomic Energy Agency, 2003

17 Regulations for the Safe Transport of Radioactive Material, International Atomic Energy Agency, 2012, SSR-6

18 BS 10008:2014 Evidential Weight and Legal Admissibility of Electronic Information

19 Government Security Classification Policy April 2014

20 ONR Classification Policy 2017 [as amended]

A4.2 Bibliography

- IAEA-TECDOC-1222 Waste Inventory Record Keeping systems (WIRKS) for the management and Disposal of Radioactive Waste, IAEA June 2001
- IAEA-TECDOC-1548 Retrieval, Restoration and Maintenance of Old Radioactive Waste Inventory Records, IAEA March 2007
- Technical report series 434 Methods for Maintaining a Record of Waste Packages during Waste Processing and Storage, IAEA January 2005
- IAEA-TECDOC-1097 Maintenance of Records for Radioactive Waste Disposal, IAEA July 1999
- IAEA-TECDOC-1398 Records for Radioactive Waste Management up to Repository Closure: Managing the Primary Level Information (PLI) Set, IAEA July 2004
- Risk Management of Knowledge Loss in Nuclear Industry Organisations STI/PUB/1248, IAEA 2006
- BS ISO 23081-1:2006 Information and Documentation – Records Management Processes – Metadata for Records Part 1: Principles
- BS ISO 15489:2016Information and Documentation – Records Management
- BS ISO 11798:1999 Information and Documentation – Permanence and Durability of Writing, Printing and Copying on Paper – Requirements and Test Methods
- BS EN ISO 9706:2000 Information and Documentation – Paper for Documents – Requirements for Permanence
- BS ISO 11108:1996 Information and Documentation – Archival Paper – Requirements for Permanence and Durability
- BS ISO 19005:2005 Document Management – Electronic Document File Format for Long Term Preservation
- BSI PD 5454:2012 Guide for the storage and exhibition of archival materials
- BS ISO 18911:2010 Imaging materials – Processed safety photographic films – Storage practices
- Command 4516 Government Policy on Archives, Lord Chancellor's Department December 1999
- Advisory Material for the IAEA Regulations for the Safe Transport of Radioactive Material,), (Safety Standard Series No. SSG-26) International Atomic Energy Agency, 2012 edition, published 2014 Near surface Disposal Facilities on Land for Solid Radioactive Wastes – Guidance on Requirements for Authorisation EA/NIEA/SEPA – February 2009
- Geological Disposal Facilities on Land for solid Radioactive Wastes – Guidance on Requirements for Authorisation, EA & NIEA – February 2009

APPENDIX 5 - Glossary

Term or Phrase	Meaning
access(ible)	Function of retrieving information, converting it to symbols that can be read and understanding the significance of the symbols (retrieve, convert, and interpret). In this sense, accessibility relates to information. However, access can also relate to the physical recovery of information
control(s)	In a quality management system there are often administrative processes employed to ensure an action has been carried out as intended – for example, a signed declaration is a form of administrative control. Physical controls can also be used, for example, a lock on a door
custodian(s)	Person or organisation that is formally and legally responsible for safekeeping (of, for example, radioactive waste or information)
data	Set of discrete, objective facts about an event
digital records	Records stored in an electronic format that will require processing to make accessible
digital signature	Electronic signature combined with a cryptographic control that enables the authentication and non-repudiation of the signatory
disposition	Range of processes associated with implementing records retention, destruction or transfer decisions which are documented in disposition authorities or other instruments
electronic signature	Electronic means of signing an electronic document – for example by including an image of a handwritten signature within a document
fit for purpose	(Information) that complies with expectations. The term is intended to reflect the fact that 'perfection' is not necessarily a pre-requisite for all information
FLATE	Electronic file compression algorithm, one of the compression methods used in ZIP technology. Not to be used for PDF/A format files
generic risk	Risk that is common in the majority of cases
hard copy record(s)	All physical records including paper, photographic and microform
historical information	Information that is no longer within its retention period, but important for historical, social and/or research purposes
information	Evaluated, validated, or useful data
information asset	Any information owner by an organisation and of value to that organisation

Term or Phrase	Meaning
information asset owner	(IAO) Person responsible for an information asset
information asset register	(IAR) Tool for organising and managing an organisations information assets and the risks associated with them
information governance	Combination of information management, information risk management, knowledge management, information and communications technology and intellectual property used to manage information at a corporate level, supporting the business, legal and regulatory requirements of the organisation
information management system	Way of working that combines people, processes and electronic tools
institutional control	When oversight is applied by a higher executive. For example, Government control and coordination of an important activity or process
intelligibility	Ability to turn recorded information into something meaningful to the user (who may be an individual or a process)
knowledge	Possessed by people, it is the effective combination of information and insight or experience
methodology statement(s)	This is a written step-by-step description of how an action is performed. For example, how the radionuclide content of a waste package is calculated
metadata	Data describing context, content and structure of records and their management through time (BS ISO 30300)
migrate	Transfer or copy information onto another storage media
provenance	Original creator and history of the information
RAID array	RAID (originally redundant array of inexpensive disks; now commonly redundant array of independent disks) is a data storage virtualisation technology that combines multiple disk drive components into a logical unit for the purposes of data redundancy or performance improvement
raw waste	Radioactive waste as created and which has not been treated or conditioned in any way
readability	Ability to recover the recorded information from the medium
record	Information created, received and maintained as evidence and information by an organisation or person, in pursuit of legal obligations or in the transaction of business (BS ISO 15489)
retention schedule	Guidance on how long information needs to be retained. The length of time is usually indicated by the combination of a 'trigger' (e.g. when the retention period starts) and a retention time

Term or Phrase	Meaning
senior information risk owner	(SIRO) Typically a board level member who takes ownership of the organisation's information risk policy
usability	Ability to interpret the information
vital record	Records that are essential to the organisation in order to continue with its business critical functions
waste package record	All the information necessary to identify a waste package and to include full details of its manufacturer, contents, location and condition

APPENDIX 6 - Abbreviations

Abbreviation	Meaning
IAEA	International Atomic Energy Agency
IAO	Information Asset Owner
IAR	Information Asset Register
IT	Information Technology
KM	Knowledge management or knowledge manager
NDA	Nuclear Decommissioning Authority
OCR	Optical Character Recognition
RAID	Redundant Array of Independent Disks
SIRO	Senior Information Risk Owner
TNA	The National Archives

APPENDIX 7 - Government Knowledge and Information Management (KIM) Professional Skills Framework

GKIM Skills Framework Overarching	 GKIM Skills Framework Overarchi
GKIM Skills Framework Information Architecture Role	 GKIM Skills Framework Informatic
GKIM Skills Framework Information Management Role	 GKIM Skills Framework Informatic
GKIM Skills Framework Information Rights Role	 GKIM Skills Framework Informatic
GKIM Skills Framework Knowledge Management Role	 GKIM Skills Framework Knowledg
GKIM Skills Framework Library Management Role	 GKIM Skills Framework Library Ma
GKIM Skills Framework Records Management Role	 GKIM Skills Framework Records M

Record Description	Record Owner	Record Format. Electronic/Hardcopy
N/A	N/A	N/A
This document is uncontrolled when printed		