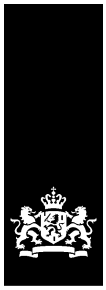

National Archives of the Netherlands
Ministry of Education, Culture and Science

Preservation policy

Contents

1 Introduction

1.1 *Preservation*[1]

The National Archives (NA) defines preservation[2] *as follows:*

> 'the documentation, storage, management and provision of digital documents (in the broad sense of the word) to ensure that they are accessible, authentic and available for consultation in the long term.'

This definition is based on the reference model for an Open Archival Information System Reference Model (OAIS). This standard work defines the frameworks and procedures for storing digital information[3]. *The OAIS was developed in 2002 to list the functional entities required for long-term management and to develop a common terminology for it.*

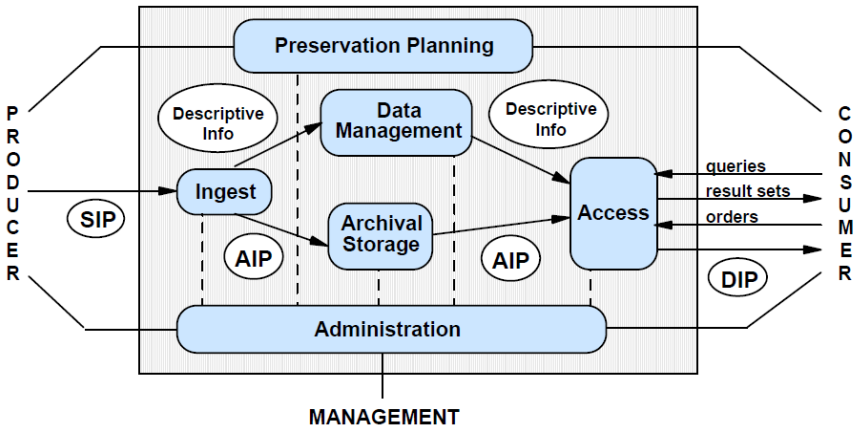

Figure 1: OAIS model

The functional entities are:

- ingest: intake of the data (digital objects and accompanying metadata)
- data management: managing the metadata of the digital objects and conducting checks
- archival storage: storing the digital objects
- administration: coordinating the activities of other functional entities
- preservation planning: planning sustainable management of the digital objects
- access: providing information to users[4]

This model will be examined in greater detail in appendix 4.5.

In addition to these functional entities, preservation revolves around the Information Package. This 'package' consists of two types of information, Content Information and Preservation Description Information (PDI), which are, in turn, encapsulated within the Packaging Information. The result can be seen in the Descriptive Information.

[1] This policy applies the terminology used by the international preservation community and described in the ISO standard ISO 14721 Space data and information transfer systems -- Open archival information system (OAIS) -- Reference model. Appendix 4.1 contains the accompanying list of definitions.
[2] http://www.nationaalarchief.nl/informatiebeheer-archiefvorming/-digitaal-archiefmateriaal
[3] This policy discusses digital information and digital information objects that fall under the Public Records Act, including the entire range of interpretations of archive files, records and digital documents.
[4] http://www.ncdd.nl/blog/?page_id=447, consulted on 22-04-2015

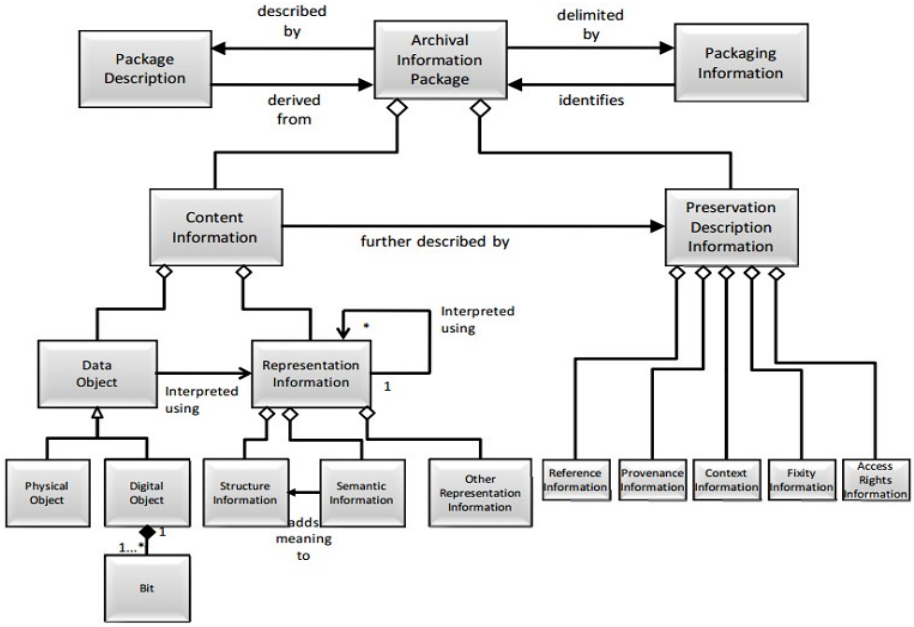

Figure 2: Archival Information Package

1.2 The National Archives

1.2.1 *Challenges*

Digital information objects are diverse in terms of collections, materials, sources and the extent to which record keeping and preservation experts influence the creation of information. Keeping digital information accessible in the long term poses a number of challenges:

- media and technological developments;
- the wide range of software formats and information carriers;
- the exponential growth of digital information;
- the mix of information that must be kept and information that must be destroyed after a period;
- complex information objects in terms of shape, structure, inter-relatedness and dependency;
- providing access to information objects with relevant context information.

1.2.2 *NA's mission*

The policy is in line with NA's mission[5], which states:

"We serve everyone's right to information and provide insight into our nation's past by:

1. working to provide a strong archive system, pursuing a well-considered policy for archive valuation and selection, and taking optimal care of all national archives;
2. managing the national archive collection in The Hague; and
3. presenting archives on-site and online."

1.2.3 *The NA Collection*

The National Archives stores almost 1000 years of Dutch history in the form of 130 km of paper archives, 15 million photographs, and approximately 300,000 maps and drawings. Its archives have been sourced from:

- the central government;
- the county of Holland and the regional/provincial administrative institutions in South Holland;

[5] http://www.nationaalarchief.nl/organisatie/missie, consulted on 17-09-2014

- private institutions and individuals.

The Dutch archive sector considers that it has the responsibility to document not only the actions of the government, but also the interaction between government and society.[6] The current collection encompasses archives that have been collected by both government agencies and within the private domain.

1.2.4 *Objective*

The policy is a policy plan that stipulates the manner in which the NA keeps the digital information that it manages authentic and useable. This policy also sets out the conditions for producers of information and the conditions for links to consumers. Developing a policy enables the NA to shape processes and procedures regarding long-term accessibility. The policy has been shaped within the frameworks of information legislation and regulations, such as the Public Records Act, the Government Information (Public Access) Act, the Personal Data Protection Act and implementation thereof. The NA wishes to be accountable to internal and external stakeholders (directors, employees, clients, citizens, partners, certification bodies) with regard to preservation and to clarify responsibilities within the organization. This will also contribute to creating a support base for preservation both within and outside the NA.

1.2.5 *Scope*

The policy concerns all digital information that is managed by the NA. The NA distinguishes between outsourced and transferred (including digitalized) archives:

- Outsourced archives are archives that have been given into the management of a third party without any change to the custody of and responsibility for the archive. These will remain with the records creator. Outsourced archives consist of closed dossiers whose objects have been stored.
- Transferred archives are archives that have been transferred to an archive repository. Consequently, the Minster of Education, Culture and Science becomes the legal caretaker and management is being transferred to the NA or a Regional History Centre (RHC).

This distinction is of no importance to the preservation functionality, but it may require different functional entities in relation to the destruction of objects, synchronization of metadata and requirements regarding access[7].

This policy is currently limited to the custodial[8] status of the digital archive, i.e. management in one location. In the long term, this policy will be extended, following on from the digital government which assumes variable forms, with non-custodial solutions for sustainable accessibility or preservation in place.

[6] http://www.nationaalarchief.nl/organisatie/over-collectie-het-nationaal-archief, consulted on 10-03-2015

[7] If applicable, this will be elaborated on further in the Products and Services Catalogue.

[8] Appendix 4.1 Definitions

	The Ministry of Education, Culture and Science is the legal caretaker	Other legal caretaker
Physical management at the NA	Example: NA Collection	Example: outsourced information from departments
Physical management elsewhere	Example: process information from implementing body (older than 20 years)	Example: process information from implementing body (as long as it has administrative value)

The NA has a digital facility[9] to manage and make available its own digital information and that of other legal caretakers and records creators. This facility also forms the basis for the Government Digital Workplace (DWR) Archive and the Government Digital Tasks (DTR) programmes whose objective it is to expand the NA facility into a national infrastructure for long-term accessible government information. The NA acts as a service organization within this context[10].

This policy does not concern paper archives that have been transferred up until now to which portable media have been added. The digital curation that is required for this will be part of an integrated approach to processing the digital legacy from the period 1985-2015 and will, if desired, be included in the products and services catalogue (PDC).

1.2.6 *Target group*

This policy has been written for the NA and the collection managers at national level (RHCs) to clarify how preservation is implemented by the NA.

1.2.7 *Accountability, audit and review*

This policy was drawn up by the board of directors of Digital Infrastructure and Advice and coordinated with the board of directors of Collection and Public. This means that this preservation policy is in line with:

- the information policy, including enterprise architecture, connection requirements and links for accessibility;
- the information security policy that ensures that information can only be accessed by authorized persons, including fall-back, back-up, etc.;
- the acquisition policy;
- the open data policy (under construction);
- the archiving policy.

As is the case with other policies, this policy will be revised regularly and developed further as part of the NA's policy cycle and will be audited and reviewed in conformity with the plan-do-check-act cycle.

[9] The NA calls this facility the e-Depot and defines it as "the combination of equipment, software, procedures, methods, knowledge and skills to ensure the ingest, management, preservation and provision of digital objects and metadata in the long term."

[10] Appendix 4.3 Service organization

1.2.8 *Standards*

The NA applies the following standards as a basis for this policy:

- ISO 14721 Space data and information transfer systems -- Open archival information system (OAIS) -- Reference model
- ISO 16363 Space data and information transfer systems -- Audit and certification of trustworthy digital repositories
- 13008:2102 Information and documentation -- Digital records conversion and migration process
- NEN-ISO 23081 Standard for Metadata
- NEN-ISO 15489-1 Information and documentation -- Information and archive management
  NEN 2082 Requirement for functionality of information and archive management in software
- Guidelines for MetaData on Government Information, version 2.5, 15 July 2009

2 Policy frameworks

2.1.1 *Core*

A number of aspects are important when it comes to preservation:

- the information that is supplied;
- the form and structure of the information object;
- the technology used (software and hardware);
- the characteristics added to the information;
- the desired manner of provision.

To sum it up briefly, the preservation policy is about ensuring that digital information objects that fall under the NA's responsibility remain accessible, authentic and available for consultation.

2.1.2 *Responsibilities*

As the manager of digital information objects, the NA has six responsibilities[11]:

1. The NA must make agreements with the Producer, the supplier of the archive material, about the form and manner in which the archive material is to be delivered, preferably by means of a Submission Agreement[12] between the archive institution and the supplier of the material.
2. The NA must draw up a transfer document, in which the intellectual property rights are transferred either in whole or in part to the NA. In case of the latter it will be necessary to specify which rights will and will not be transferred. The NA must be in a position to implement actions to maintain and store the material to ensure that it is accessible in the long term. Permission to conduct these actions must be granted by the Producer.
3. Together with others, the NA establishes the identity of the Designated Community – the envisaged and future user – as this determines the degree of accessibility[13].
4. The NA ensures that users are able to understand and use the information that it has made available without requiring explanation or assistance.
5. The NA draws up and implements processes to prevent damage to and/or the disappearance of archive material. It is strictly forbidden to remove information unless this is part of an approved strategic plan. If the NA should cease to exist, it must take measures to secure the contents.
6. The NA guarantees the authenticity of digital information from the time of ingest. Authenticity consists of three essential characteristics: reliability, integrity and usability[14].

[11] B. SIERMAN. "Het OAIS-model, een leidraad voor duurzame toegankelijkheid." *Handboek Informatiewetenschap*, Vol. 62 (2012)

[12] The Submission Agreement contains agreements about access rights and preservation rights, the time schedule and manner of delivery, and a detailed description of the structure of the SIP to be delivered.

[13] Designated communities: the process of defining, knowledge base (for example Dutch reading, reuse producer, dark archive, historical research)

[14] Appendix 4.2 Other Definitions

2.1.3 *The Framework of legislation and regulations concerning archives*

The Archive Regulation 2009 is important with regard to the final responsibility mentioned: 'Authenticity of digital information'. The NA bases its policy on this Regulation[15], which specifies that in order to keep digital archive documents in an orderly and accessible state, quality requirements apply to:

- the behaviour of digital information objects
- content, structure and visual manifestation
- the functional requirements of the object
- an up-to-date, complete, logical and coherent overview
- identification of all relevant digital files
- link to metadata
- conversion, migration or emulation
- file formats that must be validatable, fully documented and open
- encryption technology
- compression technology

[15] Appendix 4.4 Archive Regulation 2009

3 Implementation of the preservation policy of the National Archives

Figure 3: Preservation in INK

Aim	Design	Implementation		
Leadership ***Preservation Policy*** In relation to information and archive policy, the environment, staff and organization, finances and specific legislation and regulations	**Strategy and policy** **Guiding employees** Training, knowledge development and agreements on the process **Guiding means** Architecture, process organization, preservation strategies and functional management.	**Processes** Acts of preservation Technical and collection management and availability	**Added value for** Consumers and producers Employees Society	**Administration and finance** Lawful management Efficient management

Table 1 - Translation of figure 3

The responsibilities and frameworks based on standards, legislation and regulations will be examined in more detail in this chapter of the policy. The INK management model[16] *will be taken as a reference to distinguish between the three aspects of aim, organization and implementation, the related basic premises and the measures as yet to be taken.*

3.1 Aim

3.1.1 *Application of the OAIS model*

The NA follows the OAIS reference model in the policy and uses it to structure organization.

[16] http://www.ink.nl/. The INK model is the Dutch version of the European Foundation for Quality Management (EFQM) Excellence Model (http://www.efqm.org/the-efqm-excellence-model).

3.1.2 *Quality level of preservation*

Bit preservation forms the basis of the preservation functionality. This means the presence of a bitstream that always delivers a bit-perfect copy. Naturally, the NA opts for this bit-perfect copy but it also ensures that authentic, reliable information is made available in the future, a task which involves more than bitstream preservation.

The NA makes preservation plans using the basic principles to anticipate change, to determine the consequences of these changes and to intervene if there is any threat to the proper, orderly and accessible state of information objects (Just in time).

3.1.3 *Cost model*

The NA provides insight into the costs of preservation by drawing up a cost model. We do this together with NCDD/NDE (National Coalition for Digital Sustainability/Digital Heritage Network). On the basis of this, the NA weighs up the costs of preservation (time and money) against the basic quality of the information.

3.1.4 *Certification*

The NA is starting a certification programme in collaboration with the NCDD/NDE. Certification provides extra recognition as a Trustworthy (Digital) Repository and contributes to the internal quality cycle.

3.1.5 *Continuity*

Even though the existence of the NA and other archival repositories is laid down by law, it is necessary to guarantee continuity, for example by entering into escrow[17] agreements with commercial partners that provide products or services to the NA.

3.1.6 *Open Data*

The NA has an Open Data policy which also contains decisions on intellectual property, licences and waivers.

3.2 Organization

3.2.1 *Connection requirements*

The NA sets connection requirements regarding:

- the technical conditions representing system connections;
- the limitations regarding digital signatures, compression and other technical processing;
- the logical conditions for the interoperability of the metadata;
- the assessment criteria for the sustainability of the formats;
- the necessary storage period in relation to the outsourced information.

3.2.2 *Submission agreement*

The NA must make agreements with each Producer, the supplier of the archive material, about the form and manner in which the archive material will be delivered.[18]

3.2.3 *Designated community*

When transferring or relocating objects, information must be supplied about the relationship between the information file and the way in which it will be made available to the various groups of clients.

[17] Appendix 4.2 Other Definitions

[18] The Submission Agreement contains the agreements about access rights and preservation rights, essential characteristics of the digital objects, the time schedule and manner of delivery, and a detailed description of the structure of the SIP to be delivered.

The NA is also starting community monitoring. This functional entity maps out the wishes and needs of designated communities with regard to access and use of digital information through the e-Depot. A distinction is made between outsourced information (administrative chain) and transferred information (citizen chain).

3.2.4 *Open source and open standards*

The central government encourages the use of open data, open standards and open source software. The Dutch government also applies the principle of apply or explain.[19]

The Archive Regulation 2009 stipulates that digital information must be *stored in a validatable and fully documented file format that complies with an open standard no later than at the time of transfer.* If near to the time of transfer information must be converted to an open standard/format, it is recommended that you ask the NA for advice beforehand as conversion can result in an undesirable loss of information. If the records creator is faced with the task of purchasing and structuring a process application, it is advisable to carry out a risk analysis before this decision is taken: which process is supported by this application, which information is created, received, used and reused, which functionality must be retained in the future (information objective), which societal interests does this information serve and which degree of sustainable accessibly fits with this? This risk analysis can be used as a basis for the decision on whether to choose an open or a closed format.

The facility that the NA uses for long-term storage is based on OAIS.

3.2.5 *Metadata model*

The NA has a normative description of the metadata to be stored (information about information objects and the relationships between them). This description takes the form of a metadata model that is based on the Guidelines for Metadata on Government Information.

3.2.6 *File formats and essential characteristics*

The NA is working on a list of preferential formats that facilitate preservation and, therefore, sustainable accessibility. The NA does not currently impose any restrictions with regard to the number or type of file formats that are included. The relevant assessment criteria can be found in Open source and open standards. Experience has shown that the greatest risk of information loss is currently poor conversions, such as conversions from a closed format to an open format. Illegible data is often due to human error: converting or saving information is done incorrectly (e.g. forgetting to embed the font). During large bulk migrations, quality control is sometimes poor or incomplete.

Another factor is that file format or extension are not the only aspects that must be considered when making a decision on migration. Much more important are the choices regarding what you want to save with regard to the behaviour, content, form and structure of the information object; in other words, the essential characteristics. The NA has drawn up a list of criteria to use when establishing these essential characteristics.

The NA emphasizes that choosing non-open standards may affect:

- the accompanying preservation strategy, i.e. potential active and passive preservation[20].
- the form of providing information with regard to the required viewers or freely available software

[19] http://www.rijksoverheid.nl/onderwerpen/digitale-overheid/open-data-en-open-standaarden, consulted on 22-04-2015

[20] Appendix 4.2 Other Definitions

3.2.7 *Automation*

The NA uses automation as much as possible when receiving digital objects, when implementing management, with acts of preservation and with acts related to accessibility.

3.2.8 *Compression*

The Archive Regulation stipulates that: *"It is only permitted to use compression technology insofar as this does not cause such loss of information that it would be impossible to comply with the criteria set out in these regulations with regard to the accessible and orderly state of digital archive documents"*.

Compression is a technique for reducing the size of electronic data. The quality of compression depends upon the compression algorithms used and the information objects to which they are applied. If compression has already been applied within an information object, the NA will not do anything with it.

3.2.9 *Autonomy of use*

The NA ensures that users are able to understand and use the information that it has made available by making digital information, including accompanying metadata, available on websites and portals with the required viewers and download options.

3.2.10 *Encryption and access rights*

As it must be possible to provide access to digital information from the OAIS, the NA has a strong preference for non-encrypted information objects when they are delivered for ingest into the digital depot. If encryption is used, the accompanying decryption key must be provided. This also applies to passwords. The NA will ensure that the legally applicable disclosure restrictions and classifications are applied.

3.2.11 *Digital signature*

The Archive Regulation 2009 stipulates a number of conditions[21] regarding information with a digital signature. Experience has taught the NA that these conditions apply if the legal legitimacy of the information, including the signature, may be jeopardized in the event of relocation or transferral. If this is not the case, the signature will not be included. Authenticity will be maintained by being recorded in the metadata and procedures.

3.2.12 *Technical and functional management*

The roles and responsibilities for preservation as distinguished as follows:

- National Digital Archive Services (DAAD): pre-ingest, connection, identifying the producer. For outsourced archives: implementation, management. Roles: implementation manager, among others.
- Knowledge and Advice (K&A): preservation planning and preservation watch. Roles: officer, researcher and advisor, among others.
- Infrastructure and services (I&S): storage, administration, service desk and management, application management, technical management. Roles: product manager and specialist, security expert, developer, manager and tester, among others.
- Collection: ingest, data management, access. Roles: preservation manager, key user and manager, among others.
- Services: access, identifying the consumer. Roles: access, search and retrieval expert, among others.

[21] Archive regulation 2009 Article 24, paragraph c
In addition to the metadata referred to in Article 19, paragraph 2, the legal caretaker will link metadata to digital archive documents from which the following information can be derived at all times: 1°. the bearer of the digital signature; 2°. the time of validation of the digital signature as well as the result thereof; 3°. the official responsible for the validation; and 4°. insofar as it is known at the time of the work process: the identification of the certificate of the digital signature.

In figure 4, these roles and responsibilities are combined with departments of the NA and the OAIS functional entities. The NA will develop these roles further.

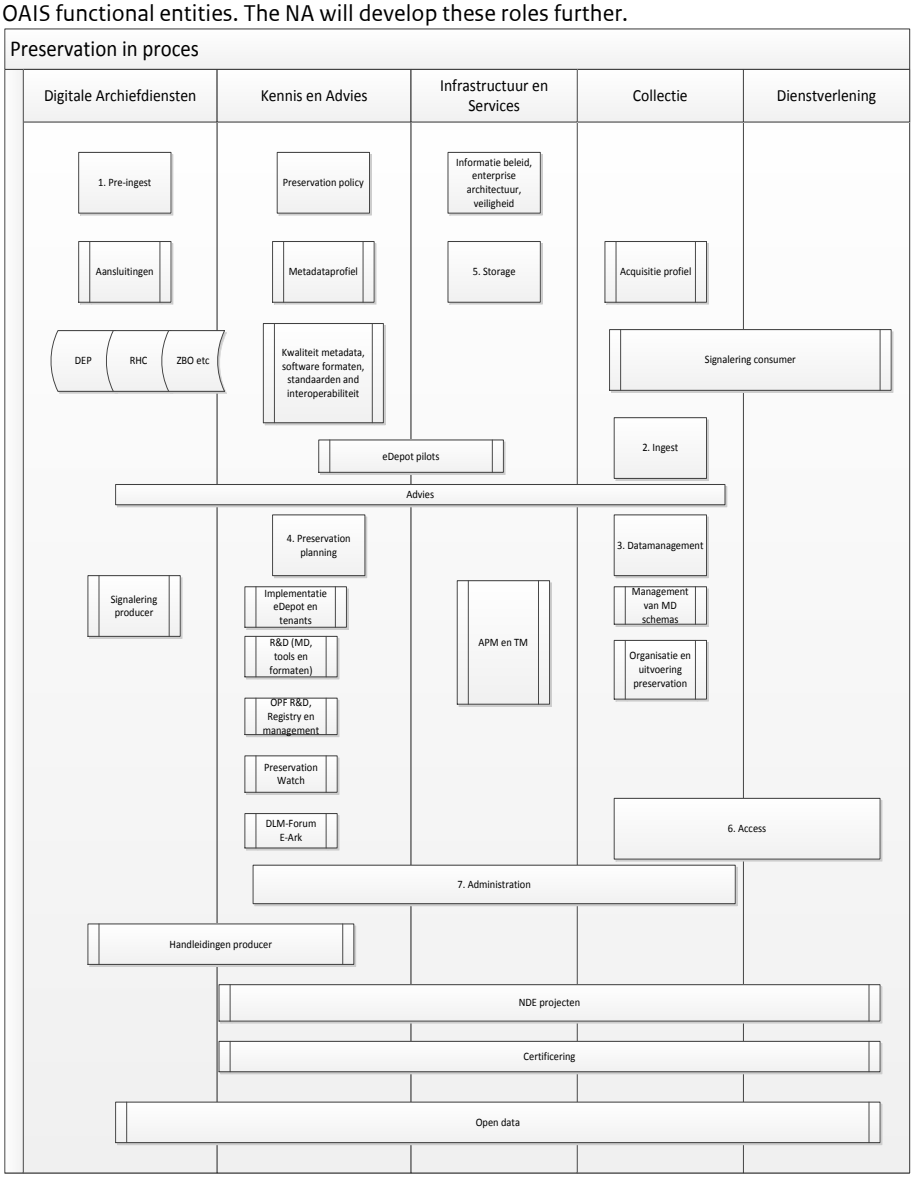

Figure 4: Preservation roles at the NA

3.3 Implementation

3.3.1 *Pre-ingest*

The Submission Agreement[22] and connection requirements will be implemented in the phase preceding ingest.

The following aspects will be checked:

- the technical conditions for system connections;
- the limitations regarding digital signatures, compression and other technical processing;
- the logical conditions for the interoperability of the metadata. A mapping will be

[22] See 2.1.2 Responsibilities

made between the producer's metadata and the NA's metadata model. If there is no match, an assessment will be made as to whether it is necessary and possible to supplement and improve the metadata;
- the necessary storage period in relation to the outsourced information;
- the relationship with public access and reuse of information;
- the information about the relationship between the information file and the way in which it will be made (machine legible) available to the various groups of clients;
- an assessment will be made of the risks related to the formats that have been used. Depending on the outcome, some formats may be converted to a more sustainable format. Both formats will be ingested with the accompanying metadata.

The producer supplies the information. The metadata is then converted to a machine-readable format so that it can be included with the digital objects (via the SIP Generator). By the end of the pre-ingest there will be a valid and useable Submission Information Package (SIP)[23].

The NA checks the integrity of the SIP though a checksum and examines whether it is complete by verifying if all the specified information objects and metadata are actually contained within the SIP.

3.3.2 *Ingest*

A number of controls and identification checks that are a precondition for the proper management and availability of digital information will be conducted during ingest of the SIP:

a. Characterization is a collective term for the following acts:

1. Identification: the file format is identified and linked to the Technical Registry[24] through one of the unique references stored in the metadata.
2. Validation: checking whether the file format is structured in conformity with the technical specifications.
3. "Measuring" technical properties that could hinder sustainable management (e.g. encryption, compression). This is also saved in the metadata using a PUID[25].
4. Identifying embedded objects (e.g. pictures or graphs in a Word file) or objects in container files (e.g. email with appendices, web pages of a website): file formats of these objects are saved in the metadata by means of a PUID.
5. Identifying file properties. The values of these properties are extracted and saved together with a reference to the property by means of a PUID. Examples include the height and width of a picture, the number of pages/words of a text document, etc.

b. Checks

There are also a number of quality checks regarding the integrity as referred to here:

1. Metadata Integrity check: it will be checked whether all content files are specified in the metadata through the correct (relative) location;
2. Content Integrity check: a check is conducted to ensure that all content files are specified in the xml metadata and that this has been done consistently.

The aforementioned checks ensure that no content is included without metadata and that no metadata is included without content.

[23] Appendix 4.1 Definitions
[24] The Technical Registry is a technical database that stores all information about file formats, software, hardware, compression, tools and for example properties.
[25] Developed by TNA for PRONOM http://www.nationalarchives.gov.uk/aboutapps/pronom/puid.htm The scheme is customizable and open and its use is broadly accepted within the Digital Preservation/registry community

Another integrity control is the Fixity Check. The checksum for each content file is compared against the original checksum specified in the metadata. This check is conducted regularly after ingest. Before ingest it can also be checked after every transport (ftp, copies, etc.).

Naturally, a virus check will be conducted and the security is arranged in conformity with the requirements of the Baseline for Information Security of the National Government (BIR)[26].

Both the original information object and the original metadata are stored. An AIP[27] is made and given the status of an original information object. This AIP receives a unique identification number and is saved in the storage data base.
A part of the incoming metadata is Descriptive Information. This part is exported to the Collection Management System and will be further enriched there. The legal caretaker's original metadata remains in the e-Depot (in the metadata database). All metadata generated during the various processes will also be saved in the same metadata base. Metadata will therefore continue to be added for the duration of the management of information objects.

Finally, the agreements in the Submission Agreement will be checked.

3.3.3 *Storage*

The aforementioned requirements on the basis of the BIR apply to the storage environment. The storage location is established and it will be assessed in the long term whether or not to apply the principles of 'tiered storage' or 'cached storage', whereby everything is in the large, slow storage, but information which is requested often is also stored in a fast 'cache' environment. Practically, this means that various types of storage media are used for various types of information objects, such as relatively small but fast – therefore more expensive – storage media for information objects that are requested often and larger, slower – and therefore less expensive – storage media for information objects that are requested less often. All sorts of cost-profit aspects come into play when making this assessment, such as the number and size of the requested information objects.

3.3.4 *Data management*

Data management involves keeping track of information about the information objects, or to put it more precisely, all operating, logging and reporting on changes to metadata, in the e-Depot facility and in a collection management system, as well as in the actual information objects. There is also an automatic relationship with the Technical Registry and the metadata scheme that is applied.

3.3.5 *Preservation planning*

The e-Depot functionality is designed for bit preservation by:

- keeping at least one available copy of every bitstream. The NA therefore always saves at least two manifestations of every bitstream: the original and at least one copy;
- guaranteeing the integrity of the bitstream (checking the checksum) and setting a check cycle;
- being able to show and document the above.

The NA has linked a Technical Registry to the e-Depot facility, where the representation information related to preservation planning is collected/updated.

The NA has set a preservation watch. This watch serves to determine the scope of the technologies for managing the information objects and metadata and to grant access to it, to

[26] http://www.earonline.nl/images/earpub/6/6f/BIR_TNK_1_0_definitief.pdf, consulted on 22-04-2015
[27] Appendix 4.1 OAIS Definitions

monitor support for these technologies in the organization and community and to embed triggers. In practical terms, this entails:

- keeping up to date with national and international developments in the area of technological change and standards and the hardware and software used by producers and publishing reports on this;
- regularly reviewing designated communities;
- conducting risk inventories on information objects and metadata in the e-Depot facility;
- monitoring the Producer, Consumer and internal organization for changes that could influence the sustainable accessibility of the information objects.

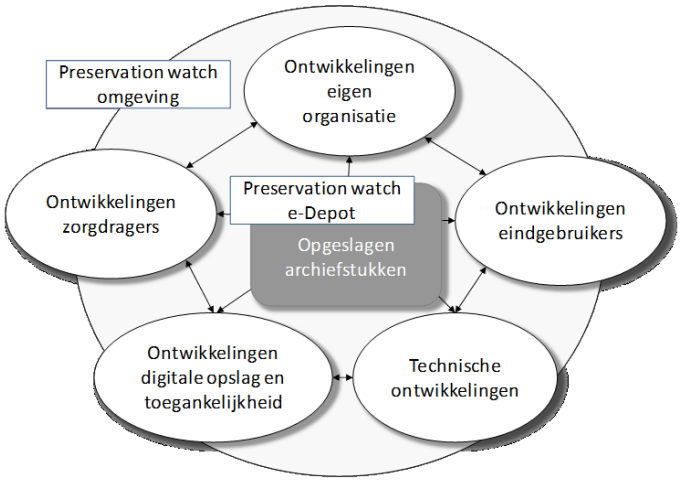

Figure 5: Preservation Watch

In order to embed triggers, the NA has a planning functionality that issues a warning if information objects are not sustainably accessible.

- Strategies have been drawn up for the preservation of various formats, made possible through conversion, emulation, using viewers or a combination thereof. This takes into account the essential characteristics of an object and the best quality is saved alongside the original. This takes the essential characteristics of an object into account. Applying a preservation strategy produces a reliable and authentic version in addition to the original file.
- The software is fitted with preservation tools which can be used to perform the necessary preservation acts (automated insofar as possible). The tools used for this are attuned to the available information objects and the most common formats used by the government.

If a trigger goes off, indicating that something is changing that may influence the technology with regard to use or access, the seriousness of the change must be assessed, in addition to the risk of the change actually occurring and the consequences that this change would have for the collection. Preservation will be planned on the basis of this.

If a preservation act is necessary, a preservation plan will be drawn up on the basis of up-to-date strategies. The following aspects are compulsory:

- a definition of the type of information object that it applies to;
- a description of the change;
- a description of the envisaged outcome;
- a step-by-step plan (including the name and version of the software and hardware to be used, necessary configurations and the exact order of the steps that must be taken);
- success factors;
- testing, approval and documentation of the process.

The NA's e-Depot facility provides a framework within which individual (third party) tools can be linked and automatic implementation will take place under the control of the repository.

3.3.6 *Access*

The access functionality supports the provision of accessible, readable and useable information objects, the handling of information and service requests, and several aggregation-friendly links for consumer interfaces, including authorization tables. A DIP will be made available in successive stages from the link to the Collection Management System and the access workflow. Information will be made available in a variety of ways, such as via a viewer or a download functionality, depending upon the designated community/user.

The NA also applies an open standard to opening up and providing access to digital archive documents (EAD). The relationship between the substantive metadata and the digital file will be guaranteed by means of a unique identifier. Continuous community monitory is necessary in order to fulfil the changing needs and demands of existing and potential user groups. The NA does this through the consumer side of the preservation watch (designated community), among other things.

3.3.7 *Administration*

The administration functionality provides all services and functionalities/tasks related to the everyday management of all the other functional entities. It is a vital part of the OAIS archive. It is a historical overview of work flows, reports, tools, security and actions for service provision and management, and provides the general organizational policy.

4 Appendices

4.1 OAIS Definitions

Access Functional Entity: The OAIS functional entity that contains the services and functions which make the archival information holdings and related services visible to Consumers.
Access Rights Information: The information that identifies the access restrictions pertaining to the Content Information, including the legal framework, licensing terms, and access control. It contains the access and distribution conditions stated within the Submission Agreement, related to both preservation (by the OAIS) and final usage (by the Consumer). It also includes the specifications for the application of rights enforcement measures.
Access Aid: A software program or document that allows Consumers to locate, analyse, order or retrieve information from an OAIS.
Access Collection: A collection of AIPs that is defined by a Collection Description but for which there is no Packaging Information for the collection in Archival Storage.
Access Software: A type of software that presents part of or all of the information content of an Information Object in forms understandable to humans or systems.
Adhoc Order: A request that is generated by a Consumer for information the OAIS has indicated is currently available.
Administration Functional Entity: The OAIS functional entity that contains the services and functions needed to control the operation of the other OAIS functional entities on a day to-day basis.
AIP Edition: An AIP whose Content Information or Preservation Description Information has been upgraded or improved with the intent not to preserve information, but to increase or improve it. An AIP edition is not considered to be the result of a Migration.
AIP Version: An AIP whose Content Information or Preservation Description Information has undergone a Transformation on a source AIP and is a candidate to replace the source AIP. An AIP version is considered to be the result of a Digital Migration.
Archival Information Collection (AIC): An Archival Information Package whose Content Information is an aggregation of other Archival Information Packages.
Archival Information Package (AIP): An Information Package, consisting of the Content Information and the associated Preservation Description Information (PDI), which is preserved within an OAIS.
Archival Information Unit (AIU): An Archival Information Package where the Archive chooses not to break down the Content Information into other Archival Information Packages. An AIU can consist of multiple digital objects (e.g., multiple files).
Archival Storage Functional Entity: The OAIS functional entity that contains the services and functions used for the storage and retrieval of Archival Information Packages.
Archive: An organization that intends to preserve information for access and use by a Designated Community.
Associated Description: The information describing the content of an Information Package from the point of view of a particular Access Aid.
Authenticity: The degree to which a person (or system) regards an object as what it is purported to be. Authenticity is judged on the basis of evidence.
Collection Description: A type of Package Description that is specialized to provide information about an Archival Information Collection for use by Access Aids.
Common Services: The supporting services such as inter-process communication, name services, temporary storage allocation, exception handling, security, and directory services necessary to support the OAIS.
Consumer: The role played by those persons, or client systems, who interact with OAIS services to find preserved information of interest and to access that information in detail. This can include other OAISes, as well as internal OAIS persons or systems.
Content Data Object: The Data Object, that together with associated Representation Information, comprises the Content Information.
Content Information: A set of information that is the original target of preservation or that includes part or all of that information. It is an Information Object composed of its Content Data Object and its Representation Information.
Context Information: The information that documents the relationships of the Content Information to its environment. This includes why the Content Information was created and how it relates to other Content Information objects.

Co-operating Archives: Those Archives that have Designated Communities with related interests. They may order and ingest data from each other. At a minimum, Co-operating Archives must agree to support at least one common Submission Information Package (SIP) and Dissemination Information Package (DIP) for inter-Archive requests.
Data: A reinterpretable representation of information in a formalized manner suitable for communication, interpretation, or processing. Examples of data include a sequence of bits, a table of numbers, the characters on a page, the recording of sounds made by a person speaking, or a moon rock specimen.
Data Dictionary: A formal repository of terms used to describe data.
Data Dissemination Session: A delivery of media or a single telecommunications session that provides Data to a Consumer. The Data Dissemination Session format/contents is based on a data model negotiated between the OAIS and the Consumer in the request agreement. This data model identifies the logical constructs used by the OAIS and how they are represented on each media delivery or in the telecommunication session.
Data Management Functional Entity: The OAIS functional entity that contains the services and functions for populating, maintaining, and accessing a wide variety of information. Some examples of this information are catalogues and inventories on what may be retrieved from Archival Storage, processing algorithms that may be run on retrieved data,
Consumer access statistics, Consumer billing, Event Based Orders, security controls, and OAIS schedules, policies, and procedures.
Data Management Data: The data created and stored in Data Management persistent storage that refer to operation of an Archive. Some examples of this data are accounting data for Consumer billing and authorization, policy data, Event Based Order (subscription) data for repeating requests, preservation process history data, and statistical data for generating reports to Archive management.
Data Object: Either a Physical Object or a Digital Object.
Data Submission Session: A delivery of media or a single telecommunications session that provides Data to an OAIS. The Data Submission Session format/contents is based on a data model negotiated between the OAIS and the Producer in the Submission Agreement. This data model identifies the logical constructs used by the Producer and how they are represented on each media delivery or in the telecommunication session.
Derived AIP: An AIP generated by extracting or aggregating information from one or more source AIPs.
Descriptive Information: The set of information, consisting primarily of Package Descriptions, which is provided to Data Management to support the finding, ordering, and retrieving of OAIS information holdings by Consumers.
Designated Community: An identified group of potential Consumers who should be able to understand a particular set of information. The Designated Community may be composed of multiple user communities. A Designated Community is defined by the Archive and this definition may change over time.
Digital Migration: The transfer of digital information, while intending to preserve it, within the OAIS. It is distinguished from transfers in general by three attributes:
– a focus on the preservation of the full information content that needs preservation;
– a perspective that the new archival implementation of the information is a replacement for the old; and
– an understanding that full control and responsibility over all aspects of the transfer resides with the OAIS.
Digital Object: An object composed of a set of bit sequences.
Dissemination Information Package (DIP): An Information Package, derived from one or more AIPs, and sent by Archives to the Consumer in response to a request to the OAIS.
Event Based Order: A request that is generated by a Consumer for information that is to be delivered periodically on the basis of some event or events.
Federated Archives: A group of Archives that has agreed to provide access to their holdings via one or more common finding aids.
Finding Aid: A type of Access Aid that allows a user to search for and identify Archival Information Packages of interest.
Fixity Information: The information which documents the mechanisms that ensure that the Content Information object has not been altered in an undocumented manner. An example is a Cyclical Redundancy Check (CRC) code for a file.
Global Community: An extended Consumer community, in the context of Federated Archives, that accesses the holdings of several Archives via one or more common Finding Aids.
Independently Understandable: A characteristic of information that is sufficiently complete to allow it to be interpreted, understood and used by the Designated Community without having to resort to special resources not widely available, including named individuals.

Information: Any type of knowledge that can be exchanged. In an exchange, it is represented by data. An example is a string of bits (the data) accompanied by a description of how to interpret the string of bits as numbers representing temperature observations measured in degrees Celsius (the Representation Information).
Information Object: A Data Object together with its Representation Information.
Information Package: A logical container composed of optional Content Information and formation. Associated with this Information Package is Packaging Information used to delimit and identify the Content information and Package Description information used to facilitate searches for the Content Information.
Information Property: That part of the Content Information as described by the Information Property Description. The detailed expression, or value, of that part of the information content is conveyed by the appropriate parts of the Content Data Object and its Representation Information.
Information Property Description: The description of the Information Property. It is a description of a part of the information content of a Content Information object that is highlighted for a particular purpose.
Ingest Functional Entity: The OAIS functional entity that contains the services and functions that accept Submission Information Packages from Producers, prepares Archival Information Packages for storage, and ensures that Archival Information Packages and their supporting Descriptive Information become established within the OAIS.
Knowledge Base: A set of information, incorporated by a person or system, that allows that person or system to understand received information.
Local Community: The community which would be served by the Archive outside of the context of Federated Archives.
Long Term: A period of time long enough for there to be concern about the impacts of changing technologies, including support for new media and data formats, and of a changing Designated Community, on the information being held in an OAIS. This period extends into the indefinite future.
Long Term Preservation: The act of maintaining information, Independently Understandable by a Designated Community, and with evidence supporting its Authenticity, over the Long Term.
Management: The role played by those who set overall OAIS policy as one component in a broader policy domain, for example as part of a larger organization.
Member Description: An Associated Description that describes a member of a collection.
Metadata: Data about other data.
Non-Reversible Transformation: A Transformation which cannot be guaranteed to be a Reversible Transformation.
Open Archival Information System (OAIS): An Archive, consisting of an organization, which may be part of a larger organization, of people and systems, that has accepted the responsibility to preserve information and make it available for a Designated Community. It meets a set of responsibilities, as defined in section 4, that allows an OAIS Archive to be distinguished from other uses of the term 'Archive'. The term 'Open' in OAIS is used to imply that this Recommendation and future related Recommendations and standards are developed in open forums, and it does not imply that access to the Archive is unrestricted.
Order Agreement: An agreement between the Archive and the Consumer in which the physical details of the delivery, such as media type and format of Data, are specified.
Ordering Aid: An application that assists the Consumer in discovering the cost of, and in ordering, AIPs of interest.
Other Representation Information: Representation Information which cannot easily be classified as Semantic or Structural. For example software, algorithms, encryption, written instructions and many other things may be needed to understand the Content Data Object, all
of which therefore would be, by definition, Representation Information, yet would not obviously be either Structure or Semantics. Information defining how the Structure and the Semantic Information relate to each other, or software needed to process a database file would also be regarded as Other Representation Information.
Overview Description: A specialization of the Collection Description that describes the collection as a whole.
Package Description: The information intended for use by Access Aids.
Packaging Information: The information that is used to bind and identify the components of an Information Package. For example, it may be the ISO 9660 volume and directory information used on a CD-ROM to provide the content of several files containing Content Information and Preservation Description Information.
Physical Object: An object (such as a moon rock, bio-specimen, microscope slide) with physically observable properties that represent information that is considered suitable for being adequately documented for preservation, distribution, and independent usage.

Preservation Description Information (**PDI**): The information which is necessary for adequate preservation of the Content Information and which can be categorized as Provenance, Reference, Fixity, Context, and Access Rights Information.
Preservation Planning Functional Entity: The OAIS functional entity which provides the services and functions for monitoring the environment of the OAIS and which provides recommendations and preservation plans to ensure that the information stored in the OAIS remains accessible to, and understandable by, and sufficiently usable by, the Designated Community over the Long Term, even if the original computing environment becomes obsolete.
Producer: The role played by those persons or client systems that provide the information to be preserved. This can include other OAISes or internal OAIS persons or systems.
Provenance Information: The information that documents the history of the Content Information. This information tells the origin or source of the Content Information, any changes that may have taken place since it was originated, and who has had custody of it since it was originated. The Archive is responsible for creating and preserving Provenance. Information from the point of Ingest; however, earlier Provenance Information should be provided by the Producer. Provenance Information adds to the evidence to support Authenticity.
Reference Information: The information that is used as an identifier for the Content Information. It also includes identifiers that allow outside systems to refer unambiguously to a particular Content Information. An example of Reference Information is an ISBN.
Reference Model: A framework for understanding significant relationships among the entities of some environment, and for the development of consistent standards or specifications supporting that environment. A reference model is based on a small number of unifying concepts and may be used as a basis for education and explaining standards to a non-specialist.
Refreshment: A Digital Migration where the effect is to replace a media instance with a copy that is sufficiently exact that all Archival Storage hardware and software continues to run as before.
Repackaging: A Digital Migration in which there is an alteration in the Packaging Information of the AIP.
Replication: A Digital Migration where there is no change to the Packaging Information, the Content Information, and the PDI. The bits used to represent these Information Objects are preserved in the transfer to the same or new media instance.
Representation Information: The information that maps a Data Object into more meaningful concepts. An example of Representation Information for a bit sequence which is a FITS file might consist of the FITS standard which defines the format plus a dictionary which defines the meaning in the file of keywords which are not part of the standard. Another example is JPEG software which is used to render a JPEG file; rendering the JPEG file as bits is not very meaningful to humans but the software, which embodies an understanding of the JPEG standard, maps the bits into pixels which can then be rendered as an image for human viewing.
Representation Network: The set of Representation Information that fully describes the meaning of a Data Object. Representation Information in digital forms needs additional Representation Information so its digital forms can be understood over the Long Term.
Representation Rendering Software: A type of software that displays Representation Information of an Information Object in forms understandable to humans.
Retrieval Aid: An application that allows authorized users to retrieve the Content Information and PDI described by the Package Description.
Reversible Transformation: A Transformation in which the new representation defines a set (or a subset) of resulting entities that are equivalent to the resulting entities defined by the original representation. This means that there is a one-to-one mapping back to the original representation and its set of base entities.
Search Session: A session initiated by the Consumer with the Archive during which the Consumer will use the Archive Finding Aids to identify and investigate potential holdings of interest.
Semantic Information: The Representation Information that further describes the meaning beyond that provided by the Structure Information.
Structure Information: The Representation Information that imparts meaning about how other information is organized. For example, it maps bit streams to common computer types such as characters, numbers, and pixels and aggregations of those types such as character strings and arrays.
Submission Agreement: The agreement reached between an OAIS and the Producer that specifies a data model, and any other arrangements needed, for the Data Submission Session. This data model identifies format/contents and the logical constructs used by the Producer

and how they are represented on each media delivery or in a telecommunication session.
Submission Information Package (SIP): An Information Package that is delivered by the Producer to the OAIS for use in the construction or update of one or more AIPs and/or the associated Descriptive Information.
Succession Plan: The plan of how and when the management, ownership and/or control of the OAIS holdings will be transferred to a subsequent OAIS in order to ensure the continued effective preservation of those holdings.
Transformation: A Digital Migration in which there is an alteration to the Content Information or PDI of an Archival Information Package. For example, changing ASCII codes to UNICODE in a text document being preserved is a Transformation.
Transformational Information Property: An Information Property the preservation of the value of which is regarded as being necessary but not sufficient to verify that any Non-Reversible Transformation has adequately preserved information content. This could be important as contributing to evidence about Authenticity. Such an Information Property is dependent upon specific Representation Information, including Semantic Information, to denote how it is encoded and what it means. (The term 'significant property', which has various definitions in the literature, is sometimes used in a way that is consistent with its being a Transformational Information Property).
Unit Description: A type of Package Description that is specialized to provide information about an Archival Information Unit for use by Access Aids.

4.2 Other Definitions

Active Preservation[28]
Every pro-active action undertaken to preserve digital archive documents (e.g. migration of files if a file format is outdated or normalization for ingest). It ensures continued access to meaningful information content.

Authenticity[29]

- Reliability: transparent and fully documented preservation strategies and provision of metadata required to describe content, context and origin.
- Integrity: bitstream preservation and provision of metadata that describes all authorized preservation acts.
- Usability: logical preservation and provision of metadata required for location, retrieve and interpretation.

Checksums[30]
A computed value that is dependent upon the contents of a packet. Sent along with the packet when it is transmitted. The receiving system computes a new checksum based on data received, compares this value with the one sent with the packet. If the two values are the same, the receiver has a high degree of confidence that the data was received correctly.

Compression[31]
The (re)coding of digital data to save storage space or transmission time.

Noncustodial[32]
Archival records, usually in electronic format, that are held by the agency of origin, rather than being transferred to the archives.

Long-term accessibility[33]
A series of guided activities that is necessary to anchor access to digital files for as long as necessary.

Escrow[34]
An escrow agreement is an agreement between the maker of software, their clients and an escrow agent. The agreement guarantees that in certain situations the client may have access to the most recent source code of the software package for which the agreement was entered into.

A final user of software has a strong interest in the continued existence of software as its business operations may be heavily dependent on it.

If it is necessary to make an adjustment to the package and the supplier is no longer able to deliver, for example due to a bankruptcy, cessation of a product or range or products or non-compliance with delivery obligations, the end user may not do or commission this themselves. This requires the source code.

In practice, escrow agreements are simply known as ‘escrow’.

Open standard[35]

[28] Adrian Brown, Practical Digital Preservation, page 228)
[29] Adrian Brown, Practical Digital Preservation, page 193)
[30] http://www.alliancepermanentaccess.org/index.php/consultancy/dpglossary/#C Source: NDHA ANZ
[31] http://www.alliancepermanentaccess.org/index.php/consultancy/dpglossary/#C [Computer and Information Sciences]
[32] http://www2.archivists.org/glossary/terms/n/noncustodial-records
[33] http://www.ncdd.nl/blog/?page_id=427
[34] Wikipedia, http://nl.wikipedia.org/wiki/Escrow-overeenkomst, consulted on 01-06-2015

'Open' relates to the standardization process. This means readily available documentation, no obstacles due to intellectual property rights (such as patent royalties), opportunities to comment, and independency and sustainability of the standardization organization.

Passive Preservation[36]
Any act that supports DP but is not directly related to digital objects (such as management of the digital files and storage method). For example: Bitstream preservation: *to create a bitstream that can ensure that a demonstrably bit-perfect copy can be retrieved on demand.*
Conditions:

- *Maintain at least 1 available copy of each bitstream;*
- *Ensure the integrity of the bitstream;*
- *Collect rigorous evidence to prove the above*

Preservation Strategy[37]
The complex of practical means formally articulated by an entity for reaching a specific purpose, that is, a plan or a road map for implementing policies.

This consists of:

- assessing risks of content loss due to technical variables such as the use of the company's own file formats and software applications;
- the evaluation of the digital content to establish which type of format conversions or other preservation acts must take place;
- establishing which metadata is necessary for each type of object and how this is associated with the various objects;
- access to the content.

[35] https://www.forumstandaardisatie.nl/open-standaarden/over-open-standaarden/
[36] Adrian Brown, Practical Digital Preservation, page 218)
[37] http://www.alliancepermanentaccess.org/index.php/consultancy/dpglossary/#C [Archives]

4.3 The Service Organization

The National Archives' Service Organization provides digital archiving services to RHCs, departments and other institutions with a public service function.

In 2013 work commenced on a national infrastructure that not only enables the National Archive, but also the Regional History Centres (RHCs) to ingest, manage and make available information objects. The objective of this national infrastructure is to:

1. guarantee the long-term accessibility of information objects;
2. effectively make information objects available to a wide audience through the internet;
3. transfer information objects from records creators to a depot in an efficient manner.
   The National Archives' digital depot (e-Depot) is part of this national infrastructure.

The clients of the National Archives' Service Organization include archive repositories, such as the RHCs, and legal caretakers, such as municipal councils, provinces, water boards and departments.
The Service Organization can either provide its services directly (such as to departments) or through the RHCs.

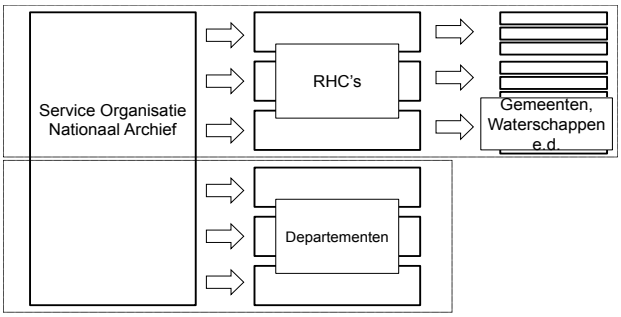

Figure 6: The National Archives' Service Organization

4.4 Orderly and accessible condition of archive records

Archives Regulation 2009, Section 3
§ 1. General regulations for archive records that must be kept

Article 16. Quality system The legal caretaker ensures that the management of their archive records complies with the verifiable requirements set by the quality system they use.

Article 17. Context and authenticity The legal caretaker will ensure that the following aspects of each archive record can be established at all times:
a. the content, structure and visual manifestation when received or formatted by the government agency, insofar as these aspects must be known in order to implement the work process in question;
b. when, by whom and for which task or work process it was received or formatted by the government agency;
c. the connection to other archive records that have been received and formatted by the government agency;
d. the management activities implemented in relation to the archive records; and
e. the operating software and application software for storing or managing the archive records.

Article 18. Overview and organizing structure
1. The legal caretaker must ensure that government agencies accountable to it have an up-to-date, complete, logical and coherent overview of the archive records in the possession of that government agency, organized according to the organization structure used at the time of creating the archive.
2. If the organization is adapted in the meantime, the original version will be kept along with the new version.

Article 19. Metadata scheme and metadata
1. The legal caretaker records a metadata scheme as referred to in NEN-ISO 23081:2006.
2. The legal caretaker links metadata to archive records from which the information referred to in article 17 can be derived at all times.

Article 20. Accessible condition The legal caretaker ensures that the archiving system guarantees the accessible condition of the archive records, so that each of the archive documents can be
a. found
1°. using the metadata linked to it; or
2°. using another disclosure method; and
b. made legible or perceptible within a reasonable period.

§ 2. Special regulations for archive records that must be kept

Article 21. Behaviour of digital archive records In addition to article 17, opening words and subparagraph a, the legal caretaker will ensure that the behaviour of each archive record can be established at all times.

Article 22. Functional requirements The legal caretaker ensures that the following functional requirements are established for each archive record:
a. the content, structure and visual manifestation, referred to in article 17, subparagraph a; and
b. the behaviour, insofar as this is necessary to guarantee the authenticity of the digital archive records.

Article 23. Identifiable digital files In addition to article 18, paragraph 1, the legal caretaker ensures that, using the overview referred to in that paragraph, all relevant digital files used to make the digital archive records in their care legible or perceptible can be identified.

Article 24. Metadata accompanying digital archive records In addition to the metadata referred to in article 19, paragraph 2, the legal caretaker will link metadata to digital archive documents from which the following information can be derived at all times:
a. the original technical nature of the digital archive documents as well as their hardware and software environment;
b. the current technical nature of the digital archive documents as well as their hardware and software environment so that it is always possible to reproduce them; and
c. insofar as a digital signature has been used:
1°. the holder of the digital signature;
2°. the time of validation of the digital signature as well as the result thereof;
3°. the official responsible for validation; and
4°. insofar as it is known at the time of the work process: the identification of the certificate of the digital signature.

Article 25. Conversion, migration or emulation
1. If, as a result of changes to operating or application software or of this software falling into disuse, there is a reasonable risk that the requirements stipulated in these regulations can no longer be met as regards the accessible and orderly condition of digital archive records, the legal caretaker will ensure conversion or migration of those digital archive records or ensure that these digital archive records may be used or consulted by applying emulation in accordance with the manner used at the time they were received or drafted by the government body.
2. The legal caretaker will draw up a statement of the migration, which will include at least a specification of the digital archive files that were converted or migrated. It will also specify how and with what result a check was conducted to assess whether the conversion or migration complies or can comply with the requirements regarding the orderly and accessible condition set under this regulation.

Article 26. General storage format requirements for digital archive records
1. Digital archive records must be stored in a validatable and fully documented file format that complies with an open standard no later than at the time of transfer, unless this cannot reasonably be required of the legal caretaker. In that case the administrator of the repository designated for transferral will be consulted about an alternative file format.
2. Insofar as encryption technology is used at the time of transferral, the administrator of the repository will be given the accompanying decryption key.
3. It is only permitted to use compression technology insofar as this does not cause such loss of information that it would be impossible to comply with the criteria set out in this regulation regarding the accessible and orderly state of digital archive documents.

4.5 OAIS: functionalities[38]

Pre-ingest (not OAIS)
Pre-ingest is the functional entity that makes information and its accompanying metadata ingestible. It concerns standardizing and checking the metadata.

Ingest
Ingest is the process of receiving the information and preparing it for archiving. During this ingest, Quality Assurance (QA) plays an important role, as a check will be conducted to ascertain whether the information provided has been transferred correctly from the creator to storage at the OAIS archive. This QA is usually conducted by means of checksums[39]. More checks may be carried out during ingest, such as virus checks and identification of the file formats. It will also be checked whether the delivered object corresponds to the agreements set out in the Submission Agreement. The result of ingest is that the information and metadata are ready to be entered into the Archival Storage and the Metadata bank.

Data management
Data management is the place in the archive where diverse information about the information is stored, including the access information. It is important for management to be able to search for information quickly. This is too cumbersome if it is necessary to search directly in Archival Storage, as all information would then have to be made 'open' before the right information could be accessed. A duplicate of the information is therefore often saved in Data Management with possible additions. There is therefore always an inseparable relationship between the actual information and the information about it in Data Management. Data Management also records where the information is stored (on the hardware).

Archival Storage
Archival Storage regulates the permanent storage of the information received through ingest. It also handles requests to provide duplicates of information that arrive through the Access functional entity and are then delivered to the user as a representation. Archival Storage also determines where the information is saved. In addition to this, Archival Storage also contains functionalities responsible for the integrity of the saved data, picking up on serious disruptions and regularly replacing the hardware on which the information is saved.

Administration
Administration covers all services and functional entities/tasks that are related to the everyday management of all the other functionalities. It is a vital part of the OAIS archive. Administration organizes all agreements related to the delivery of materials by records creators to the OAIS archive. It concerns procedures to receive the material and records the course of the process. This functional entity is also responsible for recording and maintaining standards, the policy applied by the OAIS archive and the important preconditions and policy principles for the OAIS archive. Furthermore, Administration manages the system and is responsible for the software and hardware and controls to access to these facilities.

Preservation planning
The Preservation Planning functionality monitors the OAIS archive environment and alerts other parts of the OAIS archive of measures to be taken on the basis of the information it receives. An important territory in this is the Designated Community. The world of the user and the records creator of information will change during the lifetime of the OAIS archive, which is focussed on the long term. The OAIS must be able to react to these changes,

[38] Extract from B. Sierman "Het OAIS-model, een leidraad voor duurzame toegankelijkheid." *Handboek Informatiewetenschap*, Vol. 62 (2012)
[39] Appendix 4.2 Definitions

otherwise it cannot fulfil its mission. The second, broad area that falls under the monitoring functional entity is updating and responding to technical innovations. Due to the rapid developments in file formats, software and hardware, there is a risk that the OAIS archive could miss connecting to these developments due to a lack of expertise and knowledge. The OAIS archive would be unable to fulfil its mission. This functional entity is closely related to the Develop Preservation Strategies functionality and Standards and Developing Packaging Designs. The Preservation Planning function is also responsible for regularly conducting a risk inventory and sending the results thereof to Administration.

Access

The Access functionality handles information requests from the OAIS archive. Often a OAIS archive will develop several versions of representation information to meet diverse needs. For example, by only showing the metadata or by showing the actual information in various versions (specific file format, thumbnail, etc.). Naturally, the Access function monitors that rights regarding access are respected in conformity with the agreements entered into with the records creator.

5 Publishing details

Contact person	M. van Gorsel
Editors	M. van Essen, P. Helwig, C. Leistra, P. Lucker, J. van Luin, W. van der Reijden, R. van Veenendaal, R. Verdegem
Version	1.1
Appendices	5
Date	24 November 2015