Assessment Information

CoreTrustSeal Requirements 2020–2022

Repository:	National Library of the Netherlands
Website:	https://www.kb.nl/
Certification Date:	18 June 2021

This repository is owned by: **National Library of the Netherlands**

National Library of the Netherlands

Notes Before Completing the Application

We have read and understood the notes concerning our application submission.

True

Reviewer Entry

Reviewer 1

Comments:

Reviewer 2

Comments:

CORE TRUSTWORTHY DATA REPOSITORIES REQUIREMENTS

Background & General Guidance

Glossary of Terms

BACKGROUND INFORMATION

Context

R0. Please provide context for your repository.

Repository Type. Select all relevant types from:

National repository system; including governmental

Reviewer Entry

Reviewer 1

Comments:
Accept

Reviewer 2

Comments:
Accept

Brief Description of Repository

The KB is the national library of the Netherlands. Driven by the power of the written word we further intellectual development, proficiency and creativity in the Netherlands. To this end, we seek collaboration with partners in the domains of public libraries, cultural heritage and academics. The KB promotes the visibility, usability and longevity of the Dutch Library Collection, defined as the collective holdings of all publicly funded libraries in the Netherlands.

As the National Library, the KB is tasked with ensuring that the Dutch National Library Collection remains accessible to the general public. The collection is part of the national digital library and the network of public library facilities. Broadly speaking, the KB's digital preservation activities involve the acquisition of digital publications, as well as managing them and making them available. These activities are part of the KB's mission to be responsible for the written word.

The application for certification is restricted to the current e-Depot's system components and data. The e-Depot contains the Dutch National Library Collection of born-digital publications from, and about, the Netherlands, and international publications consisting of born-digital scholarly articles included in journals produced by publishers originally based in the Netherlands. The to be certified e-Depot repository serves to safeguard long-term accessibility to born-digital publications that are part of the Dutch National Library Collection. The KB's content strategy specifies, in greater detail, which publications are part of the Dutch National Library Collection. Within the framework of the current content strategy, the KB endeavours to achieve the most complete Dutch heritage collection possible in the e-Depot for Dutch Publications. Some digital collections that are part of the Dutch National Library Collection, such as digitised material and the web archive, have not yet been incorporated into this system. Thus, the systems in which this material is stored have not been included in this certification process.

Reviewer Entry

Reviewer 1

Comments:
Accept

Reviewer 2

Comments:
Accept

Brief Description of the Repository's Designated Community.

The KB's designated community can be classified into two subgroups, based on the services required for these target groups: 1.) publishers 2.) All Dutch citizens.

The KB classifies all supplying parties into the first category. These can also be users of the material in question. These parties have special expertise with regard to the material's contents. The KB offers this target group special information concerning the processing of the material, to facilitate the ingest processes. In addition, some account managers are assigned to publishers. They are tasked with keeping in touch with the network and with establishing new links. Links with that group are also monitored collectively by various means, such as reaching and maintaining agreements with the Media Federation.

The KB defines the second category as private individuals, the media, researchers, and partners in the cultural heritage domain. The KB expects them to have a certain level of literacy in Dutch, as well as basic skills in the use of computers and search engines. On its website, the KB makes information available to help people in this target group search for – and retrieve – information. User surveys and various feedback options at the KB's websites are used to determine whether the services being provided are still fit for purpose. The KB keeps abreast of a target group's wishes through cooperation on issues such as the accessibility of digital heritage. This involves parties such as the Dutch Digital Heritage Network (NDE) and the Common Lab Research Infrastructure for the Arts and Humanities (CLARIAH).

The content strategy defines the level at which the KB wants to be able to offer access. Here, the KB's guiding principle is to offer all content as openly as possible, for current and future use. The strategy is based on the assumption that the KB will at least make material available on-site (i.e. on its premises). The agreements also stipulate the conditions under which publishers that supply material can make use of the e-Depot themselves. The publishers that supply the repository are seen as a separate 'target group'. This is because, based on the agreements reached, these parties can request the KB to provide a copy of a publication from the repository to the publisher. Alternatively, in the event of defined trigger events, they can – at the publisher's request – call on the KB to provide direct remote access to the publisher's customers.

Reviewer Entry

Reviewer 1

Comments:
Accept

Reviewer 2

Comments:
Accept

Level of Curation Performed. Select all relevant types from:

B. Basic curation – e.g. brief checking; addition of basic metadata or documentation

Reviewer Entry

Reviewer 1

Comments:
Accept

Reviewer 2

Comments:
Accept

Comments

The system is set up for Bit Preservation. See R7 for a description of the integrity checks involved. The checking of certain formats and the addition of technical metadata is part of our workflow which means we do more than Bit Preservation. In the coming years we aim to grow towards curation level C. The roadmap and the steps we need to take to achieve this is set out in the preservation plan.

Reviewer Entry

Reviewer 1

Comments:
Accept

Reviewer 2

Comments:
Accept

Insource/Outsource Partners. If applicable, please list them.

Reviewer Entry

Reviewer 1

Comments:
accept

Reviewer 2

Comments:
Accept

Summary of Significant Changes Since Last Application (if applicable).

Reviewer Entry

Reviewer 1

Comments:

Reviewer 2

Comments:
Accept

Other Relevant Information.

It is important to realise that, for some collections, the e-Depot provides access purely as an archive of last resort. In these cases material is only made available when a publisher is no longer able to supply it, for example in the event of bankruptcy. In other cases rights stipulations may prohibit access to the material in question. In addition, certain material – such as scholarly journals – is also available through other channels, such as university libraries. In cases like this, end-users can only make limited use of the e-Depot. For these collections the KB's strategy mainly focuses on the long-term preservation of the material.

Reviewer Entry

Reviewer 1

Comments:
accept

Reviewer 2

Comments:
Accept

ORGANIZATIONAL INFRASTRUCTURE

1. Mission/Scope

R1. The repository has an explicit mission to provide access to and preserve data in its domain.

Compliance Level:

4 – The guideline has been fully implemented in the repository

Reviewer Entry

Reviewer 1

Comments:
4 – The guideline has been fully implemented in the repository
Accept

Reviewer 2

Comments:
4 – The guideline has been fully implemented in the repository
Accept

Response:

The KB describes its mission in the 2019-2022 strategic plan:

“For centuries, the KB, National Library of the Netherlands has been a source of inspiration and innovation. Since our foundation in 1798, we have developed into a broad-based, versatile organisation, which makes the Dutch National Library Collection visible, sustainable and accessible for all Dutch people, for any purpose, both now and in the future. We are responsible for the written word, particularly Dutch publications, and for ensuring that everyone is able to read, learn, and conduct research. This is our way of contributing towards making the Netherlands smarter, more competent and more creative.”

The content strategy is just one means by which the mission’s principles have taken tangible form. In its 2019-2022 content strategy, the KB sets out its strategy for the growth of its digital collection during this period. In Section 2 (Taking care of the written word) of its strategic plan, the KB presents its plans for the future development of the digital repository, from 2019 to 2022. The KB has set up the Digital Repository 2.0 programme to implement these policy intentions, by further developing the e-Depot for which certification has been requested. The e-Depot to be certified serves to safeguard long-term accessibility to born digital publications that are part of the Dutch National Library Collection. The duty of responsibility for the Dutch National Library Collection is enshrined in the Higher Education and Research Act (WHW, effective since 1992 up to the present). In article 1.5 of this law (https://wetten.overheid.nl/BWBR0005682/2020-08-01/#Hoofdstuk1_Titeldeel1_Artikel1.5) it is stated thus: “The National Library of the Netherlands operates in the field of libraries and information provision systems. It caters to the areas of higher education and scholarly research, and to those involved in public administration and the pursuit of a profession or business. In that context, it is fully responsible for the Dutch National Library Collection, while promoting the establishment and maintenance of national facilities in the above-mentioned area and fostering coordination with the other academic libraries.”

The principles that underpin the KB’s duty of responsibility to ensure the preservation of born digital publications are laid down in its strategic Digital Preservation Policy and its tactical preservation plan. Over the next few years, in keeping with its content strategy, the KB intends to make a firm commitment to transition from a form of collection development that is still mainly physical to one that is predominantly digital. Further development of the e-Depot will be needed if this aspiration is to be fulfilled. The ‘Towards a New Digital Repository’ programme will provide the framework for this development. Implementation of the programme will be guided by a programme plan, and administered by a programme board. The programme budgets and project budgets will be fixed on the basis of detailed Project Initiation Documentation.

The necessary funding will be reserved within the Long-Term Budget for Digital Preservation.

Supporting documents
Content strategy 2019-2022: https://www.kb.nl/sites/default/files/docs/content_strategy_eng.pdf
Digital preservation policy: https://www.kb.nl/sites/default/files/docs/digital_preservation_policy_kb.pdf
Preservation plan: https://www.kb.nl/sites/default/files/docs/preservation_plan_2019-2022.pdf
Strategic Plan 2019-2022: https://www.kb.nl/sites/default/files/docs/kbnb_beleidsplan-eng.pdf
Organization and Policy section: https://www.kb.nl/en/organisation/organization-and-policy

An overview of all certification documents can be found at: http://www.kb.nl/certification

Reviewer Entry

Reviewer 1

Comments:

Reviewer 2

Comments:

2. Licenses

R2. The repository maintains all applicable licenses covering data access and use and monitors compliance.

Compliance Level:

4 – The guideline has been fully implemented in the repository

Reviewer Entry

Reviewer 1

Comments:
4 – The guideline has been fully implemented in the repository
Accept

Reviewer 2

Comments:
4 – The guideline has been fully implemented in the repository
Accept

Response:

The content strategy specifies which publications the KB includes in its e-Depot. The e-Depot contains the Dutch National Library Collection of born-digital publications from, and about, the Netherlands, and international publications consisting of born-digital scholarly articles. The content strategy also specifies how the KB offers access. Here, the KB's guiding principle is to offer all content as openly as possible, for current and future use. The strategy is based on the assumption that the KB will at least make publications available on-site (i.e. on its premises). The extent to which the KB can make publications openly available depends on the terms of any agreements reached with the publishers and on legislation and regulations (Copyright Act, General Data Protection Regulation). Statutory provisions and the agreements reached both determine the range of options that the KB can offer its users. In the same way, these govern the level of access that can be offered to the designated community. The KB's entire born-digital collection is subject to copyright. See R4 for details

of the legal basis on which access is granted. For individual publications, these agreements are translated into three levels (based on the metadata supplied) in the e-Depot. These levels are ‘no access’ (in the event of an embargo on availability), ‘restricted (on site access)’ and ‘open access’. Any users who require on-site access on the KB’s premises must first become KB members and agree to the KB’s regulations, which set out the terms and conditions of use. The use of open access material is free of restrictions. The agreements also stipulate the conditions under which publishers that supply material can make use of the e-Depot themselves. The publishers that supply the repository can, therefore, be seen as a separate ‘target group’. This is because, based on the agreements reached, these parties can call on the KB to supply material from the repository to the publisher. Alternatively, at the latter’s request, they can call on the KB to provide such material directly to the publisher’s customers.

The KB has agreements concluded for the e-Depot. See the agreement with the Netherlands Publishers Association: https://www.kb.nl/sites/default/files/docs/regeling_elektronisch_depot_nuv-kb_eng.pdf

The terms of these agreements concern:

- the reciprocal rights and obligations of both parties

-the level of access that the KB is permitted to offer

-cases of non-compliance by one of the parties

-notice and take-down

The metadata supplied by the publishers determines the level of access. This is determined on the basis of a mapping, which takes the form of a translation table between supplied values and authorisation levels within the system. If the KB cannot technically guarantee that it is able to provide the required level of access, then the material will not be made available. Within the KB, the Collections Department is accountable for reaching agreements, managing any agreements made, and ensuring that agreements are implemented.

The regulations give details of the consequences involved if members should fail to comply with the conditions. Any complaints submitted by visitors/users are handled in accordance with the KB’s Complaints Procedure, as adopted by the Board of Governors.

Supporting documents
Content strategy: https://www.kb.nl/sites/default/files/docs/content_strategy_eng.pdf
Selection criteria National Deposit Collection:
https://www.kb.nl/en/organisation/for-publishers/depositing-publications/selection-criteria-national-deposit-collection
Deposit Library: agreement with publishers:
https://www.kb.nl/en/organisation/for-publishers/deposit-library-for-dutch-publications
Conditions of use: https://www.kb.nl/en/services/conditions-of-use

Complaints procedure: https://www.kb.nl/sites/default/files/docs/klachtregeling-kb.pdf (Dutch only)

An overview of all certification documents can be found at: http://www.kb.nl/certification

Reviewer Entry

Reviewer 1

Comments:

Reviewer 2

Comments:

3. Continuity of access

R3. The repository has a continuity plan to ensure ongoing access to and preservation of its holdings.

Compliance Level:

3 – The repository is in the implementation phase

Reviewer Entry

Reviewer 1

Comments:
3 – The repository is in the implementation phase
accept

Reviewer 2

Comments:
3 – The repository is in the implementation phase
Accept

Response:

Agreements are entered into ‘in perpetuity’, whereby the KB guarantees permanent and long-term preservation for an indefinite period of time. If an agreement is terminated, then there is no obligation on the part of the KB to continue preserving and maintaining the archives. However, the KB does retain the right to subject the data supplied to long-term preservation.

A strategic plan is drawn up every four years, to ensure sustainable, long-term access to the material. The Content Strategy and the Digital Preservation Policy are in line with the KB’s policy cycle, and are periodically updated. The KB has also set up the Digital Repository 2.0 programme to implement its policy intentions, by further developing the e-Depot

for which certification has been requested. The necessary funding is reserved within the Long-Term Budget for Digital Preservation. The KB is answerable to the Ministry of Education, Culture and Science, and submits periodic reports. As an Autonomous Administrative Authority, the KB's evaluation framework is fixed by its parent department, the Ministry of Education, Culture and Science.

As stated above, the KB is the designated repository for the Dutch National Library Collection as stipulated in the Higher Education and Scientific Research Act (WHW). Also structural funding has been secured for preservation for the long term as confirmed by the minister. For more information see the recommendation letter: https://www.kb.nl/sites/default/files/docs/letter_ocw_0.pdf Chances that this role will change in the future are slight. However, unforeseen events may diminish funding or cause organizational change. Therefore a formal succession plan is needed to be able to provide continuity of access in the case of unforeseen changes. In the coming years, the KB will create a succession plan and make agreements to preserve the content at other institutions.

Supporting documents

Deposit Library: agreement with publishers:
https://www.kb.nl/en/organisation/for-publishers/deposit-library-for-dutch-publications
Digital Repository operating budget (Confidential document)

An overview of all certification documents can be found at: http://www.kb.nl/certification

Reviewer Entry
Reviewer 1
Comments:
Reviewer 2
Comments:

4. Confidentiality/Ethics

R4. The repository ensures, to the extent possible, that data are created, curated, accessed, and used in compliance with disciplinary and ethical norms.

Compliance Level:

4 – The guideline has been fully implemented in the repository

Reviewer Entry
Reviewer 1

Comments:
4 – The guideline has been fully implemented in the repository
Accept.

Reviewer 2

Comments:
4 – The guideline has been fully implemented in the repository
Accept

Response:

In accordance with a decision by its Board of Directors, the KB endorses the IFLA Code of Ethics for Librarians and other Information Workers (https://www.ifla.org/publications/node/11092). The KB's strategic plan sets out core values that reflect its ethical principles: "The core values that we share are: open, connective, innovative, and reliable."

Based on its core value of reliability, the KB attaches great importance to diligently protecting any personal data with which it is entrusted with or that it processes. Those who use its services, as well as its business relations and staff can be sure that the KB will deal with their personal data securely and in accordance with the GDPR. The KB drew up a Privacy Policy which can be found at: https://www.kb.nl/en/services/conditions-of-use/privacy-statement-kb-national-library-of-the-netherlands . The PrivacyPunt (a physical and digital service point) can handle all internal questions about privacy and the protection of personal data.

The administration of the e-Depot is part of the KB's legal duties, as laid down in the Higher Education and Research Act (WHW). This provides a basis for processing any personal data contained in publications. The National Library of the Netherlands (KB) takes the view that one of its key duties is to guarantee the authenticity and completeness of cultural-historical source material, as embodied in both physical and online publications. The collection also contains sensitive material, although access to such material can be restricted, in accordance with legislation. Privacy legislation includes an exception with regard to the processing of publications by institutions such as libraries, for literary, journalistic, scholarly, or historical purposes. This also includes the archiving of online publications. This means that producers can deposit publications with the KB (that the latter has requested), with no problems whatsoever. This legal basis means that the KB is not compelled to process requests from third parties to remove any publications from the collection that may contain privacy-related data.

The availability of material is subject to various limitations, as copyright considerations need to be taken into account. The KB's entire born-digital collection is subject to copyright. There are two leading principles: 1) content must be made available on the premises (on-site) and 2) the KB is entitled to create digital copies for long-term preservation. Contracts concluded with depositors always contain provisions for both situations. The KB's in-house legal team subjects complex cases to legislative review. One of these lawyers is embedded within the KB's Uitgeversrelaties (Publisher Relations) team, which is responsible for reaching cooperation agreements regarding the e-Depot. Both the contracts concluded with publishers and the KB's regulations (for users) include agreements on covering non-disclosure risks (see R2). The contracts concluded with producers stipulate that responsibility for supplying metadata to cover non-disclosure risks lies with the producer (see R2). Use of the collections is subject to conditions that can be found on the website: https://www.kb.nl/en/services/conditions-of-use

Upon commencement of employment, members of staff must be in possession of a Certificate of Good Conduct. Material can only be viewed and processed by those who are directly involved in the e-Depot. There is an application procedure for those who wish to obtain the necessary rights.

Supporting documents are part of the text.

An overview of all certification documents can be found at: http://www.kb.nl/certification

Reviewer Entry

Reviewer 1

Comments:

Reviewer 2

Comments:

5. Organizational infrastructure

R5. The repository has adequate funding and sufficient numbers of qualified staff managed through a clear system of governance to effectively carry out the mission.

Compliance Level:

4 – The guideline has been fully implemented in the repository

Reviewer Entry

Reviewer 1

Comments:
4 – The guideline has been fully implemented in the repository
Accept

Reviewer 2

Comments:
4 – The guideline has been fully implemented in the repository
Accept

Response:

Over the past two hundred years, the KB has evolved into a scholarly institution of national and international renown. Since 2015, the KB also has a key coordinating role in the public library network. It employs almost four hundred members

of staff, its collection consists of seven million items, and around ninety thousand users visit the building every year.

With regard to its funding, the KB uses the “Three lines of defence” model. The business departments are responsible for their own financial management, including the preparation of budgets. The Internal Services Department provides advice and support in this connection. It also administers aspects as contracts, personnel data, and accounting. The GR&C (Governance Risk & Compliance) Department conducts independent legislative reviews and assesses compliance with other frameworks. In addition, external accountability procedures take place at the Ministry. The KB is an Autonomous Administrative Authority that reports to the Ministry of Education, Culture and Science. In accordance with the "Autonomous Administrative Authorities Framework Act" (2017), responsibility for political oversight of the KB rests with the Ministry of Education, Culture and Science. Details of the KB’s organisation, duties and funding are set out in the “Higher Education and Scientific Research Act (WHW)”. This law provides the necessary stability regarding organizational structure and funding to ensure long-term preservation. Every four years a new organization plan is submitted to the ministry. This specifies matters such as set objectives for the upcoming years, policy and preconditions regarding staff, accommodation, and budgets.

It is important to guarantee that there is sufficient in-house expertise and that all those stakeholders who should be involved in the long-term acquisition, processing, preservation, and accessibility of digital collections in the KB are, in fact, represented. To this end, the reference model from the SHAMAN project (A “Reference Architecture for Digital Preservation”, Gonçalo Antunes, José Barateiro, José Luis Borbinha, Published in iPRES 2010) is used. The stakeholders identified in this model were mapped to specific individuals and roles within the KB. This exercise showed that all stakeholders are, in fact, represented. The related roles include two preservation officers, researchers with expertise in areas such as file formats, and metadata specialists. Each of these individuals is an expert in their own field. They work in cooperation with counterparts at various national and international partner institutions. Also in adjacent areas of responsibility, like IT infrastructure and security, the KB has in-house subject matter experts such as programmers, database experts, architects and security specialists.

Any staff who are involved in digital preservation are expected to follow the ‘Learn how to Preserve’ training course. Special annual interviews are scheduled to enable members of staff to identify specific areas for personal development. In consultation with the manager, a budget can be allocated for courses, training courses, or conferences in their own field, to keep the staff’s expertise up-to-date. See R6 for an account concerning external expertise and knowledge building.

Supporting documents

Higher Education and Research Act (WHW): Relevant parts translated to English
https://www.kb.nl/sites/default/files/docs/higher_education_and_research_act_0.pdf
The complete law in Dutch: https://wetten.overheid.nl/BWBR0005682/2020-08-01
Strategic Plan: https://www.kb.nl/sites/default/files/docs/kbnb_beleidsplan-eng.pdf

An overview of all certification documents can be found at: http://www.kb.nl/certification

Reviewer Entry

Reviewer 1

Comments:

Reviewer 2

Comments:

6. Expert guidance

R6. The repository adopts mechanism(s) to secure ongoing expert guidance and feedback (either inhouse or external, including scientific guidance, if relevant).

Compliance Level:

4 – The guideline has been fully implemented in the repository

Reviewer Entry

Reviewer 1

Comments:
4 – The guideline has been fully implemented in the repository
Accept

Reviewer 2

Comments:
4 – The guideline has been fully implemented in the repository
Accept.

Response:

The KB's e-Depot draws on the expertise of internal staff. External advisers are sometimes hired, either on an ad hoc basis or in the context of temporary employment. In addition, the KB frequently cooperates with other parties, in international partnerships.

In the field of preservation, various internal roles specialise in acquiring knowledge and in harnessing it for advisory purposes, as described in R5. Externally, contacts with other institutions involve knowledge exchange in a range of areas. The KB is a member of (or participates in) a number of national and international partnerships. These include the Dutch Digital Heritage Network, IIPC, OPF, CENL, Ligue des Bibliothèques Européennes de Recherche (Liber), IFLA, UNESCO's PERSIST Programme, Research Data Alliance. In the area of standards (such those referred to in R11), the KB is represented on the METS Editorial Board (https://www.loc.gov/standards/mets/mets-board.html), the ALTO Editorial Board (https://www.loc.gov/standards/alto/community/editorialboard.html), and the NEN's 38004611 Standards Committee for Information and Archives Management.

In the area of IT, the KB has a wide range of expertise available in-house. There are network specialists for handling connectivity, ensuring network availability, installing servers and specifying plans for the layout of the network. Specifically related to security, there is a security officer and a Computer Security Incident Response Team. The KB also has in-house developers, database administrators and a supportdesk for IT related issues. Support is organized with a 1st line of support (the Supportdesk), a second line of internal specialists and a third line of specialists working for contracted suppliers. For IT maintenance continuity of required knowledge is guaranteed because as a policy knowledge is always shared between at least two employees. Also there is an entire team of architects that is responsible for making sure all the components within the enterprise architecture work together as a whole.

Knowledge is also exchanged with external parties concerning the standards referred to in R15. This takes place on the basis of the regular maintenance and support contracts for the various components of the e-Depot or, where necessary, via consultants hired on an ad hoc basis.

The KB presents an external account of its financial actions, by submitting its budget to the Ministry of Education, Culture and Science. Financial accountability takes place via the annual financial statements. Under the Framework Act, the annual financial statements must be accompanied by a report of the auditor's findings on whether the Autonomous Administrative Authority's management and organisation comply with the efficiency requirements. The annual report is also made public, in accordance with the Ministry of Education, Culture and Science format. See the list of annual reports: https://www.kb.nl/organisatie/organisatie-en-beleid/jaarverslagen (recent reports in Dutch only)

The exchange of expertise in the area of designated communities takes place in one of two different ways, depending on the target group (publishers and the general public).

Account managers are responsible for contacts with the publishers. They are the link between content strategy and the publishers' range of products. Account managers are responsible for the further growth of the e-Depot, in accordance with strategy. To this end, they maintain a network of contacts with publishers, while also creating support for the repository (by concluding and maintaining agreements with the Media Federation, for example), and preparing specific proposals concerning links.

Concerning the general public, there are various ways to gather information about this group's needs and requirements – online (via a web form), by telephone, and at the desk in the library. The KB also conducts regular customer satisfaction surveys, with regard both to generic services and to specific digital services. Finally, the KB has its own experts in the field of digital accessibility. If required, they can investigate the accessibility of services in the KB's usability lab.

Supporting document in the text.

An overview of all certification documents can be found at: http://www.kb.nl/certification

Reviewer Entry

Reviewer 1

Comments:

Reviewer 2

Comments:

DIGITAL OBJECT MANAGEMENT

7. Data integrity and authenticity

R7. The repository guarantees the integrity and authenticity of the data.

Compliance Level:

4 – The guideline has been fully implemented in the repository

Reviewer Entry

Reviewer 1

Comments:
4 – The guideline has been fully implemented in the repository
Accept level 4

Reviewer 2

Comments:
4 – The guideline has been fully implemented in the repository
Accept

Response:

The KB’s approach to the concepts of integrity and authenticity is outlined in its Digital Preservation Policy. The tactical formulation of these concepts is set out in the preservation plan. This defines the facets that need to be taken into consideration, as part of a comprehensive treatment of these concepts. This document also explains how these facets are linked to the relevant requirements in ISO 16363. The way in which these facets are subsequently implemented at operational level is described in a document entitled ‘Overzicht authenticiteit en integriteit’ (Summary of authenticity and integrity). A summary of this document is provided here. SHA-512-checksums are used for ensuring bit-integrity. Alternative methods of ensuring bit integrity are also valid if no checksum is delivered. Checksums are also used during ingest for verification after copying data. Different versions are ingested separately. It is currently not possible to maintain relations between these versions. Information Package (IP)-integrity is verified in the different steps of the ingest process. Specific checks are documented in the Submission Information Package (SIP) specification. There is no specific check for Dissemination Information Packages (DIPs) since these are in practice identical to the Archival Information Package (AIP).

To safeguard authenticity, source information and events are preserved as metadata. Details about which information is available is documented per ingest flow as can be seen in R12. Given the above-mentioned, highly detailed definition of the two concepts that underpin the three-level preservation policy, these three documents show exactly how this is handled throughout the objects' entire life cycle. They also describe the method used to guarantee verification of the completeness of the objects and of the collection, as well as checks of the objects' origin and provenance information, the management of different versions of the objects and any changes made to them.

Supporting documents
Digital preservation policy https://www.kb.nl/sites/default/files/docs/digital_preservation_policy_kb.pdf
Preservation plan https://www.kb.nl/sites/default/files/docs/preservation_plan_2019-2022.pdf
Summary of authenticity and integrity: https://www.kb.nl/sites/default/files/docs/overview_integrity_authenticity_kb.pdf

An overview of all certification documents can be found at: http://www.kb.nl/certification

Reviewer Entry

Reviewer 1

Comments:

Reviewer 2

Comments:

8. Appraisal

R8. The repository accepts data and metadata based on defined criteria to ensure relevance and understandability for data users.

Compliance Level:

3 – The repository is in the implementation phase

Reviewer Entry

Reviewer 1

Comments:
3 – The repository is in the implementation phase
Agree level 3

Reviewer 2

Comments:
3 – The repository is in the implementation phase
Accept

Response:

When determining which materials are to be included into the repository, the content strategy is leading. This document sets out the preconditions for inclusion and prioritises the various content groups.

The Digital Preservation Policy states that the original object must always be preserved. In the past, there was a clear management preference for objects in specific master formats. The drawback of this approach is that files are stored anyway even though in a non-preferred format. In addition, many files were preserved without verification, because verification software was only in place for preferred formats. In the preservation plan, the KB sets out a strategy of retroactive verification and technical metadata extraction to ensure that in the future the same format policy will apply to all files. The quality of the file formats will then be systematically checked and metadata stored, to enhance the monitoring of data quality. This does not mean that any and all formats will be accepted upon delivery, but rather that files delivered to the KB will, in any event, undergo long-term preservation. Full details are given in the document ‘File format guideline’. As an operational formulation of the Digital Preservation Policy’s principles, this document takes precedence.

The concept of ‘knowledge levels’ has been introduced into the File format guideline. The idea is to incorporate step-by-step quality improvements into a formal process, and to gradually improve the file format information linked to the objects. The aim is to boost the knowledge level regarding all of the formats in the archives, to provide a basis for systematising the process of functional preservation. To this end, the preconditions to be met at each knowledge level are defined. This will pave the way for format migration, if necessary, based on risk analysis and results from monitoring of the designated community.

The quality of the metadata is ensured by checks and transformations in the pre-ingest phase as described in R12. Submission agreements will be drawn up for depositors. When setting up a new ingest stream, these agreements will form the basis for an inventory of what can be obtained. These documents are also used for purposes of illustration, when informing depositors about the set requirements for proper processing. The metadata format is recorded during the connection process. Next, during the ingest process, the metadata is automatically checked on the basis of a schema.

If the data or metadata is not satisfactory, the business information managers can ask the depositor to deliver the material again. If the data is corrupt, then it will not be preserved. Instead, the administrators will request the correct version. If the material has already been preserved, then a new version will be added.

Supporting documents

Digital preservation policy: https://www.kb.nl/sites/default/files/docs/digital_preservation_policy_kb.pdf
Preservation plan: https://www.kb.nl/sites/default/files/docs/preservation_plan_2019-2022.pdf
Content strategy: https://www.kb.nl/sites/default/files/docs/content_strategy_eng.pdf
File format Guidelines: https://www.kb.nl/sites/default/files/docs/file_format_guidelines_kb.pdf

An overview of all certification documents can be found at: http://www.kb.nl/certification

Reviewer Entry

Reviewer 1

Comments:

Reviewer 2

Comments:

9. Documented storage procedures

R9. The repository applies documented processes and procedures in managing archival storage of the data.

Compliance Level:

4 – The guideline has been fully implemented in the repository

Reviewer Entry

Reviewer 1

Comments:
4 – The guideline has been fully implemented in the repository
Accept level 4

Reviewer 2

Comments:
4 – The guideline has been fully implemented in the repository
Accept

Response:

The archival storage component is responsible for preserving the AIPs, in the form in which they were created, following the ingest process. The preservation principles are described, at a high level, in the Digital Preservation Policy. The storage component is implemented by means of Silent Cubes, which handle AIP preservation and replication. In the context of the storage function, storage effectiveness is checked. This involves an ETL process that checks the checksums of all files, after they have completed the ingest process. This process is set up on a Pentaho server that is accessible to the e-Depot’s business information managers.

Storage is designed according to the Write Once Read Many principle. This means that files cannot be deleted or overwritten after storage, unless the producer intervenes. In addition to data consistency, this technology also provides protection against threats such as crypto viruses. In archival storage, there are no separate storage levels. Thus, all files are stored in accordance with the same storage policy. The storage environment is monitored by the IT Management Department, so timely notification is given of any storage medium failures. The built-in replication functionality, together with storage redundancy, ensures that no data is lost, even if more than one disk should fail. If that should happen, a

process is triggered in which the disk is replaced as quickly as possible. In cases like this, the Silent Cube's self-healing mechanism guarantees that the data is subsequently replicated correctly, and that no data is lost or corrupted. This mechanism generates a monthly integrity report from the Silent Cubes themselves, which also ensures that objects have not become corrupt during storage. Two servers are arranged in a master-slave setup, so even if an entire Silent Cube were to fail, this would not result in any data loss.

Vital infrastructural elements, such as databases, are also regularly backed up. These backups can then be restored in the event of an incident. The storage component can also fulfil the access function, as the stored files can be made accessible to the public (e.g. access to journal articles via ibl.kb.nl). There is an ongoing effort to optimise the storage infrastructure, based on risk assessments and new insights. This should result in a fully modernised storage environment in the near future, which will further enhance the long-term preservation of the digital collection. In this way, geographical distribution and redundancy are also taken into account.

Supporting documents
Digital preservation policy: https://www.kb.nl/sites/default/files/docs/digital_preservation_policy_kb.pdf

An overview of all certification documents can be found at: http://www.kb.nl/certification

Reviewer Entry

Reviewer 1

Comments:

Reviewer 2

Comments:

10. Preservation plan

R10. The repository assumes responsibility for long-term preservation and manages this function in a planned and documented way.

Compliance Level:

4 – The guideline has been fully implemented in the repository

Reviewer Entry

Reviewer 1

Comments:
4 – The guideline has been fully implemented in the repository
Accept

Reviewer 2

Comments:
4 – The guideline has been fully implemented in the repository
Accept

Response:

Preservation is enshrined in the KB's mission, as this states that the KB will make its own collection "visible, sustainable and accessible". The principles of preservation are set out at strategic level in the Digital Preservation Policy. Based on preservation themes that have been established in a national context, this policy specifies how OAIS requirements are applied within the KB. The strategic policy, in turn, forms the basis for various tactical-level documents, in which principles are formulated in detail. These documents also point the way for specific solutions at operational level. Finally, operational-level details have also been formulated within the various functions of the OAIS model, in the form of specific guidelines, agreements, and documentation. With regard to integrity and authenticity, for example, a description is available for steps within the ingest flows i.e. checks that are carried out on an operational level. The file format guidelines contain operational details on how the KB is planning to enhance knowledge on file formats in order to facilitate long term preservation. The contracts concluded with depositors contain the standard provision that the KB has the right to perform any action on objects it has received that is necessary for the long-term preservation of said objects. Another provision concerns the type of availability that is applicable to the objects in question. One of the most important tactical-level documents is the preservation plan. It contains a detailed formulation of what the KB means by 'authenticity', 'integrity' and 'long-term accessibility'. Building on these terms, the document goes on to explain how preservation levels and preservation strategies are used to guarantee long-term preservation. It also specifies the measures that have already been carried out to implement the policy. The document concludes with an action list. Together, these actions form the steps required to implement the policy principles and policy developments at operational level.

Supporting documents
Digital preservation policy: https://www.kb.nl/sites/default/files/docs/digital_preservation_policy_kb.pdf
Preservation plan: https://www.kb.nl/sites/default/files/docs/preservation_plan_2019-2022.pdf
Summary of authenticity and integrity https://www.kb.nl/sites/default/files/docs/overview_integrity_authenticity_kb.pdf
File format Guidelines: https://www.kb.nl/sites/default/files/docs/file_format_guidelines_kb.pdf

An overview of all certification documents can be found at: http://www.kb.nl/certification

Reviewer Entry

Reviewer 1

Comments:

Reviewer 2

Comments:

11. Data quality

R11. The repository has appropriate expertise to address technical data and metadata quality and ensures that sufficient information is available for end users to make quality-related evaluations.

Compliance Level:

4 – The guideline has been fully implemented in the repository

Reviewer Entry

Reviewer 1

Comments:
4 – The guideline has been fully implemented in the repository
Accept

Reviewer 2

Comments:
4 – The guideline has been fully implemented in the repository
Accept

Response:

During the intake of new depositors, agreements are reached concerning the format, content and frequency of delivery of data and metadata. Care is taken to ensure that the details provided include all of the information needed for the long-term preservation of the material. As part of the ingest process, automatic checks are carried out to verify that the metadata complies with the agreed specifications. A range of checks are also performed on the data. These include a zero-byte check and file identification, to confirm that the data has been supplied in a way that is compliant with the principles of authenticity. These checks are performed automatically, by means of scripting. The results of these checks are assessed by the e-Depot's business information managers. If any errors do occur, one option is to ask the depositor to deliver the material again. This is based on an assessment of the specific error in question, and on a risk assessment of that issue, with regard to preservation. The results of this check (such as file identification details) are also stored as metadata. The arrangements made with depositors are enshrined in agreements, see:
https://www.kb.nl/sites/default/files/docs/regeling_elektronisch_depot_nuv-kb_eng.pdf
With regard to the future, the aim is the long-term preservation of this information, in the context of information integrity. The Research Department and others are constantly working to expand and broaden their expertise regarding the file formats in the archives. Plans are also being made to expand the technical metadata, through the use of additional analysis tools for the various formats. This is the practical formulation of the tactical policy regarding file formats, as set out in the File format guideline. The following categories of metadata are stored: descriptive metadata, structural metadata, rights metadata, and technical metadata. This is stored according to the METS standard, which also includes other metadata schemas, such as MODS (for descriptive metadata) and PREMIS (for preservation-related metadata). This metadata is made available to the wider public via OAI-PMH (Open Archives Initiative Protocol for Metadata Harvesting). Various websites – such as Inter Library Loans and the Online Public Catalogue – also make metadata and

objects accessible to the public. The relevant websites also enable users to give feedback on the quality of data and metadata. Users can make use of this facility to report any deficiencies they have identified. The staff can then make appropriate modifications. In the future, the accessibility of the material and the metadata will also be assessed by means of user surveys. In the case of open access material, or where permission has been granted for them to obtain material, users can also obtain the entire AIP. Thus, comprehensive preservation metadata is provided, enabling the designated community to assess the integrity and authenticity of the material supplied. The KB's terms and conditions of use require users to include a source reference when using material which has been deposited in the library in accordance with the generally applicable conventions for citing literature. The KB also offers persistent identifiers in the metadata for citing purposes.

Supporting documents

Digital preservation policy: https://www.kb.nl/sites/default/files/docs/digital_preservation_policy_kb.pdf
Terms and conditions of use: https://www.kb.nl/en/services/conditions-of-use

An overview of all certification documents can be found at: http://www.kb.nl/certification

Reviewer Entry

Reviewer 1

Comments:

Reviewer 2

Comments:

12. Workflows

R12. Archiving takes place according to defined workflows from ingest to dissemination.

Compliance Level:

4 – The guideline has been fully implemented in the repository

Reviewer Entry

Reviewer 1

Comments:
4 – The guideline has been fully implemented in the repository
Accepted level 4

Reviewer 2

Comments:
4 – The guideline has been fully implemented in the repository

Accept

Response:

The KB uses four primary process steps:

Selection – Determining what to collect, reaching agreements, and managing them. This is based on the content strategy. Details of this process are set out in R2. R2 also describes the basis for selecting or deselecting materials, and the way in which agreements with depositors are recorded.

Processing – The intake and processing of supplied material, based on the agreements reached. Details of this process are set out in R8. R8 also contains references to every item of process documentation related to this step, including details of the checks carried out during the ingest process.

Preservation – Preserving publications for the long term, and making them retrievable. Details of this process are set out in R9. Further details of the way in which preservation is handled during this step are set out in R10.

Access– Making publications available to Designated Communities. R11 and R15 indicate how this function is performed, and how the quality of this process is safeguarded. R4 gives comprehensive details concerning the security and privacy of users and staff.

Any changes to workflows are implemented by Business Information Management, in accordance with BiSL (for details, see R15). The documentation is updated at each component release. Release notes are also available.

Further details per primary process step:

Selection
In accordance with the Content Strategy a list of potential data providers is compiled. The list is prioritised and the collecting of publications is planned. The data providers with the highest priority are contacted to provide their publications for the e-Depot. The Account manager tries to make an appointment to discuss the possibility to deliver the material to the KB. The Account manager and the Digital Preservation Officer discuss the delivery of the material according to the possibilities of the data provider and the preservation capabilities of the KB. If both parties agree to deliver material to the KB, sample files are provided. This way the ingest can be prepared by analysing the files and identifying the eventual gaps in the system to process the files. If there is a clear picture to process the files an agreement is discussed and eventually signed by the head of the Library and the data provider.

This process is more elaborate than that of other National Libraries, because there is a voluntary deposit law

Processing
When the agreement with the data provider is signed, the processing of the publications in the e-Depot can start.

The collection and processing of publications consists of three steps:

Collection

Pre-ingest

Ingest

Although the naming may suggest otherwise, all three of these steps fall under the OAIS functional component Ingest.

Below the three phases are further described. Through all three phases:

Information is logged about the status of the processing and errors that may occur. Errors are dealt with by the operational managers of the system on a daily basis. If the cause of the error lies in the publication itself, the publisher is asked to resubmit the publication.

Event metadata is generated of the events and added to the metadata record that will be stored in the e-Depot. An Agent Register is used to check if the version of the software that is used during processing is known in the Agent Register.

When data is moved from one system to the other it is checked for viruses.

Collection

During this phase mainly the functionalities that are part of the OAIS function Receive Submission are performed.

There are three methods to either collect or receive publications from a publisher:

SFTP;

OAI-PMH;

Manual deposit by the publisher through our Web deposit portal.

Most publications are either retrieved (FTP pull by the KB) or received (FTP push by publisher) using SFTP.

The metadata records of the scholarly publications of the institutional repositories are retrieved via the OAI-PMH protocol. The metadata record must comply with the agreements for the exchange of metadata of scientific publications

(https://www.edustandaard.nl/standaard_werkgroepen/werkgroep-metadata-subwerkgroep-wish/). The metadata records contain the URLs of the actual content files associated with the publication. These files are then downloaded from the repository. If the files cannot be downloaded, this is reported back to the repository. Metadata and publication are then both submitted to the pre-process mentioned below.

The KB offers a web deposit portal for the manual delivery of individual monographs or periodicals. The publisher can upload a publication and submit the required metadata via a number of webforms: https://www.kb.nl/en/organisation/for-publishers/depositing-publications/depositing-individual-digital-publications Metadata and publication are then submitted to the pre-process mentioned below.

Pre-ingest

Two system components are involved in this phase: the Pre-process component and the Connector component. They provide the functionalities that are part of the OAIS functions Quality Assurance and Generate Descriptive Info.

For all collections the following process steps are performed:

Check for empty files (0-byte check).

Check on the completeness of the submission.

Metadata check (well-formed and valid).

A persistent identifier (NBN) is assigned.

For publications that should be searchable in MDO (metadata storage database), an XLST transformation is done to create a metadata record in the required format for MDO.

The supplied metadata is also transformed using XSLT to the required format for the e-Depot’s Data Management component (OAIS Generate Descriptive Info) and the record is prepared for further processing by the Ingest component.

Process steps that are specific per collection:

For e-journals:

It is checked whether a descriptive metadata record of the journal title is present in the catalogue. If there is no catalogue record, it must be created first.

The PDF version is determined by reading the header information and the outcome is stored in the metadata.

For eBooks from commercial publishers:

It is checked whether the e-book was submitted before by using checksum information. If the checksum is the same, the publication is not further processed.

The version of the ePub file and PDF are checked and the outcome is stored in the metadata. For ePubs the ePubcheck tool is used (https://github.com/w3c/epubcheck). For PDFs the version information is read from the header of the file.

The ePub check tool is also used to extract technical metadata of the ePub file. The outcome is stored in the metadata.

It is checked whether the publisher of the eBook and the version of the version of the Epubcheck tool is known in the Agent Register.

An automatic matching process tries to match the submitted eBook to a bibliographical description in the catalogue. If an automatic match is not possible the Books is set aside for manual matching to a catalogue record. The metadata as supplied by the publisher is added to the metadata record in the catalogue. The full metadata record is then added to the publication that is processed for the e-Depot.

Web portal for individual deposit of monographs and periodicals:

It is checked whether the publication was submitted before by using checksum information. If the checksum is the same, the publication is not further processed.

The version of the ePub or PDF file is determined. For ePubs the ePubcheck tool is used (https://github.com/w3c/epubcheck). For PDFs the version information is read from the header of the file.

For periodicals only:

It is checked whether the publisher of the periodical is known in the Agent Register.

There is check to determine if a descriptive metadata record of the journal title is present and then pulling this record from the catalogue and adding it to the publication that goes into the e-Depot. If the record is not present in the catalogue, it must be created first.

Scholarly publications:

It is checked whether the publication was submitted before. If based on the checksum of the metadata and files, it is

concluded that there were no changes, the publication is not further processed.

The mime-type is determined using Apache Tika and it is compared to the file extension. If there is a difference between the mime-type and the related extension that cannot be explained, the repository is contacted and asked to explain the difference or change the extension.

It is checked whether the publisher of the publication and the versions of the Apache Tika and the Harvest software are known in the Agent Register.

Ingest

The Ingest module provides the functionalities that are part of the OAIS function Generate AIP and Co-ordinate Updates. The AIP is compiled on the basis of the files supplied by the pre-ingest (Generate AIP). The metadata (PDI) is written to the system's Data Management database (MDS) and the full AIP is offered to the Archival Storage component. A verification process checks whether both the AIP and PDI are correctly stored.

Preservation

Workflows for preservation purposes mainly revolve around measures taken to ensure bit integrity. Data is stored on an infrastructure that supports redundancy. Data is checked for bit corruption and reports are generated to verify this mechanism. More details on these storage components and bit integrity measures can be found in R9.

Access

As described in R2 the metadata supplied by the publishers determine the level of access. This is determined on the basis of a mapping, which takes the form of a translation table between supplied metadata values and one of the three authorisation levels within the system:

No access (in the event of an embargo on availability);

Restricted (used for publications that are only accessible to KB members on site in the KB);

Free (freely available without restrictions).

Unknown (default which means no access in practice)

A user will find a publication using one of the discovery methods as described in R13. A link containing the unique NBN will send the user to the system component DRAM (Digital Rights and Access Manager).

DRAM is the gateway to the e-Depot. DRAM also communicates with other system components such as the Digitaal Magazijn Web (DMW), MetaData Storage (MDS) and Archival Storage (AS) to check permissions and retrieve content.

DRAM checks the access level in the metadata of the requested publications in MDS. Combined with the user's IP address DRAM decides whether the user is granted access.

A user with an IP-addresses from KB personnel has access to all publications. Users with an IP-address from the KB reading rooms have access to publications with the access levels "free" and "restricted". All others users have access to publications with the access level "free" only.

If a user is not granted access, he will be presented with a page describing the reason for the denial.

If a user is granted access, he is transferred to the DMW system component. DMW is the presentation layer of the e-Depot. DMW will retrieve the necessary XML from MDS, translate is into HTML using stylesheets and return the requested page to the user. The page will show the publication's NBN, its title and access level, a copy right statement and a table of content showing the files that can be retrieved from Archival Storage. The table of content contains the files of the publication itself, the original metadata as supplied by the publisher and an AIP manifest as a METS file. If the user requests one of these files the DRAM component will check again if the user, based on its IP address and the access level of the publication, is allowed access.

Supporting documents

Content strategy: https://www.kb.nl/sites/default/files/docs/content_strategy_eng.pdf
Digital preservation policy: https://www.kb.nl/sites/default/files/docs/digital_preservation_policy_kb.pdf
Preservation plan: https://www.kb.nl/sites/default/files/docs/preservation_plan_2019-2022.pdf

An overview of all certification documents can be found at: http://www.kb.nl/certification

Reviewer Entry
Reviewer 1
Comments:
Reviewer 2
Comments:

13. Data discovery and identification

R13. The repository enables users to discover the data and refer to them in a persistent way through proper citation.

Compliance Level:

4 – The guideline has been fully implemented in the repository

Reviewer Entry

Reviewer 1

Comments:
4 – The guideline has been fully implemented in the repository
Accept

Reviewer 2

Comments:
4 – The guideline has been fully implemented in the repository
Accept.

Response:

The KB uses a range of data retrieval methods. The types of material that are accessible, and how these are accessed, differ from one collection to another. Retrievability is considered one of the key aspects of the overarching concept of long-term accessibility as stated in the preservation plan.

Every digitally published, monographic publication produced by foundations, associations, private individuals and minor publishers can be inspected on-site (on the KB's premises). Those that were deposited as an Open Access title can also be viewed remotely (off-site). There is a growing trend for e-books from commercial publishers to be deposited at the KB. However, this material is not yet available for inspection. In line with the relevant agreements, the e-Depot's existing facilities for making material available first need to be supplemented with additional security measures. The associated metadata is available, but any users who access it are informed that the material itself is not available.

The scholarly output of Dutch Universities and of various academic research institutions is held in long-term preservation at the KB, but this cannot yet be retrieved from the e-Depot. Digital articles from a number of major academic publishers can be inspected on-site (on the KB's premises), via the e-Depot's Digital Library. The publishers in question include Elsevier, Springer, Koninklijke Brill, IOS Press, Biomed Central, Blackwell Publishing, Directory of Open Access Journals (DOAJ), International Union of Crystallography (IUCr), Mary Ann Liebert, Oxford University Press, Sage Publications and Taylor & Francis. Some of these publishers are not active anymore but we still preserve publications that have been ingested previously. Periodicals that are deposited at the KB as individual issues are not yet available for inspection at the library.

Monographs and journals are search-enabled and retrievable at metadata level (based on the descriptive metadata provided) via the KB's own catalogue interface (the Online Public Catalogue or OPC). They are also search-enabled via

the external WorldCat Discovery repository. Books, journals and newspapers are also externally registered in the National Bibliography, via the Online Computer Library Center (OCLC). The collection of scholarly articles is search-enabled, via Inter Library Loans. These are registered externally, in the Keepers registry (a global monitor on archiving arrangements for electronic journals).

At intake, publications are assigned a persistent identifier (NBN). If a publication has already been assigned an NBN by its publisher, no new NBN will be assigned. Any other persistent identifiers that may be provided, such as DOI, are also stored as metadata. See https://www.kb.nl/organisatie/onderzoek-expertise/informatie-infrastructuur-diensten-voor-bibliotheken/registration-agency-nbn/principes (in Dutch only) for details of the principles governing the allocation and management of NBNs, and of the quality guidelines that NBNs must meet. The KB's terms and conditions of use require users to include a source reference when using material that has been deposited with the library.

To protect the interests of rights holders (see R0, 1, 2, 4), any digital publications that have been deposited can generally only be inspected on-site (on the KB's premises), for the purpose of study and research. Any visitors wishing to inspect material in the KB's reading room, must first register as a member and agree to the KB's membership conditions, which impose conditions on the use of digital files.

The KB also offers a range of options for harvesting metadata. Descriptive metadata can be harvested from the e-Depot set via the KB's data architecture (KBGA), which supports OAI-PMH and SRU protocols.

Supporting documents

Conditions of use: https://www.kb.nl/en/services/conditions-of-use
Online Public Catalogue: https://opc-kb.oclc.org/
Dutch Bibliography: https://picarta.on.worldcat.org/discovery
Keepers: https://keepers.issn.org/
NBN registration: https://www.kb.nl/organisatie/onderzoek-expertise/informatie-infrastructuur-diensten-voor-bibliotheken/registration-agency-nbn/principes
OAI-PMH: http://services.kb.nl/mdo/oai
SRU: http://jsru.kb.nl/sru/
Inter Library Loans catalogue: http://ibl.kb.nl/
Data services: https://www.kb.nl/en/resources-research-guides/data-services-apis

An overview of all certification documents can be found at: http://www.kb.nl/certification

Reviewer Entry

Reviewer 1

Comments:

Reviewer 2

Comments:

14. Data reuse

R14. The repository enables reuse of the data over time, ensuring that appropriate metadata are available to support the understanding and use of the data.

Compliance Level:

3 – The repository is in the implementation phase

Reviewer Entry

Reviewer 1

Comments:
3 – The repository is in the implementation phase
Accept

Reviewer 2

Comments:
3 – The repository is in the implementation phase
Accept

Response:

The Digital Preservation Policy's stated goal is to ensure the long-term usability of the objects. This is formulated in detail in the preservation plan, under the concept of 'accessibility' which is used as an overarching concept also covering aspects of usability. The way in which this concept is defined in the preservation policy means that various aspects need to be explored to determine whether a given item can be considered sustainably accessible and reusable. Accessibility in this sense is defined separately from the legal component, which also needs to be taken into consideration in all aspects relating to accessibility. In short, while the object must be accessible and reusable to users, this should not automatically mean that it can be made freely available, in terms of copyright. Further details of how the legal aspects associated with the objects are handled are set out in R2. Accessibility, in this sense, is determined on the basis of the following aspects: retrievable, readable, interpretable, reliable, and available. This means that users must be able to find material using metadata, it must be possible to display any object found, an object's contents must be comprehensible, the user must be able to determine an object's integrity and authenticity, and it must be possible to issue an object as a DIP. These aspects combined should guarantee long-term usability by covering understandability of data and metadata and file format obsolescence among other things. If user surveys show that these principles can no longer be met, the preservation plan sets out the measures needed to restore quality to the appropriate level for users. This could mean adding extra context information, if the designated community feels that use of the term 'interpretable' can no longer be fully justified. The preservation plan sets out various strategies to provide ongoing, long-term guarantees for these aspects. The File format guideline is specifically intended to guarantee the readability of formats. It implements the principles relating to knowledge levels, which are set out in the preservation plan. The aim is to use knowledge building and analysis to obtain a better

understanding of the various formats, thus paving the way for functional preservation.

Supporting documents

File format guideline: https://www.kb.nl/sites/default/files/docs/file_format_guidelines_kb.pdf
Preservation plan: https://www.kb.nl/sites/default/files/docs/preservation_plan_2019-2022.pdf

An overview of all certification documents can be found at: http://www.kb.nl/certification

Reviewer Entry

Reviewer 1

Comments:

Reviewer 2

Comments:

TECHNOLOGY

15. Technical infrastructure

R15. The repository functions on well-supported operating systems and other core infrastructural software and is using hardware and software technologies appropriate to the services it provides to its Designated Community.

Compliance Level:

4 – The guideline has been fully implemented in the repository

Reviewer Entry

Reviewer 1

Comments:
4 – The guideline has been fully implemented in the repository
accept

Reviewer 2

Comments:
4 – The guideline has been fully implemented in the repository
Accept

Response:

The e-Depot as a whole is modelled on the Open Archival Information System's (OAIS) functional model, which features clear components for ingest, archival storage, and access. The various software components run on broadly supported operating systems whose software is regularly updated. The servers run Red Hat Enterprise Linux and Windows Server.

Ingest

The ingest function retrieves material using GoAnywhere (an FTP solution), OAI-PMH (Open Archives Initiative Protocol for Metadata Harvesting), or custom scripting for retrieving data via remote FTP servers. Next comes the pre-ingest process, which involves a number of checks based on shell scripting. The ingest application is a Java application that was developed in-house. Processes such as metadata mapping take place in the connector, based on XSLT. These are based on software developed and supported by a supplier by the name of '42'.

Data management

Metadata is stored in a relational database in the MDS component. This data is also stored in an MDO database, for the purpose of making material available. The database used for both MDS and MDO was implemented in the Oracle database.

The database schema is documented and maintained in-house.

Archival storage

Data is stored on a Silent Cube disk storage system, based on the WORM principle. A support contract for this system has been concluded with the supplier.

Access

To make the material accessible, metadata is supplied to the integration component named KBGA (KB data architecture). The KBGA's OAI-PMH provider enables the data to be used in services. This API contains the resolver, which enables information objects to be retrieved by means of their persistent identifiers. In this service, the information objects themselves are supplied from the Silent Cube. The Inter Library Loans browsing tool (http://ibl.kb.nl) is a service that is based on this API.

As previously stated, the above software was largely developed in-house. The processes and scripting are sufficiently well understood and documented for us to maintain the system. Occasionally, changes have to be made to the infrastructure, based on producer-related changes or improvements proposed by the internal organisation. This is based on a structured change management process that is directed by IT Service Management, in accordance with the Information Technology Infrastructure Library (ITIL) process. A Development, Testing, Acceptance and Production (DTAP) environment has been set up to test functionality before going into production. There is also a release process, in which release notes are created. Product management has also produced a roadmap and a development plan, to facilitate responses to any

technological developments. There is a list of services, which also identifies the software required for the service in question. The system uses standards such as OAI-PMH for ingest and access, SRU for searching metadata, and XSLT for metadata mapping. The servers are monitored to ensure that any potential connectivity problems are identified in time and that there is sufficient bandwidth available to implement the services. In addition, aspects such as storage capacity are monitored. The management organisation's structure is in keeping with principles derived from international standards, such as ITIL and BiSL.

Glossary of terms used in the text above:
OAI-PMH: Open Archives Initiative Protocol for Metadata Harvesting
XSLT: Extensible Stylesheet Language Transformations
KBGA: Software developed by the KB that combines different pieces of software. They are used as an integration layer. It includes
* MDO: Metadata database for integration layer
* Sesam: Access rights application
* Web storage: storage for our access copies of our digital collection
* Resolver: URL resolver, resolves our persisntent identifiers
Silent Cubes: Archival Storage
ITIL: Information Technology Infrastructure Library
BiSL: Business Information Services Library
SRU: SRU- Search/Retrieve via URL
DTAP: Development, Testing, Acceptance and Production environment
MDS: metadata database for our e-depot
WORM: Write once read many

Reviewer Entry

Reviewer 1

Comments:

Reviewer 2

Comments:

16. Security

R16. The technical infrastructure of the repository provides for protection of the facility and its data, products, services, and users.

Compliance Level:

4 – The guideline has been fully implemented in the repository

Reviewer Entry

Reviewer 1

Comments:
4 – The guideline has been fully implemented in the repository
accept

Reviewer 2

Comments:
4 – The guideline has been fully implemented in the repository
Accept

Response:

As stated in the Digital Preservation Policy, the KB has adopted a wide-ranging approach to security. Policy documents have been drawn up for the various types of risks identified in the above policy. These documents specify the guidelines and procedures to be followed in the event of an incident. In the area of IT security, an information security policy document has been drawn up. This contains guidelines to mitigate threats from internal and external attacks, for example. In this context, server hardening is used to ensure that systems have fewer vulnerabilities that could be exploited by malicious parties. A data classification system has been drawn up for the e-Depot. It indicates how the risks associated with data are classified, and what this means in terms of the required level of protection. The systems also make use of rights and roles, to ensure that users do not have more rights than are strictly necessary for the performance of their duties. A checklist has been drawn up to assess agreements reached with external producers. This checklist features a range of principles that are intended to guarantee the privacy and security of users. Within the organisation, security considerations have prompted the creation of a Computer Security Incident Response Team. This team is a contact point for security incidents and data breaches. The team also handles the follow-up to any matters that have been reported. The in-house Chief Information Security Officer has overarching responsibility for all such matters. This team also actively monitors the situation, and submits reports that provide a basis for further improvements. In addition, all members of staff receive basic training (in the form of online training courses) in the area of security, which also focuses on their own responsibilities in this area. This also includes measures to safeguard physical access security. In addition to IT security, consideration is given to risks in other areas. For instance, a Company Emergency Response Plan and a Company Emergency Plan have been drawn up for accidents such as fire and external physical threats. These plans set out the procedures to be followed, together with details of the corresponding arrangements within the organisation. There is also a Disaster Recovery Plan, specifically for dealing with the impact that situations like this could have on the collection.

Supporting documents

Information security policy (Dutch only and send as confidential document)
Management summary Information security policy:
https://www.kb.nl/sites/default/files/docs/information_security_policy_summary_0.pdf
Privacy and security checklist (Dutch only and send as confidential document)
Company Emergency Plan (Send as confidential document)
Digital preservation policy: https://www.kb.nl/sites/default/files/docs/digitaal_preserveringsbeleid_kb_def.pdf

DPA (Send as confidential document)

An overview of all certification documents can be found at: http://www.kb.nl/certification

Reviewer Entry

Reviewer 1

Comments:

Reviewer 2

Comments:

APPLICANT FEEDBACK

Comments/feedback

These Requirements are not seen as final, and we value your input to improve the CoreTrustSeal certification procedure. Any comments on the quality of the Requirements, their relevance to your organization, or any other contribution, will be considered as part of future iterations.

Response:

Reviewer Entry

Reviewer 1

Comments:

Reviewer 2

Comments: