Regionaal Archief Alkmaar

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:
Accept

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:

Archive

Reviewer Entry

Reviewer 1

Comments:
Accept

Reviewer 2

Comments:
Accept

Brief Description of Repository

Regionaal Archief Alkmaar (RAA) is a joint arrangement that operates within a large region in the province of Noord-Holland. The first purpose of this arrangement is to fulfill the function of a regional knowledge and information center through the acquisition and preservation of a broad collection of historical sources. The second purpose is to make these sources actively available. It does so according to the Dutch Public Records Act (Archiefwet 1995).

At the time of writing, the joint arrangement services include 9 municipalities, namely: Alkmaar, Bergen, Castricum, Den Helder, Heiloo, Hollands Kroon, Schagen, Dijk en Waard and Texel. The arrangement also includes other joint arrangements. These are the GGD Hollands Noorden and Veiligheidsregio Noord-Holland Noord. Also, the RAA keeps the archives of the water authority Hoogheemraadschap Hollands Noorderkwartier and its predecessors. This is being done on the basis of a service agreement.

Finally many archives of families, persons of interest, companies and non-governmental organizations are being collected and managed. This is a secondary task of the RAA, but these archives are also being managed on the ground of the Dutch Public Records Act.

Reviewer Entry

Reviewer 1

Comments:
Accept

Reviewer 2

Comments:
Accept

Brief Description of the Repository’s Designated Community.

The RAA focuses on five designated communities. In its Preservation Policy (“Preserveringsbeleid”, chapter “Toegang”, https://archiefalkmaar.atlassian.net/wiki/spaces/WRAA/pages/1409025/Toegang) these communities are further explained.

In short, the five designated communities are part of two main groups:

Users of governmental records: the producer of a governmental archive, other governmental departments, and civilians searching for prove and justice.

Users of records created by private producers: the producer of a private archive, users interested in cultural heritage.

We choose to specify these groups, as they have different wishes as well as different access rights to the archives. By learning about these wishes and rights, the RAA ensures to provide the best experience in consulting the archives (see below).

The RAA uses different strategies in making the archives accessible for each community. To give an example: A user working in a governmental organization and needing a technical file (AutoCAD for instance) will not be happy with a plain text PDF file without technical details, whereas a civilian with an interest in cultural heritage may not be able to consult a technical file. In this case we will make sure that both files are acquired and managed in the digital repository. That way, both types of consumers can be provided with either the basic information or the technical file for expert use.

Knowledge about the wishes of the designated communities is important for the RAA and will be obtained in different ways. Customer satisfaction surveys are being conducted regularly to measure how happy the designated communities are with the services the RAA provides. At the same time, information and other insights are gathered by exchanging experiences with other archival institutions (national and international) and by consulting relevant literature on the subject.

Reviewer Entry

Reviewer 1

Comments:
Accept

Reviewer 2

Comments:
Accept

Level of Curation Performed. Select all relevant types from:

A. Content distributed as deposited, B. Basic curation – e.g. brief checking; addition of basic metadata or documentation, C. Enhanced curation – e.g. conversion to new formats; enhancement of documentation, D. Data-level curation – as in C above; but with additional editing of deposited data for accuracy

Reviewer Entry

Reviewer 1

Comments:
Accept

Reviewer 2

Comments:
Accept

Comments

Content distributed as deposited;

Most of our content is distributed as it is deposited. This means that the municipalities deliver the data to RAA and RAA ingests this data into the repository exactly as the municipalities have delivered it to us. This does not mean that there are no quality measures taken before RAA deems it ready for ingesting. RAA works closely with the municipalities to achieve that level of quality. As stated in the Digital Preservation Policy of RAA (hoofdstuk Digitaal Object, https://archiefalkmaar.atlassian.net/wiki/spaces/WRAA/pages/1015853/Digitaal+object), RAA has a list of file types with preferred and accepted file formats to which they must comply.
Basic curation – e.g. brief checking; addition of basic metadata or documentation;

Next to filetypes, there is certain metadata that the RAA requires for every file before ingesting, to meet the quality requirements. RAA commits to the Dutch governmental national metadata standard; Toepassingsprofiel Metadatering Lokale Overheden (TMLO: https://bit.ly/3hzli7b). This metadata standard gives context to the files and structure to the big data storage in the repository. Thanks to this standard, files can still be found, by searching for keywords, and consulted at a later moment in time. RAA furthermore advises on publication of the files regarding the compliance with the European GDPR. This decision is stored in the metadata too. As the municipalities keep ownership of the data, they are responsible for the correct definition of this metadata field.

Enhanced curation – e.g., conversion to new formats; enhancement of documentation;

If the measures decribed above, are met, the data can be ingested into the repository. During this stage, the repository checks all the file types to see if there are newer common file formats available. If a newer common file type is available, the repository will convert the file to the new file format and will store this copy together with the original file. As stated in the digital preservation policy of RAA (hoofdstuk Functionele Preservering, https://archiefalkmaar.atlassian.net/wiki/spaces/WRAA/pages/1114113/Functionele+preservering), RAA never changes the original deposit file. RAA only adds the newer common filetype to the repository.

Data-level curation – as in C above; but with additional editing of deposited data for accuracy.

Even after the above processes, data in the repository can be in need of editing. For example, if a specific field needs a more accurate explanation. Before RAA makes adjustments to the data in the repository, RAA investigates the changes that need to be made and how this affects the collection. Based on the findings, RAA advises the municipalities on the right course of action carries out these changes. All these modifications are recorded in the repository, as explained in the digital preservation policy of RAA (chapter Toegang, https://archiefalkmaar.atlassian.net/wiki/spaces/WRAA/pages/1409025/Toegang).

Reviewer Entry

Reviewer 1

Comments:
Accept

Reviewer 2

Comments:
Accept

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

RAA has two outsource partners concerning the repository; Picturae Holding B.V. (https://bit.ly/2T1f3yK) and MvBWorks (https://bit.ly/3wjlY4M).

Picturae Holding B.V. supplies the software, storage, and hosting of our repository. RAA is registered as a beneficiary of the Picturae Escrow Arrangement (https://bit.ly/3otTfr7) which applies to all the services from Picturae Holding B.V. (https://bit.ly/3hCtfIB) such as the preservation of collections (https://bit.ly/3yrqhwO). This is in case the continuity of Picturae Holding B.V. is threatened. Picturae Holding B.V. is also ISO 9001:2015 (https://bit.ly/3wd31jS) certified (quality management) and utilizes a security management system that complies with the requirements of the information security standard ISO 27001:2017 (https://bit.ly/3u2vKqn). Both certificates are added to the CTS application as attachments.

RAA has commissioned MvBWorks to write the software tool 'Topx Creator' (https://bit.ly/33XTMrO) which is used as a pre-ingest application for our repository. The tool is built to be used with the Dutch governmental national metadata standard; Toepassingsprofiel Metadatering Lokale Overheden (TMLO: https://bit.ly/3hzli7b), but can adjusted to fit different standards like the upcoming; Metagegevens Duurzaam Toegankelijke Overheidsinformatie (MDTO: https://bit.ly/3ote7ia) through redevelopment of MvBWorks. The tool is specifically written for our type of repository. RAA advises the supplying municipal administrations to check and add metadata with this tool to ensure a correct ingest of the metadata. Through this application, our participating municipalities can create a TopX-file (https://bit.ly/2HjWFLP) supplementary to their data Combined, these files form the SIP, which will be ingested into our repository.

Artefactual, the supplier of the Archivematica digital preservation software is no outsourcing partner of het RAA. Picturae delivers the software as a service. This firm is in direct contact with Artefactual. The RAA has no direct contact with Artefactual.

Reviewer Entry

Reviewer 1

Comments:
Accept

Reviewer 2

Comments:
Accept

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

- Reviewers suggestions for spelling are accepted and applied.
- R13's level of application is changed from level-4 to level-3.
- Picturae's ISO 27001:2017 and ISO 9001:2015 certificates are added as attachment for proof of compliancy.
- Declaration added as to why Artefactual is no outsourcing partner of the RAA (R0).
- Two registries where the RAA is listed are added to 'Other Relevant Information'.
- Link to the Dutch Digital Heritage Network is added in R10.
- Extra information added to R12 on pre-ingest checks.
- At R16 the section on redundancy storage is added.

- English summary of Preservation policy (https://archiefalkmaar.atlassian.net/wiki/spaces/WRAA/pages/29458433/Digital+Preservation+Policy+RAA+English+summary) and Continuity plan (https://archiefalkmaar.atlassian.net/wiki/spaces/WRAA/pages/29294593/Continuityplan+RAA+English+summary) are available online.
- Confluence environment made public, so the preservation policy and continuity policy is now public.

Reviewer Entry

Reviewer 1

Comments:
Accept

Reviewer 2

Comments:
Accept

Other Relevant Information.

An English summary of the Preservation Policy is available here: https://archiefalkmaar.atlassian.net/wiki/spaces/WRAA/pages/29458433/Digital+Preservation+Policy+RAA+English+summary

An English summary of the Continuity Plan is available here:
https://archiefalkmaar.atlassian.net/wiki/spaces/WRAA/pages/29294593/Continuityplan+RAA+English+summary

The RAA is listed in the following registries:
Archives Portal Europe: https://www.archivesportaleurope.net/nl/directory/-/dir/ai/code/NL-AmrRAA
Wikimedia Commons: https://commons.wikimedia.org/wiki/Category:Media_from_Regionaal_Archief_Alkmaar

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 mission of the RAA is as follows: ‘The Regional Archive Alkmaar enables people to have access to and learn about the history of Alkmaar, Bergen, Castricum, Den Helder, Heerhugowaard, Heiloo, Hollands Kroon, Langedijk, Schagen and Texel with ease and in an attractive fashion. For connected governmental organisations the Regional Archive Alkmaar is a professional partner that keeps information in a prolonged reliable and accessible state for the sake of business operations, proof lining, investigation and democratic control. It does so, according to the current legislation.’ (Tijdreizen: Beleidsplan_Tijdreizen.pdf (regionaalarchiefalkmaar.nl).

The mission is largely based on the Public Records act and is focused on both the access and preservation of digital archives, as well as analog archive.

In the policy plan ‘Tijdreizen, Beleidsplan Regionaal Archief Alkmaar 2019-2022' and in all other policies the method for preserving digital information is named e-depot. This is a term that stands for the following: “An e-depot is the entirety of organization, policy, processes and procedures, financial management, personnel, data management, data security, and available hardware and software, which enables sustainable management and consultation of digital archive objects to be stored.” (Nationaal Archief: https://bit.ly/3aF6yQI). Whenever digital preservation is mentioned, the term e-depot is used to embody the act of digital preservation as a whole and not just as a technical solution.

Reviewer Entry

Reviewer 1

Comments:

Reviewer 2

Comments:
Accept

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:

Archives from governmental institutions under the stewardship of RAA are public and can be consulted by users unconditionally on the grounds of the Public Records Act. There are no licenses or admission criteria. At most, it is possible to impose publication restrictions on some files for a specific period of time on the grounds of Articles 15, 16, and 17 of the Public Records Act. The municipality indicates which files are subject to publication restrictions, for what period, and on what grounds the restrictions are in place. As mentioned in the digital preservation policy from RAA (chapter Rechten, https://archiefalkmaar.atlassian.net/wiki/spaces/WRAA/pages/1212417/Rechten), reasons for restriction can be due to copyright or the GDPR.

The municipality makes these decisions based upon the following criteria:

Respect for personal living conditions/quality of life

The interests of the State and its allies

Disproportionate advantage or disadvantage

If restrictions on access to the files are imposed due to copyright, then this must be included in the metadata. As mentioned in the digital preservation policy of RAA (chapter Rechten, https://archiefalkmaar.atlassian.net/wiki/spaces/WRAA/pages/1212417/Rechten), this is added in the metadata by a copyright start and end date, to avoid disputes regarding the publishing of the records. Additional conditions can be added to the metadata as well, such as 'reuse under conditions' or 'ban on reuse until 75 years after the death of the author'. Thanks to this metadata, the system knows exactly when the files can be made public.

As mentioned in R0, the municipalities remain the owner of the data and are therefore responsible for the displayed content. The municipalities need to verify in the metadata whether the files are copyrighted. The repository of RAA makes the files technically visible or hidden based on this metadata. If the copyright date has passed, the files become public. If someone wishes to peruse one of the copyrighted files during the copyrighted period, a request must be made to the management of the RAA. They determine whether the data can be viewed or not. If the request is granted, the files will be handed over to the requestor with a disclaimer that the files are meant for personal use only and are not to be distributed.

As for files from the public domain, the same process as mentioned in R0, applies. This means idealy that they need to be completely donated (including the copyright) to the RAA, before RAA will add them to the repository. In some cases, the RAA cannot know whether the works are copyrighted. In those cases, if the work is of interest to the RAA, the not kowing is seen as a calculated risk in the part of the RAA.

All the governmental institutions that are part of the joint arrangement, must sign a service agreement (e-depotcontract) with RAA for the first stage of using the e-depot services. The services around the e-depot are not yet incorporated in the joint arrangement. This will be done when all the governmental institutions are using the services to some degree. At that point, the e-depot services are in line with all the other services that the archival institution provides for the connected governmental organizations.

Reviewer Entry

Reviewer 1

Comments:

Reviewer 2

Comments:
Accept

3. Continuity of access

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

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 continuity of operation of the repository is guaranteed through its statutory task. The Public Records Act stipulates that all governmental institutions should designate a repository. Archives are deposited, managed, published, and made available through the repository. Nevertheless, a wide range of threats may obstruct the continuous operation of the repository.

To prevent threats and implement appropriate measures RAA has a continuity plan. This plan describes that the RAA ensures there is enough capacity, funding and methods to make sure that adequate measures can be taken for continuitity. Technical back-up and security measures will be further explained in R9, R15, and R16.

The RAA has a digital preservation policy. This is a tactical continuity plan. It describes measures and actions that are taken when a threat occurs to maintain the preservation goals and it shows the level of knowledge that is embedded in the organization.

The Service Level Agreement between Picturae Holding B.V. and RAA can be consulted via https://bit.ly/2WGo7aC. This agreement ensures that the supplier takes all the measures needed to maintain, secure and provide the collections for continuous access.

The measures described below are designated a high risk in the digital preservation policy of RAA and have been implemented:

RAA is registered as a beneficiary of the Picturae Escrow Arrangement. The source codes and documentation of the application curated by the escrow agent, will be given to the owner of the data (RAA). This means that RAA can completely export the data from the Picturae Holding B.V. repository and import the data into a different repository hosted by another institute, if or when Picturae Holding B.V. is unable to do so.

The Service Level Agreement (SLA) with Picturae contains agreements on performance, processes, and procedures for the following aspects: back-up & restore, fixity controls, exit-strategy, service provision, and hosting.

Organizational and financial continuity of RAA is imbedded in the joint arrangement Regionaal Historisch Centrum Alkmaar and is specified in the continuity plan and preservation policy.

The statutory task of RAA obliges the organisation to maintain a repository. RAA is designated as the repository based on the archival regulations of the participating depositors: the governmental organizations. Medium-term plans are to connect all adjoined governmental organizations to our repository through a manual ingest procedure. This means that all organizations must have established a manual transmitting connection with our repository, through which they can store files conforming to the Public Records Act. This can be done by using the TopX-Creator or by creating export tooling within the document management systems that are being used within the organization.

For the long-term, RAA has plans to create a stable and continuous digital connection between the municipalities and RAA, which will result in the automatic transfer of files. RAA has already taken measures for this long-term strategy by creating a universal connector in the repository to which the municipalities can connect their Document Management Systems. The first talks are already being held for the use and further development of this connection.

Reviewer Entry

Reviewer 1

Comments:

Reviewer 2

Comments:
Accept

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 principle, the digital files that RAA manages are public records, according to the law under the Public Records Act. At most, it is possible to impose publication restrictions for a certain period of time. The depositor indicates the documents to which the restrictions apply, for what period, and on what grounds. The repository of RAA complies with this by excluding the files from the public domain during this period.

Apart from the Public Records Act, governmental institutes are subject to the General Data Protection Regulation; GDPR (https://bit.ly/3nR4UiK) from the moment they bring data into the public domain. The Public Records Act and GDPR conflict with each other. The Public Records Act is geared to active publication and according to the GDPR, you may only publish (process) the minimal amount of data that is required to complete the task. The GDPR prescribes that organizations must be cautious with the publication of personal data and of course, archival documents may contain a great deal of personal data. However, the restriction on personal data only applies to living persons. Therefore, RAA does not actively publish files with personal data which have been created within the last 100 years on the ground of the GDPR regulation and 75 years according to the Public Records Act. RAA has multiple procedures for this, such as a random check of files during ingest into the repository.

The depositors themselves have accurate procedures concerning personal data as well. They store security checks in organizational and technical procedures conforming to the security standard for governmental institutions called; Baseline Informatiebeveiliging Overheid (BIO: https://bit.ly/3vM0226). BIO is a security standard based on ISO 27001:2017, and ISO 27002:2017. This security standard has multiple requirements concerning privacy, such as required Data Processing Agreements with IT-suppliers and privacy by design demands for applications and systems.

To ensure that the repository of RAA only publishes files that are allowed to be published, the system needs to know for each file that is about to be ingested, which value (public or hidden) applies. Therefore, RAA has created a specific field in the metadata files that are part of the SIP during ingest. This is an extra field for each file and contains the value hidden or public. Thanks to this procedure the system knows exactly which files need to be published and which files do not. To commit to this procedure the municipalities deliver the correct criteria in the metadata through their own systems or manual by responsible experts. It is only possible to deviate from this if the executive council receives written permission from the depositor. In case of a complaint, RAA will forward this issue to the depositor for further settlement.

The host institute Picturae Holding B.V. takes the necessary technical security measures to prevent any unauthorized access or data leaks from the repository application. Picturae Holding B.V. is ISO 27001:2017 compliant and works by its procedures. Proof of certification is added to the CTS application as an attachment.

Reviewer Entry

Reviewer 1

Comments:

Reviewer 2

Comments:
Accept

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:

The continuity of financial resources to maintain our repository is guaranteed due to its statutory task. The Public Records Act prescribes that all governmental institutions must designate a repository. Archives (regardless of form) are curated, managed, made accessible and available through the repository. The available financial resources are included in the long-term budget of the organization's joint arrangement Regionaal Historisch Centrum Alkmaar. The budget is reviewed yearly. This guarantees that the funds are sufficient enough to keep the repository up-to-date.

The technical management of the software, storage, and hosting of the repository is provided by Picturae Holding B.V. This company is specialized in the digital management and disclosure of heritage collections. Since 2005 RAA and Picturae Holing B.V. cooperate on the development of our heritage portal. Over those years Picturae Holding B.V. has proven to be a trustworthy partner and in 2016 RAA started the co-development of the current repository with an ever-growing clientele.

Thanks to those developments Picturae Holding B.V. has become a managed hosting provider. They use their own facilities in Heerhugowaard and the data center Global Switch in Amsterdam. All data storage is mirrored, and Global Switch is the primary site. Picturae Holding B.V. uses the Information Security Management System from the ISO 27001:2017 standard which is applicable to the long-term storage of digital heritage. Proof of certification is added to the CTS application as an attachment.

The RAA reserves the annual budget for the repository and sufficient funds for staff, IT resources, and education. The staff keeps their knowledge up-to-date by attending courses and seminars. Together this guarantees a stable organization to maintain and continue the development of the repository in accordance with the policy plan 'Tijdreizen, 2019-2022'. As mentioned in our digital preservation policy (hoofdstuk Organisatie, https://archiefalkmaar.atlassian.net/wiki/spaces/WRAA/pages/1376257/Organisatie) RAA has the following roles defined for staff that focus on the sustainability of the repository:

Information Consultant (Adviseur Digitale Informatievoorziening)
Functional Consultant (Functioneel beheerder)
Consultant Archives and Services (Adviseur Dienstverlening en Archief)
Digital Preservation Officer (Functionaris Digitale Duurzaamheid)
Chief Information Security Officer
Data Protection Officer
Policy Officer
Managing Director (Directeur)

The staff is responsible for maintaining the sustainability of the repository, the continuous influx of digital files, up-to-date security, testing and implementing new functionalities, forming a digital strategy, forming a digital preservation policy, and making digital information available. The range and depth of expertise of both the organization and its staff contribute to the National Archive knowledge base KIA (https://kia.pleio.nl/). They organize and join multiple meetings to exchange knowledge and gain expertise on archival and repository subjects.

Besides financial stability, trusted cooperation with Picturae Holding B.V., well-educated staff, and contributing to the national archival community, the organizational infrastructure of the repository is based on stability, quality, and continuity. As mentioned in R1 (mission) and R3 (continuity). A wider description of these aspects is included in the digital preservation policy (see attachment).

Reviewer Entry

Reviewer 1

Comments:

Reviewer 2

Comments:
Accept

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:

As mentioned in R5, RAA has multiple advisors concerning the repository. They all have their own specific field of expertise. Together they orchestrate the functional processes concerning the repository. Technical advice is provided by an independent external Technical Repository Advisor. Once every two months the Director of RAA arranges a multidisciplinary meeting about the repository in which all these employees discuss new developments about all aspects of the repository to ensure its continued relevance and to improve the repository. Additional technical IT advice is being obtained by engineers from the managed hosting provider Picturae Holding B.V.

Besides our own repository advisers, the archival sector has many national and international communities where advice can be found. These communities meet to draw up standards and provide advice about all kinds of archival and repository subjects. As mentioned in point R5, employees of RAA participate in many of these expertise groups in order to share and obtain knowledge. These communities communicate through various methods like online forums, e-mail, (video)calls, and physical meetings. Specific to our Archivematica (https://bit.ly/2FKLX0h) solution, RAA joins up with other Dutch regional repositories, for continuous product improvement.This is being done trough meetings and knowledge-sharing sessions which are mostly informal. Further explanation on these collaborations can be found at R10.

If a case from RAA deems other external advice necessary, advisers from the community may be consulted to find a definitive solution and vice versa. RAA always provides their learning lessons as feedback to the community so they can grow.

Reviewer Entry

Reviewer 1

Comments:

Reviewer 2

Comments:
Accept

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

Reviewer 2

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

Response:

Concerning data integrity, RAA requires that the files are to be ingested, are accompanied by metadata in compliance with the Toepassingsprofiel Metadatering Lokale Overheden (TMLO: https://bit.ly/3hzli7b).This metadata profile applies to all the ingested files in the repository. RAA uses this standard to ensure authenticity within the repository and to provide context and searchability. Therefore, all types of depositors (municipalities or private) need to comply with this standard.

Another important standard that is being used is the Open Archival Information System (OAIS) model, part of ISO 14721 (https://bit.ly/2WIa5FF). The repository from RAA is completely based on this model. The model and a reference to the repository of RAA can be found in the digital preservation policy (chapter Standaarden, https://archiefalkmaar.atlassian.net/wiki/spaces/WRAA/pages/1245185/Standaarden).

The Dutch metadata standard TMLO contains, among other things, elements of the identity of the depositor and the filenames of the deposit which are added to the Submission Information Package (SIP, notice the OAIS overview). The repository of RAA has multiple sections for each municipality. By adding the value of the identity of the depositor, RAA can ensure that the files from municipality X, are stored in the repository section of municipality X and not in the repository section of municipality Y. Furthermore, a checksum is another compulsory metadata element (TMLO 21.7: Physical Integrity). As mentioned in the digital preservation policy (chapter Authenticiteit, https://archiefalkmaar.atlassian.net/wiki/spaces/WRAA/pages/983041/Authenticiteit), RAA requires a checksum (SHA256) as part of a SIP. During an ingest in the repository, the checksum is generated again and the repository checks if the generated checksum matches the unique checksum in the SIP. This ensures the integrity and authenticity of the data.

The completeness of the supplied data and metadata is checked during the ingest procedure. This is done by microservices (https://bit.ly/3hgoqT1) that are part of the application Archivematica. Microservices are running jobs configured in the application (for example, starting an antivirus scan on the files to ingest). These jobs check the validity and completeness of metadata based on a diagram called ToPX-2.3_1.xsd (https://bit.ly/34GB2xW). Besides that, the data is checked on packaged contents, doublures, viruses, identification of the file format, etc. After ingesting, the files are entered into the storage environment as an Archival Information Package (AIP, notice the OAIS overview). Corruption of data objects is prevented by permanent checksum checks at block-level. Every executed command triggers the creation of a checksum which proves the integrity of the files. The entire ingest procedure and all changes in data, version management, and metadata in storage are logged in the Metadata Encoding and Transmission Standard (METS) file (https://bit.ly/37Lyy3a). This METS file is stored in Archivematica, combined with the deposit files in the AIP. All changes to the AIP are logged in this METS file.

Besides the checks above, RAA follows the preservation planning of each file as mentioned by PRONOM (https://bit.ly/30IIDt2) from the U.K. National Archives. To fulfill this preservation strategy, the rules from PRONOM are implemented in the format policy registry in Archivematica. As mentioned in R0, the repository checks file types that are being ingested to see if they comply with the format policy register. So far, all ingested files complied with the preservation planning, but it is highly possible that deposit files will have file extensions in the future that are no longer sustainable, meaning that preservation actions need to be taken to ensure continuous access to the files. If that is the case, RAA needs to make sure that a sustainable file format is created from those original files. The repository will therefore create an extra copy of the original file during the ingest procedure, with a new sustainable file format, and stores this file in the AIP, together with the original file and original metadata. To execute the same preservation policy to already ingested files, Archivematica has the possibility to create new files in the AIP and records these changes in the METS file that is part of that AIP.

As mentioned in R0 and in the digital preservation policy (hoofdstuk Authenticiteit, https://archiefalkmaar.atlassian.net/wiki/spaces/WRAA/pages/983041/Authenticiteit), RAA never makes any changes to the original file (or its extension) to prevent data loss. Thanks to this preservation strategy, the original and preserved file are both stored in the repository. This functionality is part of our repository and is frequently tested (for example, during every new release). This process results in multiple stored files referring to the same metadata, but only one file is the original deposit file. To guard the authenticity, original deposit files will always keep their original file extension. With this policy, RAA prevents those certain functionalities from the original files are lost over time. For example, changing an Excel file to a PDF file has as a consequence that all macros (https://bit.ly/3iHXBKf) will be lost and thereby the functionality of the file is lost too.

RAA is able to maintain this strategy because a copy of each file is sent to an external Digital Asset Management System (DAM) where changes can be made without touching the deposit files in the AIP. The repository sends all the data in a Designation Information Package (DIP, notice the OAIS overview) to this system. This means that any extra files which are added due to the preservation policy, all files will be part of this DIP. The DAM is used as an access database for the website to publish the records. Most of the data producers at RAA are governmental institutions. RAA uses the preservation planning strategy as a unique selling point for these organizations. RAA makes data producers aware of this strategy during the first introduction to the repository and will continue to provide them with updates on changes in the strategy. Data producers, therefore, provide closed files (without any source of encryption or passwords) that contain final versions of the documents.

Due to the OAIS basis of Archivematica provenance information is saved within the AIP (https://bit.ly/2WFzZK8). 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. This information refers to the storage, handling, and migration of the repository files. This information is centrally being logged and can be viewed for audit purposes.

Reviewer Entry

Reviewer 1

Comments:

Reviewer 2

Comments:
Accept

8. Appraisal

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

The Public Records Act is the most important reference for the selection of data eligible for archiving. Governmental institutions are obliged by this law to preserve archives which are 20 years or older, by transferring them to an appropriately designated repository. Once the files are transferred to RAA they are, based on the Public Records Act, meant to be made public and to remain public. Therefore, stored files in the repository are never deleted. The obligation to deposit archives according to the Public Records Act does not apply to private archives. Files from private archives can be donated or brought into custody at will, after which the RAA will take proper care of them. The RAA is obligated to ensure that donated private archives and archives in custody are in good, structured and accessible state according to the Public Records Act.

To determine the correct metadata RAA commits to the Toepassingsprofiel Metadatering Lokale Overheden (TMLO) structure. The RAA works with the producers to ensure all metadata is correctly collected before ingesting the SIP. RAA uses the TopX creator tool to ensure this. This tool contains all the necessary metadata procedures, checks if the metadata is delivered in the right way, and creates a TopX file. The TopX file puts the metadata of the files and records and the relationship between them in a defined structure. RAA requires that all provided metadata meet the requirements of TMLO.

Besides the above standards, RAA commits to a list of default preferred file formats to maintain sustainability based on PRONOM. As mentioned in the digital preservation policy (chapter Digitaal Object, https://archiefalkmaar.atlassian.net/wiki/spaces/WRAA/pages/1015853/Digitaal+object), RAA commits to the preferred file formats list of the Dutch National Archive (https://bit.ly/2ONQIHd), which is a published subset list of file formats that are accepted according to the PRONOM registry. When governmental institutions create a SIP with the TopX creator tool, the integrity of the metadata and the file formats are checked and are therefore ensured. During an ingest, the repository checks the file formats again. This ensures (next to the checksum check mentioned in R7) that the SIP has not been modified during the delivery process and is correctly being imported into the repository. It is also important to state that the preferred file formats list is not a fixed set. The RAA always keeps in mind that it is most important that the authenticity, as well as the usefulness of a digital object is assured. This means that in some cases different file formats will be accepted if this is necessary for one of the designated communities.

RAA communicates the required file formats beforehand with the governmental institutions. The files are rejected by the repository if the supplied files do not comply with the preferred file format list. This happens through microservices that check the file format of each ingested file. RAA notifies the governmental institutions when this occurs so they can convert the files to a sustainable file format or the decision will be made to accept the current one.

Before the files are transferred to RAA, the responsibility for these files lies with the governmental institutions. This responsibility consists of making sure the files are in good condition and accessible, as is stated in the Public Records Act. After the files are transferred to RAA, the responsibility for the condition of and access to the files, transfers to RAA. However, because the governmental institutions are still own the data, they stay responsible for the contents of the files. In a worst-case scenario where the governmental institutions do not longer exist, RAA will take responsibility for maintaining the mentioned data.

Reviewer Entry

Reviewer 1

Comments:

Reviewer 2

Comments:
Accept

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

Reviewer 2

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

Response:

Processes and procedures are documented in the Strategy note 2019-2022, GDPR Data Processing Agreements, and the Service Level Agreement with Picturae.

As described in the digital preservation policy of RAA (chapter Bitpreservering, https://archiefalkmaar.atlassian.net/wiki/spaces/WRAA/pages/655368/Bitpreservering), RAA anticipates data loss by duplicating our application data to a different data center and yearly test the failover-recovery procedure. The repository of RAA is therefore hosted and managed by Picturae Holding B.V. Eight times a day (every three hours) a snapshot is created from all the applications to ensure RAA can react quickly if an issue occurs. These snapshots give us the possibility to go back to the state of an application earlier that day. A complete data back-up is made on a daily basis and copied to the passive datacenter for redundancy. The progress is monitored by Picturae Holding B.V. systems and employees.

In addition, Picturae Holding B.V. has fixity checks at block-level in place for all its hosting and storage environments, including the Archivematica environments. This means that all files get a fixity check each time they are consulted. For the files that are not consulted regularly, the system runs a fixity check every month to guarantee the integrity of those files. This is one of the measures taken to ensure that the back-ups are correct.

The repository runs on multiple virtual servers. Because the servers are virtual, they can easily move from one storage location to another. This means they do not lean on one physical hard disk. The harddisks can be removed and replaced (hot-swappable) if necessary to prevent data loss. Picturae Holding B.V. constantly monitors the current state of the physical hard drives and acts accurately on replacing them in time to prevent bit-rot. Throughout the process (from ingest to publication), all data and metadata are processed and hosted by Picturae holding B.V.

Reviewer Entry

Reviewer 1

Comments:

Reviewer 2

Comments:
Accept

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:

RAA has described their view on digital preservation in the digital preservation policy. This document describes the policy about authenticity, preservation, digital objects, metadata, rights, norms, access, organization, and certification. The preservation plan is part of the entirety of measures to facilitate the long-term accessibility of the RAA repository. The plan is available via our Confluence site:
https://archiefalkmaar.atlassian.net/wiki/spaces/WRAA/pages/655361/Preserveringsheidsbeleid+E-depot.

The plan shows the preservation actions that RAA executes and how RAA documents those actions in their context, motives, criteria, and tools. The document can be consulted via Preserveringsheidsbeleid E-depot added in the attachment and is available as an English summary here: https://archiefalkmaar.atlassian.net/wiki/spaces/WRAA/pages/29458433/Digital+Preservation+Policy+RAA+English+summary.

To show the level of responsibility and commitment of RAA to digital preservation RAA has obliged itself to the Scalable Preservation Environments (SCAPE) framework (https://bit.ly/3qFlzGQ). This framework has been developed with an overview by the Open Preservation Foundation (OPF) and is a European standard for preservation policy. The digital preservation policy of RAA is based on this framework.

In December 2020, RAA has signed the Dutch Manifest Digital Heritage Network. Being part of the Digital Heritage Network (https://netwerkdigitaalerfgoed.nl/) means that RAA works according to certain principles and has made a shift from “institutional thinking” to “network thinking”. A growing number of organizations from the heritage sector support this approach. Network thinking is crucial in the way RAA engages with the designated community and the market.

To engage with the designated communities, RAA hosts and joins multiple knowledge-sharing sessions about market changes. These meetings often arise from the input RAA receives from users of the repository through the website, from the municipalities through information exchange, or RAA receives information from the designated community by sending out customer satisfaction surveys. For example, the municipalities will let us know that there is a need for the recording of video files in the repository. RAA then investigates the possibilities to meet these needs and, if it is deemed necessary, RAA will start to work on a possible solution for it. To investigate needs and possibilities further, RAA hosts a yearly meeting for all institutions that use the same Archivematica repository system from the supplier Picturae Holding B.V. In these meetings new developments are discussed and is decided if further actions are needed.

Besides that, the staff of RAA attends multiple meetings about all kinds of subjects related to digital preservation, for example about metadata. RAA does this to create national working methods related to metadata. RAA does this for the new national metadata standard; Metagegevens voor Duurzaam Toegankelijke Overheidsinformatie (MDTO: https://bit.ly/3vRMcur), which is the successor of the current standard Toepassingsprofiel Metadatering Lokale Overheden (TMLO). RAA monitors these developments closely so upcoming changes can be implemented on time. To prevent obsolescence of data the repository converts files in bulk. With this ability, RAA can convert the files in time to a more common file format. To anticipate which files need to be changed, the staff of RAA monitors the national and international communities closely. To manage format risks, and other risks such as governance of the authenticity of the files, RAA has a test environment of the repository with representative data. If a certain file needs to be changed to a new file format, or metadata needs to be improved or enriched with additional metadata, this is first tested in the test environment before any changes are made in the production environment. This process applies to all changes RAA makes to the repository and stored data (including updates from the system, services, or changes in metadata). RAA does this to ensure that all changes being made to the repository or (meta)data stored in the repository have no negative effect on other parts of the repository. Thanks to these procedures RAA can ensure a clean and well-functioning repository system.

RAA has e-depot contracts with all governmental institutions that are using the services for digital preservation. After a transfer of digital records, RAA is responsible for maintaining and publishing the files, but the content of the files stays a responsibility of the governmental institutions. By signing this document, the governmental institutions grant us permission to copy, transform, and store the items to make preservation and publication of the files possible.

The actions RAA takes to copy, transform and store files are based on their preservation policy. To make sure these policies are taken in place, RAA takes technical and organizational measures. These are technical measures like fixity checks. If proven necessary storage of multiple file-formats is being performed. Organizational measures are executed by specialized staff. The repository management monthly reviews the complete operating of the repository to ensure these policies are applied. RAA makes risk assessments (impact analyses) and implements proper countermeasures to minimize possible risks. For example, as mentioned in R9, and further mentioned in R16, back-ups are done of a daily basis and tested every year as a countermeasure to the risk of possible data loss. Besides the back-up, the security of the repository is being checked as well by a yearly penetration test which is done by an independent supplier.

The goal of the penetration test is to minimize the vulnerability of cybersecurity threats a digital repository is being exposed to. This will be further explained in R16.

Reviewer Entry

Reviewer 1

Comments:

Reviewer 2

Comments:
Accept

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:

Quality requirements on the repository are described in the Public Records Act and related regulations. Art.3 of the Public Records Act stipulates that governmental institutions are obliged to ensure that the files entrusted to them are and remain in a good, orderly, and accessible condition, which is in line with the strategy of RAA.

Archive regulation (Archiefregeling: https://bit.ly/3aET1sg) art.17 stipulates that the following aspects of every stored file in the repository can be accessed at any time:

- the content, structure, and form when ingested or created by the government organ, in as far as these aspects had to be knowable for the execution of
- the work process in question,when, by whom, and based on what task or work process it was ingested or created by the government organ;
- the connection with other archive documents ingested and created by the government organ;
- the management activities executed in relation to the archive documents;
- the software or application software with which the archive documents are stored or managed.

Clause 2 of Art. 19 of the archive regulation stipulates the governmental institutions to add metadata to the files to meet with the given aspects mentioned in art. 17. These together create the SIP which the governmental institutions deliver to RAA to ingest in the repository. Articles 21 to 26 specifically discuss special regulations for digital archive documents to be stored. RAA only ingests archives to be stored permanently (as mentioned in R8). Therefore, the quality of the data and metadata depends on the degree to which governmental institutions comply with the requirements in the Public Records

Act and the archive regulation.

Checking the integrity of the data is secured in an automatic process. The completeness and authenticity (see also R7) are checked during the transfer and ingest process in Archivematica. To ensure the quality of the metadata, it needs to be compliant with the standards given in Toepassingsprofiel Metadatering Lokale Overheden (TMLO). The municipal archivist will evaluate the data. If it is apparent that the governmental institution fails to meet the quality requirements in the Public Records Act and archive regulations, the ingest is rejected and the governmental institution must first ensure compliance before ingesting can be considered again.

Reviewer Entry

Reviewer 1

Comments:

Reviewer 2

Comments:
Accept

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
Accept

Reviewer 2

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

Response:

The digital preservation policy of RAA contains all the workflow subjects regarding the repository. The business processes related to the workflows in the repository are completely based on the OAIS model and, naturally, the requirements of the Public Records Act apply. The document includes descriptions of functions, responsibilities, and specific business processes regarding the delivery of the files and the ingest process. These processes can only be run by authorized personnel. Various references to documentation and descriptions of processes are already included in the answers to different questions.

As mentioned in the digital preservation policy, RAA ensures that the digital archives are ingested (chapter Bitpreservering, https://archiefalkmaar.atlassian.net/wiki/spaces/WRAA/pages/655368/Bitpreservering), managed, and made accessible and available (chapter Toegang, https://archiefalkmaar.atlassian.net/wiki/spaces/WRAA/pages/1409025/Toegang). For ingest in the repository, the depositor delivers the files and metadata to RAA by a hard disk or by a digital (cloud) storage platform. Before the files are ingested, they are transferred to the repository from these storage locations. At this location, the delivered files are being analyzed and checked for compliance to the following demands:

- Metadata: The metadata describing the digital objects have to be compliant to the TMLO (https://www.nationaalarchief.nl/archiveren/kennisbank/tmlo) of MDTO (https://www.nationaalarchief.nl/archiveren/mdto) metadata schemas.
- File formats: Not every file format is accepted by the repository. The RAA aims to be compliant to the Handreiking Voorkeursformaten, created by the Nationaal Archief (https://www.nationaalarchief.nl/archiveren/kennisbank/handreiking-voorkeursformaten-nationaal-archief). If a file format is not compliant, furter measures might be taken to normalize or tolerate a file format (for instance when it is not possible to convert a format into a desired format).
- Structure: De delivered objects have to be structured in a hierarchical way. The standard which is used for this is also created by the National Archive and is called TopX. TopX uses five aggregation levels: Archive, Serie, Dossier, Record and object. (more info: https://www.nationaalarchief.nl/archiveren/kennisbank/metagegevens-en-het-e-depot).
- Publicity: Are all aggregation levels restricted in publicity if these contain information that cannot be made public according to the GDPR or Dutch Public Records Act (Archiefwet 1995, artikel 15: https://wetten.overheid.nl/jci1.3:c:BWBR0007376&hoofdstuk=II&artikel=15&z=2022-05-01&g=2022-05-01).

The E-depot team makes sure that these elements are being analyzed before ingesting.

If the deliverd digital archives are compliant to the above stated standards they are ingested to the digital repository. During the ingest, compliancy to these is again checked by the software.

After succesfully ingesting, the files are copied to a Digital Asset Management (DAM) system from which they can be accessed and managed by our Collection Management System; Memorix Archives (https://bit.ly/3wSLKNR) and made publicly available through our website www.regionaalarchiefalkmaar.nl. This process is first completed in the test environment of the repository.

Whenever a step in this process is done, the governmental institution will receive an update about the result. If a specific part of the workflow is worth mentioning, even if it is not a breaking point, they will get notified about the progress. RAA reminds the governmental institutions about new publications that are scheduled. When the files are published, RAA communicates this internally through the intranet and externally through the website www.regionaalarchiefalkmaar.nl.

Our repository hosting supplier Picturae Holding B.V. is ISO-27001:2017 certified. This means that all their workflows and business processes are based on those standards. Part of this certification is Role Based Access Control (RBAC). RBAC authorizes employees of RAA based on their function group. This means that only personnel with the right responsibilities are authorized to execute the necessary processes to achieve the goal of archiving the files. Proof of certification is added to the CTS application as an attachment.

During the transfer and ingest process multiple qualitative and quantitative checks are executed. In the digital preservation policy of RAA is described how these integrity checks are monitored. One of these integrity checks contains object identification, which validates the file formats. This means that the format needs to comply with the accepted formats that RAA requires for ingesting in the repository to ensure long-term preservation. If a file does not comply with the accepted format, the process is stopped, and the transfer of the files is declined.

The repository has as many as possible automatic decision handling processes built-in, and some others are being performed manually. An example of a manual decision is the choice of the AIP storage location for certain ingest. In case RAA notices that a workflow could be improved a request is made and reviewed by the repository management. If the request is granted, the change will be implemented in the workflow description. Any technical change that follows from this decision is implemented by the hosting provider Picturae Holding B.V.

Reviewer Entry

Reviewer 1

Comments:

Reviewer 2

Comments:
Accept

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:

3 – The repository is in the implementation phase

Reviewer Entry

Reviewer 1

Comments:

3 – The repository is in the implementation phase
Accept.

For level 4 persistent identifiers should be available for all archived digital objects.

Reviewer 2

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

Response:

In the application Archivematica, it is possible to search directly in the Archival Information Packages (AIP's) for metadata. The FullText Open Source Search Engine Elastic Search (https://bit.ly/3nIr06O) is used to search through the data. In compliance with the OAIS model, a DIP is created from the AIP in order to make the digital archive available. The DIP can be accessed through through the Collection Management System; Memorix Archives (https://bit.ly/3hilINa) and published on the website www.regionaalarchiefalkmaar.nl. The portal to search through files on our website can be found via Archieven (regionaalarchiefalkmaar.nl).

The Collection Management System; Memorix Archives uses several international archival standards, such as:
- ISAD(G): General International Standard Archival Description (https://bit.ly/3jbx5t4);
- ISAAR (CPF): International Standard Archival Authority Record for Corporate Bodies, Persons and Families (https://bit.ly/3gSmZM1);
- ISDIAH: International Standard for Describing Institutions with Archival Holdings (https://bit.ly/3gPjEgK).

Thanks to these standards, the ingested metadata conforming Toepassingsprofiel Metadatering Lokale Overheden (TMLO) becomes functional in Memorix Archives. TMLO contributes to the standardization of metadata and ensures that enough metadata is stored in the system with the files. The archival standards from Memorix Archives ensure that all this metadata is applicable, meaning that Memorix Archives is able to work with the metadata, and users can search through, or find the files.

The use of persistent identifiers (PID: https://bit.ly/3h7lcSu) is possible but currently not implemented in the repository. RAA intends to implement this PID functionality in the future and in the meantime, RAA uses Universally Unique Identifiers (UUID's: https://bit.ly/31v8gxl). UUID's can be used for reliably identifying persistent objects across a network. In Archivematica UUID's are added to the Archival Information Package (AIP) and are unique for every AIP (https://bit.ly/2SSIZ0l).

The repository provides options for automated harvesting of metadata via linguistic analyzers based on OAI-PMH (https://bit.ly/3wnr9Qz). These are analyzers for text processing. RAA does this for example by connecting to the Archives Portal Europe (https://bit.ly/35PE3w4) network from Europeana (https://bit.ly/3gSFNuJ). This connection is created by an Application Programming Interface (API: https://bit.ly/3vQxJ1F) between our own Collection Management System; Memorix Archives and the systems of Archives Portal Europe. This connection enables Archives Portal Europe to harvest our data and makes our files available to a wider audience in the world. The portal to search for files from RAA in Archives

Portal Europe can be found via Archievenoverzicht (NL-AmrRAA - HG_149863523) (archivesportaleurope.net).

Reviewer Entry

Reviewer 1

Comments:

Reviewer 2

Comments:
Accept

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:

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:

Various stipulations relating to metadata are already described in R11. The supplied metadata must meet the Toepassingsprofiel Metadatering Lokale Overheden (TMLO) standard. This metadata is stored in the repository and collection management system. When a digital archive is accessed, users can search through the database based on the metadata elements from TMLO. TMLO provides mandatory requirements for metadata for the long-term preservation of records, including requirements for contextual, technical, and data management metadata. These requirements are in place to ensure that all users and designated communities will get access to unchanged, authentic, and understandable information.

Of course, changes in the (digital) world can affect the standard and therefore the standard is constantly reviewed, with input from lots of archives in the Netherlands, by the Dutch national archive; 'Nationaal Archief' (https://bit.ly/3jpw9kY) to check if it still fits the needs of the users and the designated community as best as possible. Thanks to those reviews, a new version of this standard is being developed named; Metagegevens Duurzaam Toegankelijke Overheidsinformatie (MDTO: https://bit.ly/3ote7ia).

To ensure continued understandability of the data changes in file formats, RAA continuously monitors the common file formats from the PRONOM database from the U.K National Archives (https://bit.ly/38r6Do8). If a new commonly used file type replaces an older file type, RAA creates a copy of the original file with the older file type and creates a new file with the new 'common' file type in the AIP. This means that the originally ingested files from the SIP remain unaffected, and a completely new file will be generated, in a different file format. As already mentioned in R7, original files will never be changed or deleted in our repository. Original files will always have the same file extension as they had during the ingest to ensure the authenticity of the original deposit file.

To give the public access to the files, the rendering of many common file formats is possible through the repository's extensible render facilities. Alternatively, files can be made available as downloadable copies. Files are also - in a viewable file format - stored in a different storage system (e.g. a JPEG version of a specific page from a PDF file).

Feedback from our designated communities helps to decide which file formats to prioritize for adding to the viewable file formats, and which files can be made available as a downloadable copy. For continued understandability of metadata, every AIP in Archivematica contains a README.html file that describes the content of the AIP.

Our archives are open to the public and a lot of files are legally available for re-use. However, there are exceptions if files are copyrighted. As mentioned in R2, if the files are copyrighted a request must be addressed to the executive council of the responsible governmental institution. They determine whether the data can be viewed or not. If the request is granted, the files will be handed over to the requestor with a disclaimer; for personal use only, do not distribute. Sometimes reuse or publication of the files can possibly have an impact on the security or privacy of those involved. If that is the case then those files are not published, not available for the public, and not available for re-use.

Reviewer Entry

Reviewer 1

Comments:

Reviewer 2

Comments:
Accept

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 infrastructure of the repository from RAA is being hosted and maintained by Picturae Holding B.V. Their infrastructure is physically situated in the data center Global Switch in Amsterdam and in their own data center in Heerhugowaard, as mentioned in R5 and R9. These two data centers have multiple ISO certifications: ISO 9001, ISO 14001, OHSAS 18001, and ISO 27001. Picturae Holding B.V. is constantly developing the infrastructure.

Upon this infrastructure run various virtual servers are needed to host the Open Source Archivematica repository. The infrastructure and servers are scalable without causing downtime of the provided services. Archivematica itself is completely based on another international ISO standard: ISO 14721. This standard includes the OAIS model. All ISO certification of the ISO family needs to be reviewed every 5 years to ensure their relevance.

Picturae Holding B.V. has started a partnership with Artefactual Systems Inc. (https://bit.ly/3r8SKDQ), the lead developer of Archivematica to make sure that their strategy is aligned with theirs and the infrastructure is ready for future developments of the repository. Thanks to the Open Source vision of Artefactual and its continuous development of the software, Archivematica is a highly appreciated application within the community.

Picturae Holding B.V. is responsible for maintaining system software, documentation, sustainable bandwidth, sufficient connectivity, and availability of the services as mentioned in the Service Level Agreement (SLA). In this document rules are applied for back-up and recovery procedures, to maintain the continuity of the online services RAA provides. Within the Service Level Agreement, an exit strategy is in place, which obliges Picturae Holding B.V. to support us till two months after the ending of the contract. The Service Level Agreement can be consulted via https://bit.ly/2WGo7aC.

Reviewer Entry

Reviewer 1

Comments:

Reviewer 2

Comments:
Accept

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:

Technical infrastructure

Picturae Holding B.V. is responsible for the technical infrastructure and security of the repository. Picturae Holding B.V. has an ISO 27001 certification, and takes various measures to be compliant, including:

Logical access control;

Screen locks;

Physical measures for access security;

Securing network connection using TLS technology;

Purpose-specific access to personal data;

Checking assigned authorizations.

Checksum and data scrubbing
Critical components of the infrastructure are installed with checksumming and data scrubbing (https://bit.ly/3rmJyvP). The correctness of the data is checked and repaired, if necessary, with every read command. The technical infrastructure is monitored to detect disruptions early. The correctness of data is checked monthly. If a checksum is incorrect, personnel of Picturae Holding B.V. is warned automatically. If a discrepancy is detected by the system, personnel of Picturae Holding B.V. will act and solve the issue.

Replacement of system
When a storage system is replaced, all data is checked with the aid of checksums.

Back-up and retention policy
Back-ups are conducted by Picturae (twice a day) and checked daily for integrity. Back-ups are saved for 62 days. Possible data loss will be recovered from images from the back-ups.

Redundancy
As stated in R5 all data storage is mirrored, and GlobalSwitch Amsterdam is the primary site and a identical copy is being stored in Heerhugowaard.

Pen test
To ensure that the security of the application is top-level, and to ensure already implemented measures are in place and working correctly, RAA yearly conducts a PEN test.

I-awareness
To ensure a safe and sound access to and use of the repository, the RAA trains its employees periodically in I-awareness.

Reviewer Entry

Reviewer 1

Comments:

Reviewer 2

Comments:
Accept

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:

I've had some problems adding multiple attachments. i've solved this by adding a .zip file containing everything. Most documents are already available as public documents via Confluence, so not a large issue.

Reviewer Entry

Reviewer 1

Comments:
Board comment: For R13 - The CoreTrustSeal Board encourages the use of PIDs for the renewal of certification in 3 years.

Reviewer 2

Comments:
Accept