Predstavitev posodobljenih smernic CoreTrustSeal za repozitorije in podpora morebitnim prijaviteljem

11. november 2025, online

Maja Dolinar, Arhiv družboslovnih podatkov in Slovensko vozlišče RDA

Urnik delavnice

- Uvod v CoreTrustSeal
- Pregled zahtev R0 - R09
- Odmor
- Skupinsko delo
- Pregled zahtev R10 - R16
- Vloga RDA pri oblikovanju CoreTrustSeal
- Razprava

Biti zaupanja vreden

- Zaupanje, verodostojnost in zanesljivost so vrednote odprte znanosti
- Infrastrukture in repozitoriji so ključni viri podatkov
- Zaslužiti si morajo zaupanje:
  - Svojih uporabnikov
    - Dajalcev, ki podatke ustvarjajo in predajajo digitalne vire
    - Uporabnikov podatkov
  - Svojih organov in financerjev

Utemeljitev za formalno certificiranje

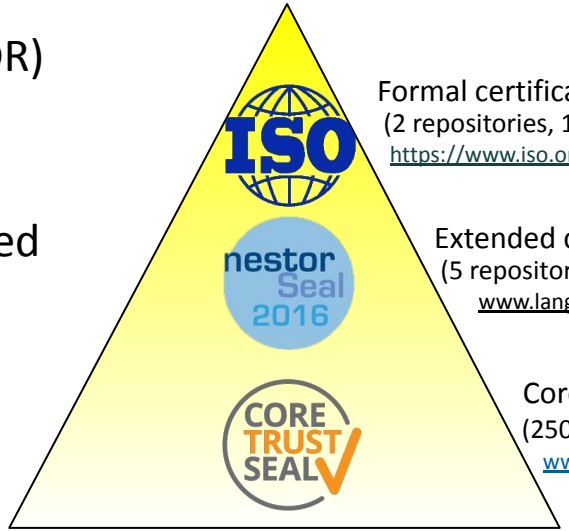
- Poslanstvo zagotavljati zanesljiv, dolgoročen dostop do upravljanih digitalnih virov za svojo ciljno skupnost
- Neprekinjen nadzor, načrtovanje in vzdrževanje
- Zavedanje groženj in tveganj znotraj sistemov
- Redni revizijski in/ali cikli certificiranja

Utemeljitev za formalno certificiranje

- Kriteriji, ki jih oblikujejo pristojni strokovnjaki in so uporabni ne glede na disciplinarni kontekst.
- Predhodna samoocena na podlagi kriterijev, ki omogoča preverjanje organizacije in procesov ter prepoznavanje možnih izboljšav.
- Zunanja presoja s strani pristojnih strokovnjakov.
- Oddaja podatkov v certificiran podatkovni center je pomemben element načrtov ravnanja z raziskovalnimi podatki (DMP-jev).

CoreTrustSeal

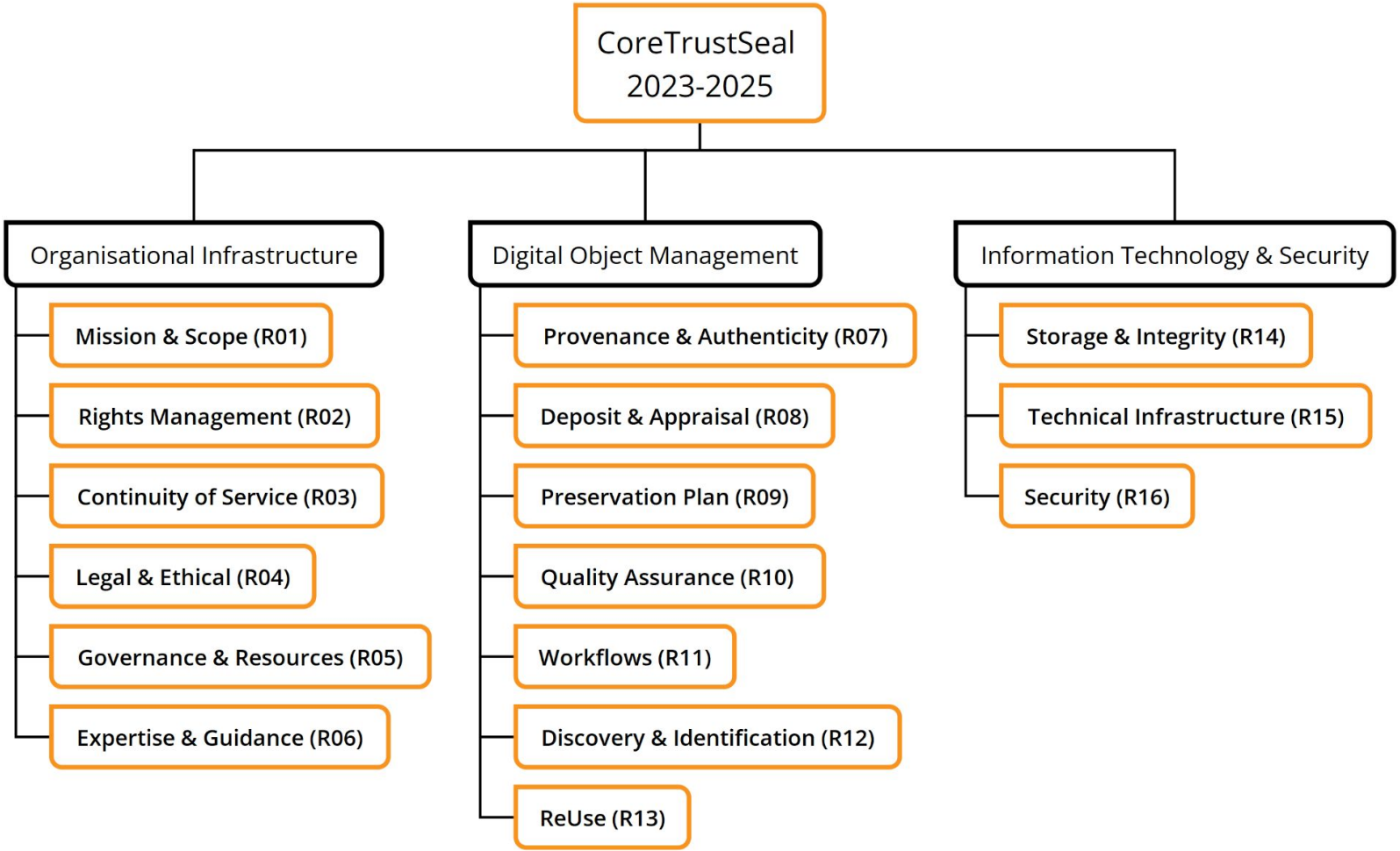
- Trustworthy Digital Repository (TDR)
  - Requirements
  - Certification
- Not for profit and community-based
- Global and domain agnostic
- Low barrier to entry
- Three year certification
- Objectives
  - enable repositories to safeguard data
  - ensure high quality
  - guide reliable management of data for the future



Formal certification ISO 16363:2012
(2 repositories, 100+ requirements)
https://www.iso.org/standard/56510.html/

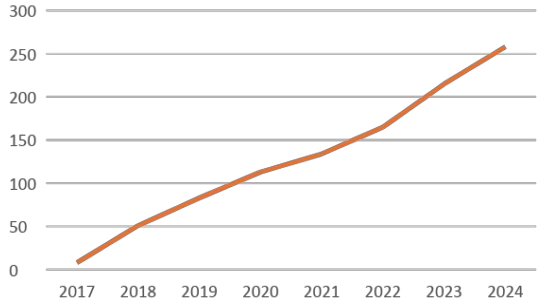
Extended certification DIN 31644
(5 repositories, 34 requirements)
www.langzeitarchivierung.de

CoreTrustSeal certification
(250+ repositories, 16 requirements)
www.CoreTrustSeal.org

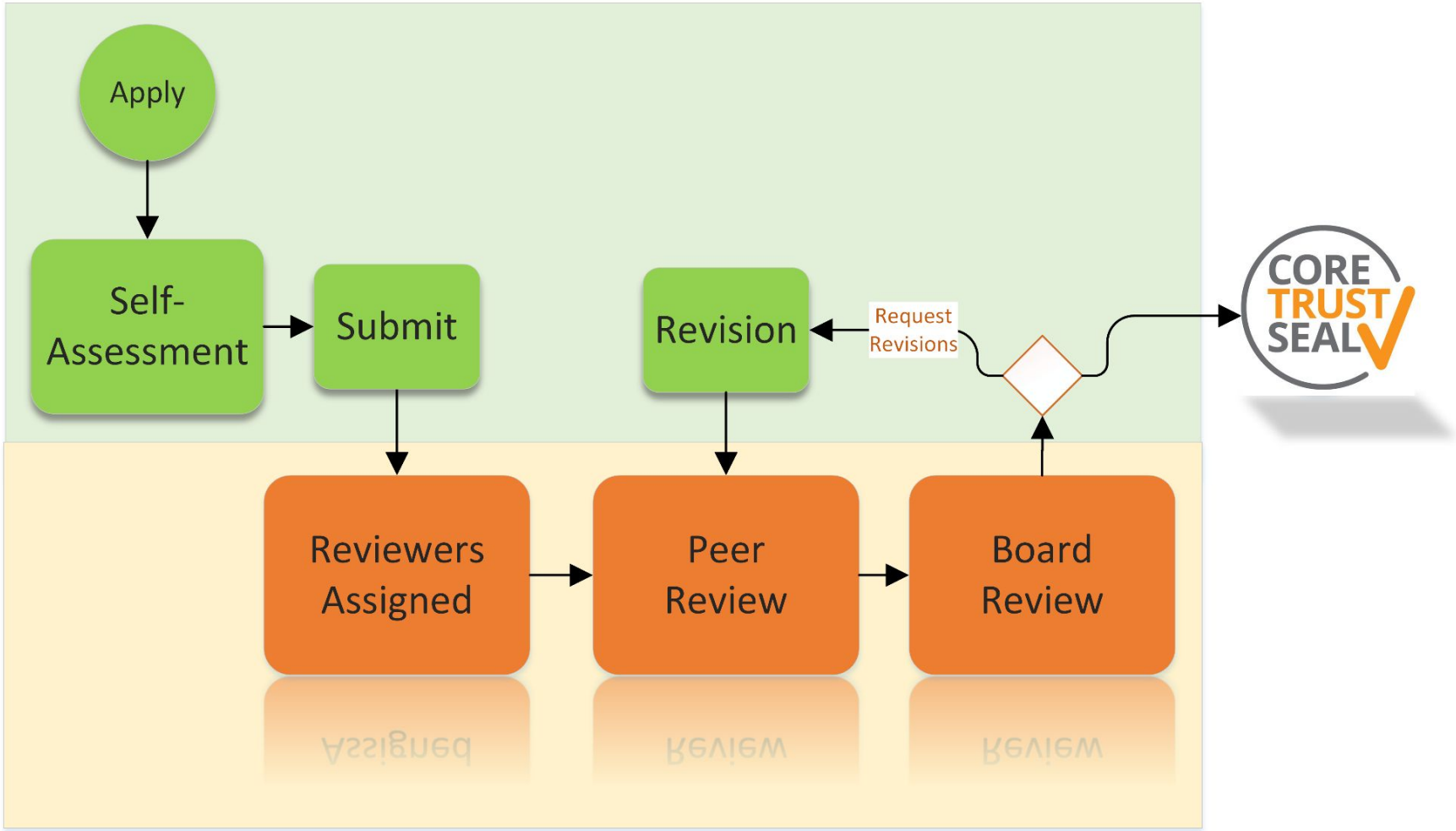

CoreTrustSeal
2023-2025
Organisational Infrastructure
Mission & Scope (R01)
Rights Management (R02)
Continuity of Service (R03)
Legal & Ethical (R04)
Governance & Resources (R05)
Expertise & Guidance (R06)
Digital Object Management
Provenance & Authenticity (R07)
Deposit & Appraisal (R08)
Preservation Plan (R09)
Quality Assurance (R10)
Workflows (R11)
Discovery & Identification (R12)
ReUse (R13)
Information Technology & Security
Storage & Integrity (R14)
Technical Infrastructure (R15)
Security (R16)

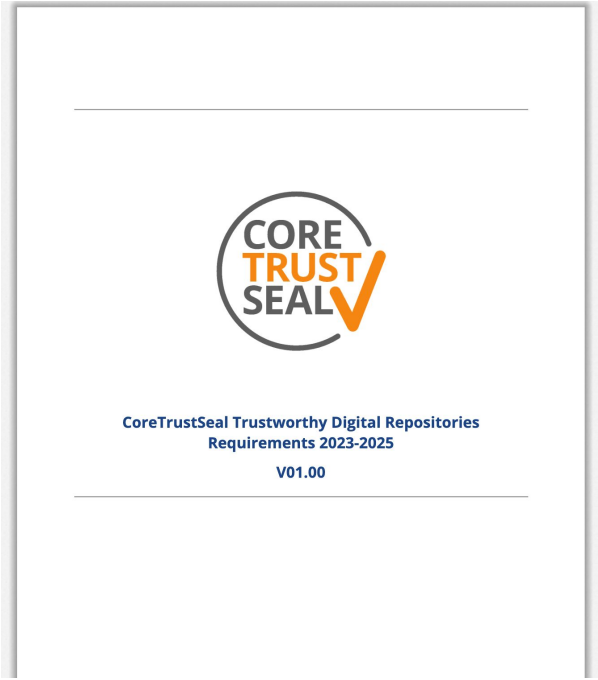
Benefits of certification

- Documentation of (data) management processes
  - A few weeks of teamwork in most cases (all included)
  - Sometimes a bit longer for others, but still worth it!
- Evaluation, reflection on the criteria – continuous improvement
  - Self-assessment
  - External evaluation



- Growing importance for funders of infrastructures and projects (DMPs)
- Political priority in Europe, with strong interest from key players (EOSC, etc.)


Apply
Self-Assessment
Submit
Revision
Request Revisions
CORE TRUST SEAL
Reviewers Assigned
Peer Review
Board Review
HLH-CoreTrustSeal-Process_01_00.vsdx



CoreTrustSeal Trustworthy Digital Repositories
Requirements 2023-2025
https://doi.org/10.5281/zenodo.7051012

CoreTrustSeal Trustworthy Digital Repositories
Requirements 2023-2025 - Extended Guidance
https://doi.org/10.5281/zenodo.7051096

CoreTrustSeal Trustworthy Data Repositories Requirements: Glossary 2023-2025

v01.00

This Glossary of Terms from other sources is provided to support the CoreTrustSeal Requirements and Extended Guidance.

The CoreTrustSeal texts use 'Digital Objects' to refer to 'data', 'metadata' and other materials managed together by repositories. These encompass the definitions provided for metadata, datasets and digital objects provided below.

OAIS uses the term Producer (included below for context alongside other definitions). The CoreTrustSeal texts use 'depositor' to refer to the actor that offers a digital object to a repository to be curated and preserved because that actor may not be the literal 'producer' of the data or metadata.

Definitions for Archive and Repository are provided below. The CoreTrustSeal texts use the term repository, but also follow OAIS (Open Archival Information System) assumptions about mandatory responsibilities. Some organisations that self-identify as archives or repositories may not meet those mandatory responsibilities, including active preservation of digital objects, and so may not be in scope to become CoreTrustSeal- certified.

(Taken from: * OAIS[1]; † the Society of American Archivists[2]; ‡ the CASRAI Dictionary[3]. (**) the DPC Handbook[4])

Appraisal[1]: The process of determining whether records and other materials have permanent (archival) value. Appraisal may be done at the collection, creator, series, file, or item level. Appraisal can take place prior to donation and prior to physical transfer, at or after accessioning.

Appraisal[]: Appraisal of born digital objects should include a measured assessment of their value to the parent organisation set against the challenges of long-term preservation and providing access. These challenges may include an organisation's ability to read or open a version of the master file, the ability to secure sufficient rights to manage and provide access to current and future versions of the file, or simply staffing and funding resources [...]. It should be remembered that organisations can provide access to resources that they have accessioned without placing them in specific preservation or retention workflows. A detailed policy document which clearly identifies the most important digital resources (from either a format or content perspective) can give guidance on appraisal of born digital objects destined

CoreTrustSeal Trustworthy Data Repositories
Requirements 2023-2025 - Glossary
https://doi.org/10.5281/zenodo.7051125

CoreTrustSeal Requirements Revision: Update & Next Steps

- The **last revision** introduced **significant structural and textual improvements** to enhance clarity and align with the evolving repository and data infrastructure landscape.
- The **upcoming changes** proposed by the Board are **minimal**, focusing on **stability** and preserving the **low-barrier, broadly applicable 'core'** standard.
- **Guiding Principles Going Forward:** The **broad scope**, **self-assessment structure**, and **evidence expectations** will remain as **stable** as possible.
  - Any updates will be **clearly communicated**.

Requirements revision 2026-2028

Review

- Review applications over last three years
- Draft suggested changes and additions

Consultation

- Survey the community
- Review and incorporate feedback into draft
- Board process the community feedback and creates new draft version

Publication

- Application Management Tool closed from 1 Nov - 1 January 2026
- Applications currently under review will remain under version 3
- Release of 2026-2028 requirements (1 January 2026)

Certificirani repozitoriji

- **263** certificiranih repozitorijev
- Trenutno ima **133** repozitorijev veljaven certifikat
  - **1 (2)** v Sloveniji
- Okoli **50** repozitorijev pridobi ali obnovi certifikat na letni ravni

Seznam repozitorijev s veljavnimi certifikati CTS:
https://amt.coretrustseal.org/certificates

CoreTrustSeal Trustworthy Digital Repositories Requirements 2023-2025
https://doi.org/10.5281/zenodo.7051012

However…

CoreTrustSeal is not for every repository

Being in scope for CoreTrustSeal means:

- You must provide **active** long term digital preservation
- **You** must be responsible for the preservation
- You must have a **designated community** that you can describe clearly

Start with a triage

Is the definition of the Designated Community clear enough?

Check R0 to ensure that the applicant understands the scope, knowledge base, and methodologies of the group(s) of users at whom the curation and preservation measures are primarily targeted.

Does the applicant offer active preservation?

Check Preservation Plan (R09) to ensure that active preservation is in place.

Check Deposit & Appraisal (R08) to confirm that digital objects receive active preservation.

Are the outcomes of the curation aligned with the needs of the Designated Community?

Check Reuse (R13) to confirm that appropriate information is available to support understanding and use of digital objects over time.

If it is not clear

- that the applicant offers active preservation, or
- what levels of curation are offered, or
- that the Designated Community is well served by the information in Reuse

=> the applicant is **either not in scope, or has provided insufficient information for a review**

=> application will be returned to the applicant with comments on the relevant items for revision.

Compliance level

The applicant must indicate a compliance level for each of the Requirements:

- In Progress: the repository is in the implementation phase.
- Implemented: the requirement has been fully implemented by the repository.

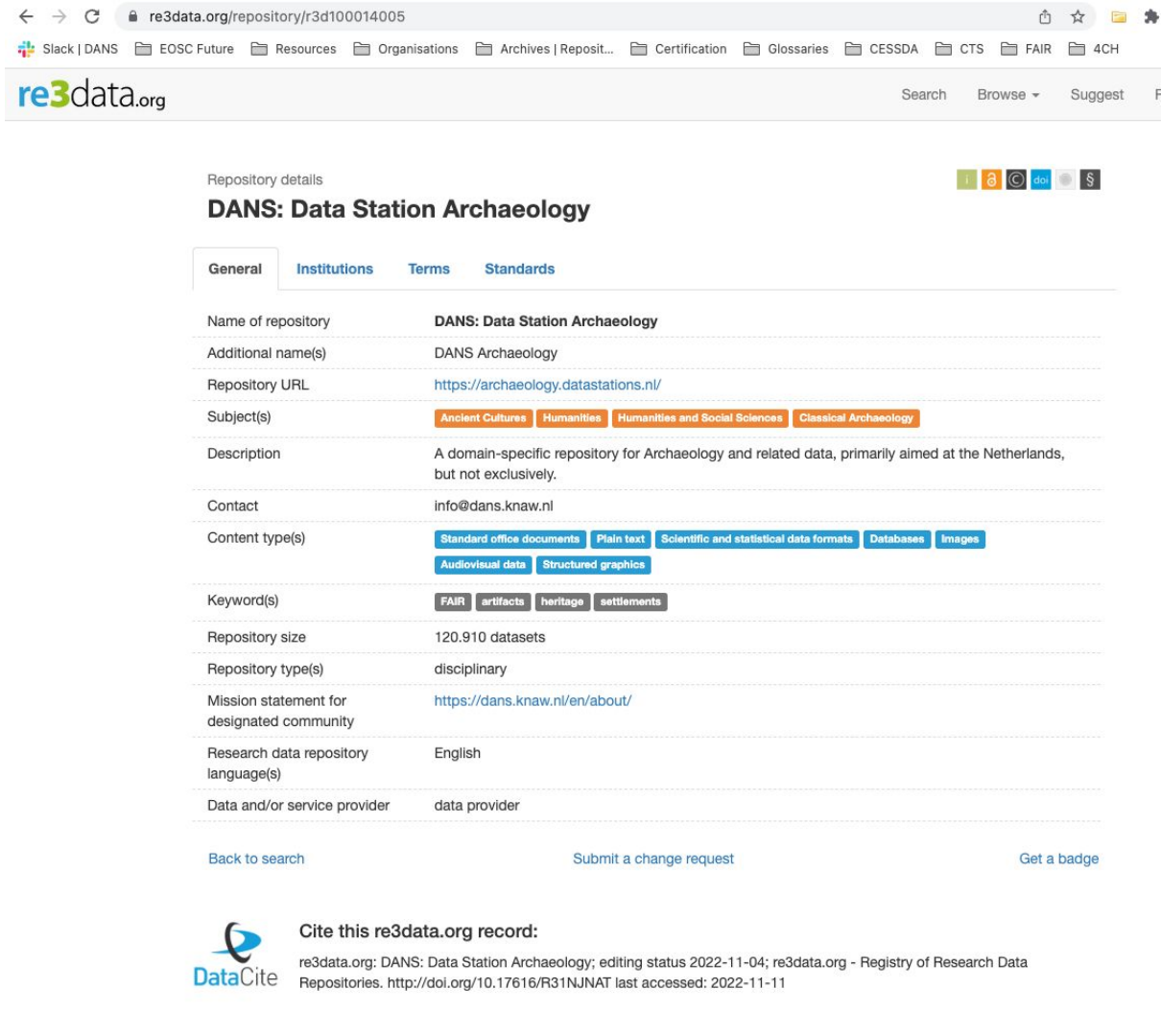
- Assess compliance level against:
  - Response statement
  - Supporting evidence
- Reviewer may propose a lower Compliance Level than selected by the applicant. In that case, a reason is given.

Background Information & Context (R0)

(1) Re3data Identifier
(2) Repository type
(3) Overview
(4) Designated Community
(5) Levels of Curation and Preservation
(6) Cooperation and outsourcing to third parties, partners and host organisations.
(7) Applicants renewing their CoreTrustSeal certification: summary of significant changes since last application.

(1) Re3data Identifier

www.re3data.org



(2) Repository type

Change:
⟶ Select between generalist and specialist repository
⟶ For specialist, provide the domain and disciplines (free text)

Repository A does not specialise in a domain, discipline, specific (research) field or data type, and contains a mixture of everything:

Generalist repository

Repository B contains a lot of social sciences and humanities research datasets, but also caters for other disciplines:

Generalist repository

Repository C only takes on climate datasets:

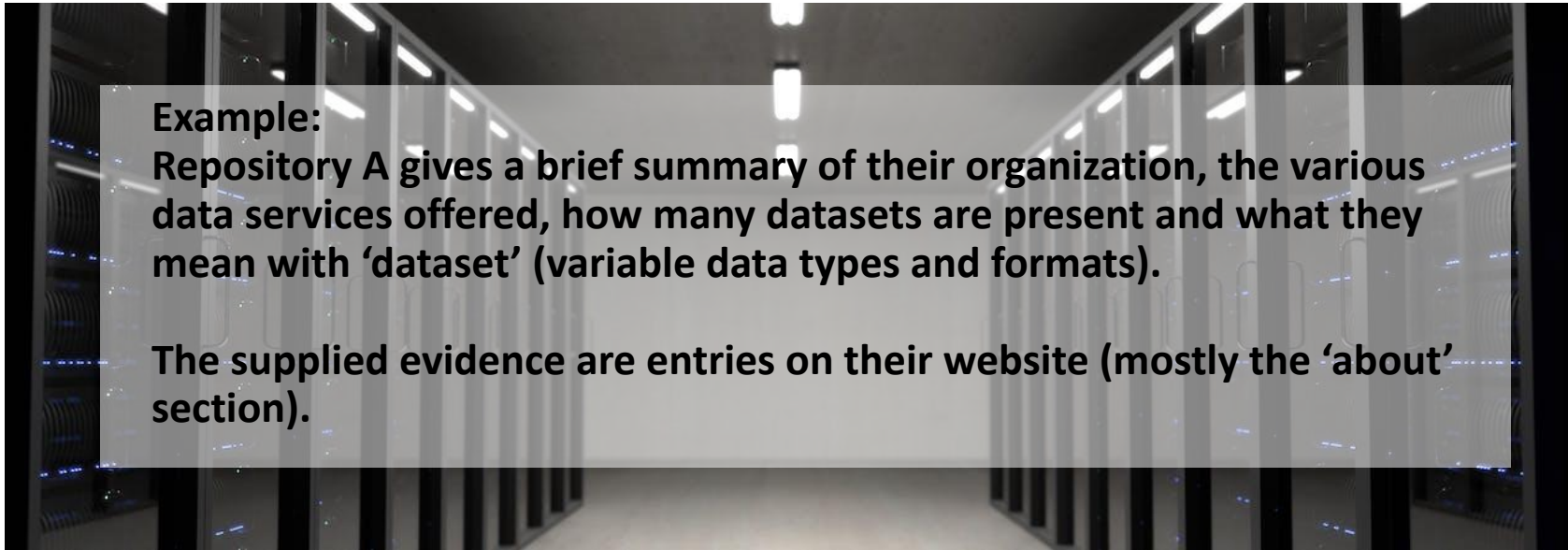
Specialist repository

+ specification of domains

(3) Overview

Key characteristics of the repository:

- **Scope and size of data collections**
- **Data types and formats**
- **Contextual information not covered elsewhere**



Example:
Repository A gives a brief summary of their organization, the various data services offered, how many datasets are present and what they mean with ‘dataset’ (variable data types and formats).

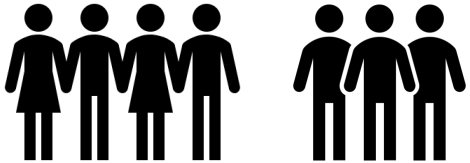
The supplied evidence are entries on their website (mostly the ‘about’ section).

(4) Designated Community

Does the applicant understand the **scope, knowledge base, and methodologies of the (main) target user group(s)?**

Specific definition(s) and description(s), including:

- Composition (how homogeneous?)
- Skills (research methods, language, software)
- Needs (infrastructure, access, file formats)
- Typical re-use scenarios (e.g. read-only or run statistical analyses)



It is possible to have different sub-communities: a description is needed for each.

(4) Designated Community – Example

Repository D's Designated Community is *the immunological research community*, even though its datasets are also of interest for other medical researchers and others like medical users.

The Designated Community may be smaller than the overall group of consumers of the repository data, metadata, and services.


pexels.com/Pavel Danilyuk

(5) Levels of Curation and Preservation

Z. Level Zero. Content distributed as deposited. Unattended deposit-storage-access
D. Deposit Compliance
C. Initial Curation
A. Active Preservation

For each level, concise information on how the level is reached should be added.

e.g. automatic checks of metadata, file format identification, transformation to preservation file formats, etc.

‘Levels of care’

Curation & Preservation levels

Z. Level Zero. Content distributed as deposited. Unattended deposit-storage-access.

D. Deposit Compliance. Non-compliance triggers action as required to meet defined criteria.

C. Initial Curation. Repository takes action as required to meet defined criteria.

A. Active Preservation. Long-term responsibility to take action as required to ensure reuse

Curation is defined as the actions that deliver an **immediate** benefit to digital objects.

Preservation is defined as the additional steps to ensure data and metadata remain accessible, usable, and understandable **into the future**.

Long-term ≠ Forever

Retention ≠ Preservation

CoreTrustSeal Standards and Certification Board. (2022). Curation & Preservation Levels: CoreTrustSeal Discussion Paper (v02.00). Zenodo. https://doi.org/10.5281/zenodo.6908018

Repository types

- **Retention Only**. The repository has no further responsibilities other than to provide effective retention-based services.
- **Deposit Compliance**. The repository checks the deposited materials for compliance with defined criteria and may reject data that do not meet these criteria. No initial curation or further preservation is offered.
- **Initial Curation**. The repository curates the deposited materials to ensure they meet defined criteria. No further preservation is offered.
- **Active Preservation**. In addition to the other levels of care, this repository also takes long-term responsibility for ensuring that the data and metadata can be understood and used by the designated community.

CoreTrustSeal Standards & Certification Board. (2024). Types of Repository: Entities, Responsibilities, Objects. CoreTrustSeal Board Discussion Paper (v01.00). Zenodo. https://doi.org/10.5281/zenodo.13133041

Table of Repository Type Alignment to CoreTrustSeal Requirements

CoreTrustSeal Requirements 2023-2025

1-Applicable, 0- Not applicable,

			Retention Only	Deposit Compliance	Initial Curation	Active Preservation
Part	**Short Name**	**Full Text**	1	1	1	1
Organisational Infrastructure	Mission & Scope (R01)	R01. The repository has an explicit mission to provide access to and preserve digital objects.	1	1	1	1
Organisational Infrastructure	Rights Management (R02)	R02. The repository maintains all applicable rights and monitors compliance.	1	1	1	1
Organisational Infrastructure	Continuity of Service (R03)	R03. The Repository has a plan to ensure ongoing access to and preservation of its data and metadata.	1	1	1	1
Organisational Infrastructure	Legal & Ethical (R04)	R04. The repository ensures to the extent possible that data and metadata are created, curated, preserved, accessed and used in compliance with legal and ethical norms.	1	1	1	1
Organisational Infrastructure	Governance & Resources (R05)	R05. The repository has adequate funding and sufficient numbers of staff managed through a clear system of governance to effectively carry out the mission.	1	1	1	1
Organisational Infrastructure	Expertise & Guidance (R06)	R06. The repository adopts mechanisms to secure ongoing expertise, guidance and feedback-either in-house, or external.	1	1	1	1
Digital Object Management	Provenance and authenticity (R07)	R07. The repository guarantees the authenticity of the digital objects and provides provenance information.	0	1	1	1
Digital Object Management	Deposit & Appraisal (R08)	R08. The repository accepts data and metadata based on defined criteria to ensure relevance and understandability for users.	0	1	1	1
Digital Object Management	Preservation plan (R09)	R09. The repository assumes responsibility for long-term preservation and manages this function in a planned and documented way.	0	0	0	1
Digital Object Management	Quality Assurance (R10)	R10. The repository addresses technical quality and standards compliance, and ensures that sufficient information is available for end users to make quality-related evaluations.	0	1	1	1
Digital Object Management	Workflows (R11)	R11. Digital object management takes place according to defined workflows from deposit to access.	1	1	1	1
Digital Object Management	Discovery and Identification (R12)	R12. The repository enables users to discover the digital objects and refer to them in a persistent way through proper citation.	1	1	1	1
Digital Object Management	Reuse (R13)	R13. The repository enables reuse of the digital objects over time, ensuring that appropriate information is available to support understanding and use.	0	1	1	1
Information Technology & Security	Storage & Integrity (R14)	R14. The repository applies documented processes to ensure data and metadata storage and integrity.	1	1	1	1
Information Technology & Security	Technical Infrastructure (R15)	R15. The repository is managed on well-supported operating systems and other core infrastructural software and hardware appropriate to the services it provides to its Designated Community.	1	1	1	1
Information Technology & Security	Security (R16)	R16. The repository protects the facility and its data, metadata, products, services, and users.	1	1	1	1

Metadata implications

What specific actions follow from being a certain type of repository offering a certain level of care?

How can you be easily transparent about them? E.g. standardised, machine-actionable.

Making agreements to facilitate easy (automated) assessment in the future.

Aspect	Implied Repository Level Information	Implied Object Level Information	Notes
Retention	Standard/Minimum/Maximum Retention Periods (Time)	Minimum Retention Period: Time Maximum Retention Period: Time Retention Start Date: YYYY-MM-DD	Essential information, independent of the level of care
	Exceptions to retention periods applied by the repository.	Exception to retention periods for this specific object.	Documented exceptions that might impact the retention period.
Level of Care	All Levels of Care provided by the repository to objects it holds (Z, D, C, A)	Current Level of Care received by this specific object (Z, D, C, A)	Levels of care from the controlled vocabulary of levels.
D. Deposit Compliance	Documented criteria that a digital object should meet at the point of deposit. Including Semantic (metadata, documentation, rights), technical (format), quality (formal data quality, scientific quality, ethical)	Link to repository level criteria in place when the object was deposited.	E.g. sufficient metadata to meet DataCite criteria when assigning a DOI. e.g., Metadata schema, version: URI e.g. Accepted formats, version: URI e.g. Quality criteria, version: URI
	Outcomes. All potential outcomes of the Deposit Compliance assessment.	Information about the outcome for this specific object.	Non-compliance causes a digital object to be rejected, or a non-

L'Hours, H., Kleemola, M., & Recker, J. (2024). CoreTrustSeal Levels of Curation and Preservation: Implied Repository and Object Metadata Characteristics (v01.00). Zenodo. https://doi.org/10.5281/zenodo.12701324

CoreTrustSeal on Active Preservation

CoreTrustSeal Standards and Certification Board. (2022). Curation & Preservation Levels: CoreTrustSeal Discussion Paper (v02.00). Zenodo. https://doi.org/10.5281/zenodo.6908018

CoreTrustSeal Standards & Certification Board. (2024). Types of Repository: Entities, Responsibilities, Objects. CoreTrustSeal Board Discussion Paper (v01.00). Zenodo. https://doi.org/10.5281/zenodo.13133041

L'Hours, H., Kleemola, M., & Recker, J. (2024). CoreTrustSeal Levels of Curation and Preservation: Implied Repository and Object Metadata Characteristics (v01.00). Zenodo. https://doi.org/10.5281/zenodo.12701324

Summary: https://dans.knaw.nl/en/news/wdpd-evolving-repository-definitions-and-descriptions/

(5) Levels of Curation – examples

Repository D converts data to the relevant data model also incorporating metadata (Curation level D). Their documentation is publicly available.

Repository B offers multiple levels of curation, depending on specific agreements with depositors.

(6) Cooperation and outsourcing to third parties, partners and host organisations

If supported for one or more of the requirements by **another organization** in making decisions or taking actions.
If any function and/or supporting evidence is **not under own control**.

Specified about the organization:

- Its role / function / service
- Its relationship/agreement with the applicant
- Its certifications

The applicant **must retain responsibility for the preservation planning and actions** undertaken to data and metadata to ensure they remain usable by their Designated Community for the long term.

(6) Cooperation and outsourcing to third parties, partners and host organisations – Examples

Repository A uses the premises, HR, and IT support from another, larger organization.

Repository B uses the hosting services from another organization for its backend system.

In both cases, contracts are in place.

(7) Applicants renewing their CoreTrustSeal certification: summary of significant changes since last application

For changes since the last certification (>3 years),
NOT since the last review of the same application.

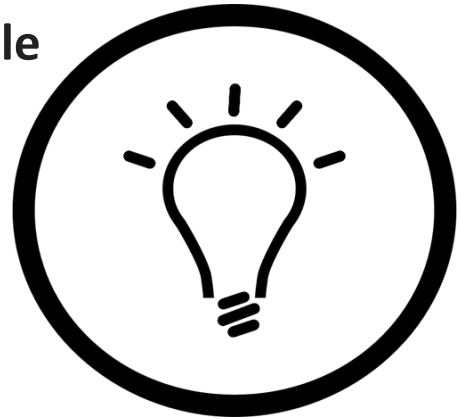
Mission & Scope (R01)

R01. The repository has an explicit mission to provide access to and actively preserve digital objects.

Mission & Scope (R01)

R01. The repository has an explicit mission to provide access to and actively preserve digital objects.

For Trustworthy Repositories it must be clear to depositors and users that **active preservation** of and **continued access** to the digital objects is an **explicit role** of the repository.



Evidence

R01. The repository has an explicit mission to provide access to and actively preserve digital objects.

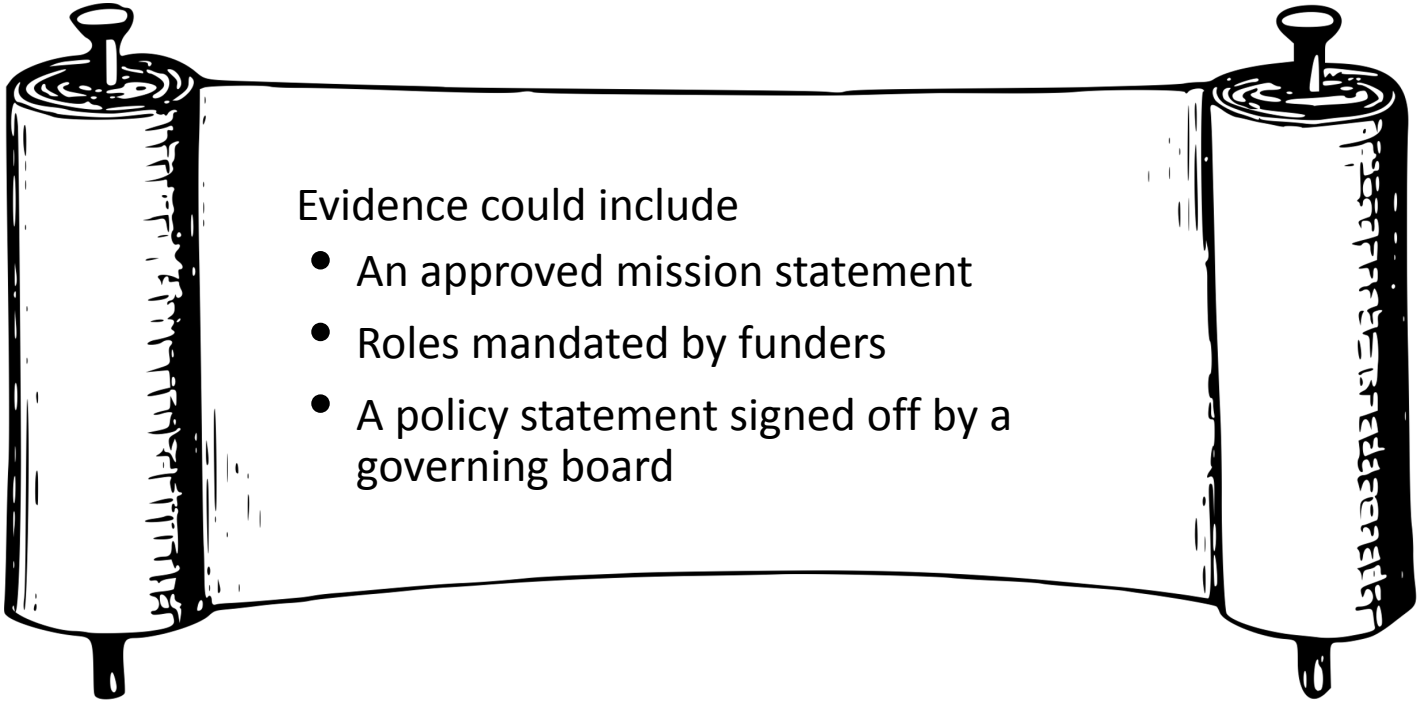
It must be clear that active preservation of and continued access to digital objects is an **explicit role** of the repository.

Required: Evidence of the **mission** as well as the **approval rate**.

! **If preservation is not referred to in the mission of the repository or other relevant public documents, then the compliance level cannot be higher than “In Progress”.**

Evidence

R01. The repository has an explicit mission to provide access to and actively preserve digital objects.



Evidence could include

- An approved mission statement
- Roles mandated by funders
- A policy statement signed off by a governing board

Examples

"Even though it is not stated anywhere, the repository obviously has a mission to preserve data and keep it accessible."

"The Policy, on the public website of the repository, makes explicit the repository's commitment to preserving its digital resources through a comprehensive digital preservation program."

"The policy document referred to above has been approved by the repository's governing board."

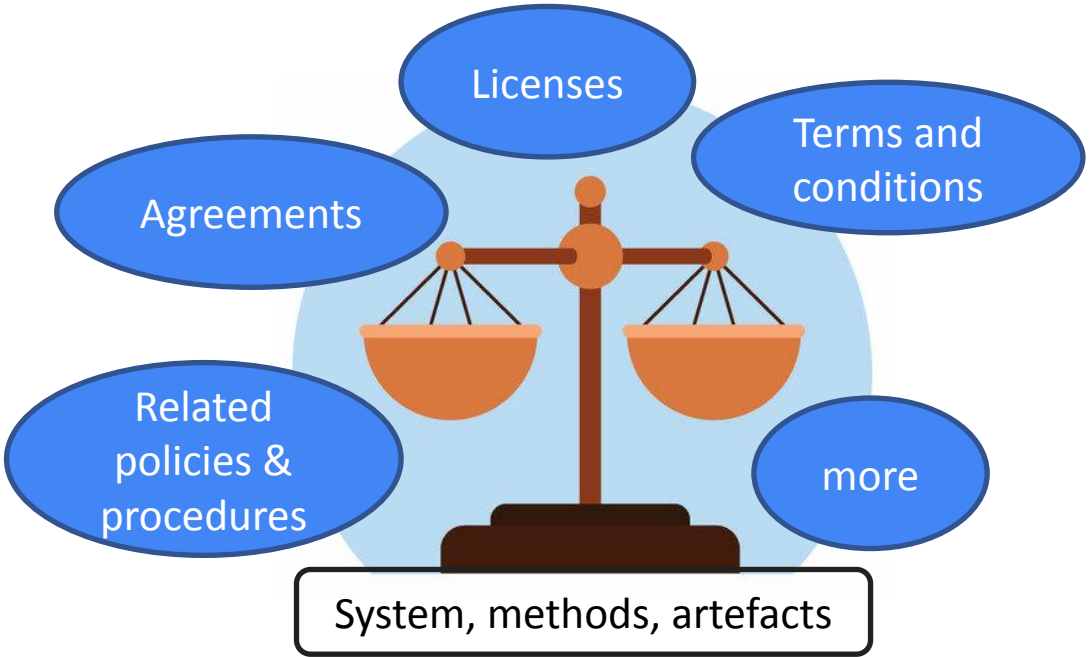
Changes between 2023-2025 and 2026-2028

1. Mission/Scope. R1. The repository has an explicit mission to provide access to and preserve digital objects.

Mission & Scope (R01). The repository has an explicit mission to provide access to and **actively** preserve digital objects.

Rights Management (R02)

R02. The repository maintains all applicable rights and monitors compliance.



Rights Management (R02)

R02. The repository maintains all applicable rights and monitors compliance.

The repository:

- manages and communicates all rights covering data and metadata deposit, storage, preservation, access, use.
- must obtain all necessary rights from the depositor.
- must demonstrate that there are sufficient controls in place to apply and monitor the rights.

Permissions

Prohibitions

Obligations

Evidence

Evidence required of:

- Overall rights management approach to deposited files, data and metadata
- Rights to copy, transform, store, and provide access to Digital Objects
- Conditions of use
- Deposit and access agreements / licenses
- How are rights metadata managed for humans or machines?
- Monitoring of compliance
- Measures for non-compliance (ideally public policy)

Examples

“A user license has to be acquired, even if the resource is available free of charge.”

”The data can be used for non-commercial purposes without restriction."

“If the license conditions are not complied with, the repository will request the user to immediately discontinue using the dataset.”

License / agreement:

CC-BY 4.0

Examples

Absence of monitoring (or evidence of this).

Absence of measures in place if non-compliance is detected.

For applicants that hold data or metadata with a disclosure risk: measures planned but not yet implemented is not accepted.

Changes between 2023-2025 and 2026-2028

Rights Management. R02. The repository maintains all applicable rights and monitors compliance.

NO CHANGES

Continuity of Service (R03)

R03. The repository has a plan to ensure ongoing access to and preservation of its data and metadata.

Continuity of Service (R03)

R03. The repository has a plan to ensure ongoing access to and preservation of its data and metadata.

- Business continuity
- Disaster recovery
- Succession planning

Romain Guy (Public Domain)

Evidence

The response and evidence should demonstrate:

- Functions and services offered. Are they shared? What is the **level of responsibility** taken by the repository?
- The approach to rapid changes in circumstance and long-term planning. What is the **level of risk**?
- **Succession planning**: Relocation / transition options. Ideally a formal agreement between the repository and a successor.
- The a… …e.

If there is no formal, written agreement between the repository and a successor, then the compliance level cannot be higher than "In Progress".

Examples

"In the unlikely event of closure, Repository A will be transferred to National Repository B (link to written agreement)."

"It is unlikely Repository A will ever be closed."
[without further plans]

"While we deem closure of the repository very unlikely due to steady funding levels and the presence of a parent organisation who are committed to open science, we are working hard on securing an official agreement with this parent organisation."

Changes between 2023-2025 and 2026-2028

Continuity of Service (R03). The repository has a plan to ensure ongoing access to and preservation of its data and metadata.

NO CHANGES, small additions to the Extended Guidance to clarify things even further.

Legal & Ethical (R04)

R04. The repository ensures to the extent possible that data and metadata are created, curated, preserved, accessed and used in compliance with legal and ethical norms.

Legal & Ethical (R04)

R04. The repository ensures to the extent possible that data and metadata are created, curated, preserved, accessed and used in compliance with legal and ethical norms.

A trustworthy repository has practices in place that reflect the **legal status** and **sensitivity** of the digital objects in their holding, including guidance for depositors and users on how to create, curate, and use the object.

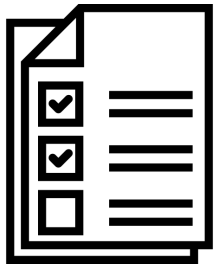
Depositors should feel **safe** to deposit sensitive or confidential data in the repository. Users should feel **informed** on how to interact with all digital objects.

Evidence

R04. The repository ensures to the extent possible that data and metadata are created, curated, preserved, accessed and used in compliance with legal and ethical norms.

Evidence needed in response statement:

- How does the repository identify and manage relevant legal and ethical standards?
- How does the repository comply with specific legal and/or ethical discipline or domain standards?
- What information is requested from depositors to confirm that data collection or creation was carried out in accordance with legal and ethical criteria?
- Does the repository hold any data or metadata with disclosure risk (e.g. depositor/user information, personal, cultural, or environmental information)?



Further evidence

➔ Does the repository hold any data or metadata with **disclosure risk** (e.g. depositor/user information, personal, cultural, or environmental information)?

If **yes**, the repository must include further evidence on:

- Special procedures applied to manage disclosure risk;
- Conditions of distribution, access protection and use;
- Processes to review disclosure risk and to take the necessary steps to either anonymize files or to provide access in a secure way;
- Staff training in the management of digital objects with disclosure risk;
- Guidance provided on the responsible deposit, download, and use of disclosive or potentially disclosive data and metadata.

Target compliance level: ***"Implemented: the requirement has been fully implemented by the repository"***

Related evidence that should be reported elsewhere:

Management of related rights and compliance checks → **Rights (R02)**

Measures to protect digital objects → **Security (R16)**

Examples

"The repository assumes the depositor complies with relevant regulations."

"The depositor must sign a Deposit Agreement which specifies the obligations for the Depositor, such as the written confirmation of compliance with relevant legislations."

"Document X on the public website of the repository details guidance on the ethical deposit and use of (disclosive) data."

"The repository is 'In Progress' of developing staff training on the managing of digital objects with disclosure risk."

Changes between 2023-2025 and 2026-2028

Legal & Ethical (R04)

R04. The repository ensures to the extent possible that data and metadata are created, curated, preserved, accessed and used in compliance with legal and ethical norms.

NO CHANGES

Governance & Resources (R05)

R05. The repository has adequate funding and sufficient numbers of staff managed through a clear system of governance to effectively carry out the mission.

Governance & Resources (R05)

R05. The repository has adequate funding and sufficient numbers of staff managed through a clear system of governance to effectively carry out the mission.

A trustworthy digital repository is **transparent** about its financing, governance, responsibilities, and decision making.

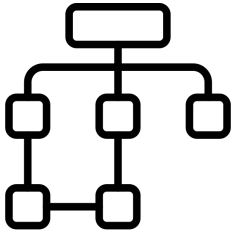
Depositors and users should feel **assured** that the repository can adequately offer the service it promises

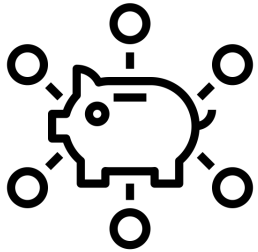
Evidence

R05. The repository has adequate funding and sufficient numbers of staff managed through a clear system of governance to effectively carry out the mission.

Evidence needed in response statement:

- Descriptions and diagrams of governance bodies, groups and hierarchies.
- Timescales for provision and renewal of funding for operational costs and recruitment.
- Evidence that the repository is, or is hosted by, a recognized institution (supporting long-term stability and sustainability) appropriate to its Designated Community.
- Demonstrate that the repository can meet its obligations, including sufficient funding, staff resources, IT resources, and a budget for external engagement when necessary.





Further evidence could include: structural/project funding balance, total FTEs, permanent/temporary contracts.

Related evidence that should be reported elsewhere:

Availability of appropriate expertise → **Expertise (R06)**

Examples

"The repository is organised and governed as follows (...). There is no public webpage displaying this information."

"The repository receives funding from X for the period of xxxx-xxxx and is involved in external project A in the year xxxx."

"Repository for discipline X is hosted by the National Institute for X."

"The repository invests ample opportunity for the professional development of staff."

Changes between 2023-2025 and 2026-2028

Governance & Resources (R05)

R05. The repository has adequate funding and sufficient numbers of staff managed through a clear system of governance to effectively carry out the mission.

NO CHANGES. Addition of "Description and diagrams of governance bodies, groups and hierarchies" to the Extended Guidance.

Expertise & Guidance (R06)

R06. The repository adopts mechanisms to secure ongoing expertise, guidance and feedback - either in-house, or external.

Expertise & Guidance (R06)

R06. The repository adopts mechanisms to secure ongoing expertise, guidance and feedback - either in-house, or external.

A trustworthy digital repository must identify the **skills** necessary to deliver the services it offers, as well as strive to remain **valuable** to its Designated Community by improving its expertise and skills for the future.

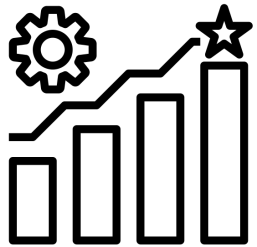
Depositors should feel **convinced** that the repository knows how to deliver on the services it promises, and that it looks to **maintain or improve** these capabilities over time in line with the developments that are expected to occur in the community.

Evidence

R06. The repository adopts mechanisms to secure ongoing expertise, guidance and feedback - either in-house, or external.

Evidence needed in response statement:

- Guidance and expertise reflects the scientific scope of the repository.
- The repository aligns internal recruitment and external engagement with the services it offers.
- The repository ensures that its staff have access to ongoing training and professional development.
- The range and depth of expertise of both the organisation and its staff is appropriate to the mission.
- Information on the in-house advisers, or external advisory committees that include technical, curation, data science, data security, and disciplinary experts that are used by the repository.
- Information on how the repository communicates with experts for advice.



Examples

"All staff is knowledgeable."

"The repository has an external advisory board that oversees the activities and gives advice both on request and as they see fit."

"The repository exchanges expertise and skills in the context of project X and collaboration Y."

"The repository interacts directly with its Designated Community to identify developments in the field that the repository needs to address in its expertise and or services."

Changes between 2023-2025 and 2026-2028

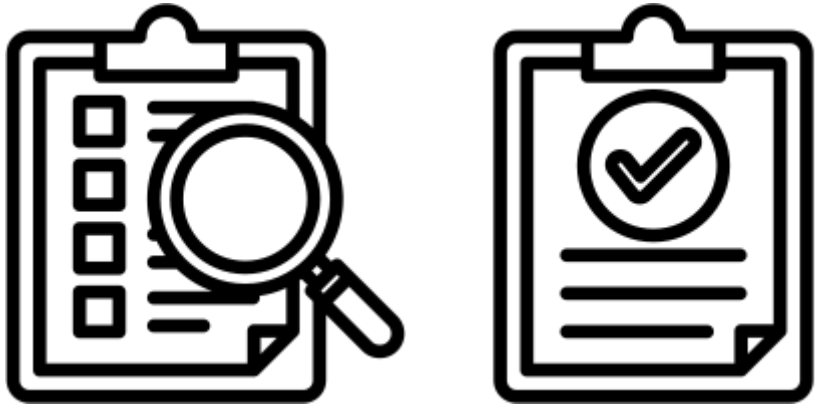
Expertise & Guidance (R06)

R06. The repository adopts mechanisms to secure ongoing expertise, guidance and feedback - either in-house, or external.

NO CHANGES

Provenance and authenticity (R07)

R07. The repository guarantees the authenticity of the digital objects and provides provenance information.



Provenance and authenticity (R07)

R07. The repository guarantees the authenticity of the digital objects and provides provenance information.

The repository should provide evidence to show that it operates a data and metadata management system that maintains provenance information to ensure authenticity from deposit, and through curation and preservation to the point of access.

Any intentional changes to data and metadata should be documented, including the rationale and originator of the change. Authenticity covers reliability and provenance, including the relationship between the deposited digital objects and those provided at the point of access.

Evidence

R07. The repository guarantees the authenticity of the digital objects and provides provenance information.

Evidence needed in response statement:

- The repository approach to changing and versioning data and metadata. How the approach and records of changes are communicated to data depositors and users.
- The provenance information and audit trails recorded for data and metadata processing and versioning.
- How the repository compares the essential properties of different versions of the same file.
- Identification checks for depositors.

Examples

The depositor has permissions to make changes to the record at any time, and assumes responsibility to update a change log.

A relational database maintains a timestamped record of metadata changes, including which staff member applied that change based on their account login.

The data manipulation software used to transform data is saved in a code repository with versioning history. A record of when these routines are applied to a given dataset is retained.

Automated testing ensures that consistent results of a particular data query returns the same product over time, with any discrepancies investigated and rectified or justified as deemed appropriate.

Changes between 2023-2025 and 2026-2028

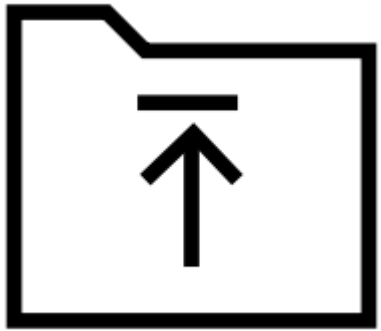
Provenance and authenticity (R07)

R07. The repository guarantees the authenticity of the digital objects and provides provenance information.

NO CHANGES.

Deposit & Appraisal & Accessibility (R08)

R08. The repository accepts data and metadata based on defined criteria to ensure relevance and accessibility for users.



Deposit & Appraisal & Accessibility (R08)

R08. The repository accepts data and metadata based on defined criteria to ensure relevance and accessibility for users.

The appraisal function during deposit is critical to evaluate whether digital objects meet all criteria for selection and to ensure appropriate management for their preservation. Appraisal ensures that deposited digital objects are relevant and are, or can become, understandable to the Designated Community.

This Requirement covers the selection criteria applied at the point of deposit. Data Quality (R11) should be used to address steps taken by the repository during the curation process.

Evidence

R08. The repository accepts data and metadata based on defined criteria to ensure relevance and understandability for users.

Evidence needed in response statement:

- Any documented deposit process that includes steps to ensure that data and metadata are sufficient for long-term preservation.
- A collection development policy or procedures to guide the selection of digital objects.
- Criteria for prioritisation and any different curation-levels or preservation levels defined during appraisal.
- The approach to digital objects that do not fall within the mission/collection profile.
- Procedures to determine that the metadata required to interpret and use the digital objects are provided.

.

Evidence

R08. The repository accepts data and metadata based on defined criteria to ensure relevance and understandability for users.

Evidence needed in response statement (continued):

- Any automated assessment of metadata adherence to relevant schemas.
- The repository approach if metadata provided is insufficient for long-term preservation.
- A list of preferred formats.
- Checks in place to ensure that depositors adhere to the preferred formats.
- The approach towards digital objects that are deposited in non-preferred formats.
- The transfer of custody and responsibility during the handover from the depositor to the repository.

Examples

Researchers self-assess whether the repository meets their needs, and then upload their files to receive a DOI

The assigned curator evaluates the dataset submission using a criteria checklist (link here) to ensure the dataset is in scope and contains essential elements.

All required metadata from the depository are automatically verified upon submission. Any errors or omissions are flagged, so that they can be addressed.

In the event that the dataset is in scope, but curatorial processes do not yet exist, a committee evaluates the priority of that dataset according to an established rubric. New processes can then be defined for high priority datasets as resources permit.

Changes between 2023-2025 and 2023-2025

Deposit & Appraisal (R08)

R08. The repository accepts data and metadata based on defined criteria to ensure relevance and understandability for users.

Deposit & Appraisal & Accessibility (R08)

R08. The repository accepts data and metadata based on defined criteria to ensure relevance and accessibility for users.

Preservation plan (R09)

R09. The repository assumes responsibility for long-term preservation and manages this function in a planned and documented way.

Preservation plan (R09)

R09. The repository assumes responsibility for long-term preservation and manages this function in a planned and documented way.

The repository, depositors, and Designated Community need to understand the level of responsibility undertaken for the long-term preservation of data and metadata. This exceeds bit level integrity alone and covers plans to respond to potential future changes which may impact the understandability and reusability of data and metadata over time. Procedures must be documented and their completion assured.

The execution and details of these plans relate to other requirements that can be cross-referenced, although this requirement to ensure that preservation has a thoughtful documented plan that ensures accountability and longevity.

Evidence

R09. The repository assumes responsibility for long-term preservation and manages this function in a planned and documented way.

Evidence needed in response statement:

- The documented approach to preservation, including whether this involves format migration, emulation, etc.
- File formats and metadata schemas for long term preservation.
- How the level of responsibility for the preservation of each item is defined.
- Plans related to future migrations or similar measures to address the threat of obsolescence.
- Actions relevant to preservation specified in documentation, including custody transfer, submission information criteria, and preservation information metadata.

Evidence

R09. The repository assumes responsibility for long-term preservation and manages this function in a planned and documented way.

Evidence needed in response statement (continued):

- Measures to ensure these actions are taken.
- Any minimum stated retention and/or preservation periods.
- How often the digital objects are re-appraised and the possible outcomes of reappraisal.
- The repository approach to deleting/removing data and metadata from collection/holdings including the impact on persistent identifiers as well as the availability and curation of tombstone records.

.

Examples

Once a dataset is published, preservation is fully achieved by bit-level verifications on the metadata and data contents.

While submitted data is stored its original form, a conversion to a standardized non-proprietary format is always ensured for interoperable distribution and preservation. The list of preferred formats is available on our website (link here).

The preservation plan (link here) accounts for metadata updates, data format evolution, and technology migrations. Metadata procedures are in place to handle evolving community standards and information availability, such as schema updates (e.g., DataCite schema), controlled vocabularies, or related resources(e.g., publications).

In the rare occasion that access to a dataset is removed, the persistent identifiers can still be resolved with basic descriptive metadata and the rationale for removal (e.g., sensitive data issues or duplication).

Changes between 2023-2025 and 2026-2028

Preservation plan (R09)

R09. The repository assumes responsibility for long-term preservation and manages this function in a planned and documented way.

NO CHANGES, only some additional explanation to the Extended guidance.

SKUPINSKO DELO (15-20 min)

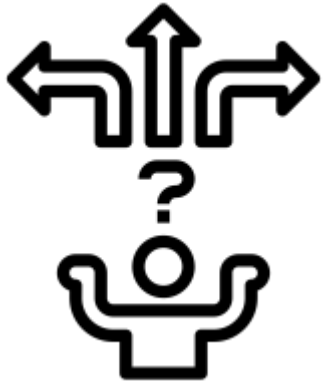
Nastopate v vlogi ocenjevalca CoreTrustSeal prijav.

Vaša naloga je, da pregledate odgovor izmišljene organizacije na izbrano zahtevo CTS in ga kritično ocenite, kot bi to storil uradni ocenjevalec CTS.

- 3 skupine

Quality Assurance (R10)

R10. The repository addresses technical quality and standards compliance, and ensures that sufficient information is available for end users to make quality-related evaluations.



Quality Assurance (R10)

R10. The repository addresses technical quality and standards compliance, and ensures that sufficient information is available for end users to make quality-related evaluations.

Different repositories undertake different levels of curation on data, metadata and documentation depending on the needs and expectations of their depositors and Designated Community. Quality assurance by the repository ensures that digital objects comply with a range of standard criteria including acceptable formats, metadata schema, metadata content and links to other digital objects.

This relates to 'technical quality' rather than the 'scientific quality' of the original digital objects creation or collection prior to deposit, though the repository must ensure there is sufficient information about the digital objects for the Designated Community to assess their fitness for use. Data, or associated metadata, may have quality issues relevant to their research value, but this does not preclude their use if a user can make a well-informed decision on their suitability through provided documentation.

Evidence

R10. The repository addresses technical quality and standards compliance, and ensures that sufficient information is available for end users to make quality-related evaluations.

Evidence needed in response statement:

- The approach to data and metadata quality taken by the repository including variations for different curation-levels.
- The standards that data, metadata and documentation must comply with to be acceptable for preservation and access. Whether these are general external standards, internally developed standards or specific to a community of practice.
- The quality control checks in place ensure the completeness and understandability of data and metadata.
- The approach to resolving issues e.g. whether the digital objects are returned to the depositor for rectification, fixed by the repository, noted by quality flags, and/or included in the accompanying metadata.

Evidence

R10. The repository addresses technical quality and standards compliance, and ensures that sufficient information is available for end users to make quality-related evaluations.

Evidence needed in response statement (continued):

- The approach to managing changes to expected standards (e.g. new or updated data formats of metadata schemas) in response to changes in the technical environment or to changes in the needs of the Designated Community.
- Any links provided to other digital objects' data and metadata e.g. related digital objects, publications, or the use of controlled vocabularies and ontologies.

Examples

The depositor who enters the metadata and uploads data files is solely responsible for quality assurance, as outlined in their agreement with the repository.

A data curator is assigned to each deposited dataset to verify that all required metadata and data content is properly entered and formatted, using a combination of validation tools and expert judgement.

The metadata includes information that influences data quality, such as measurement accuracy, calibration records and method limitations.

Automated data assurance checks are executed for real-time data streams for core instrument types (listed at link). Results are provided in the data files, and curators investigate failures to determine cause and remediation.

Changes between 2023-2025 and 2026-2028

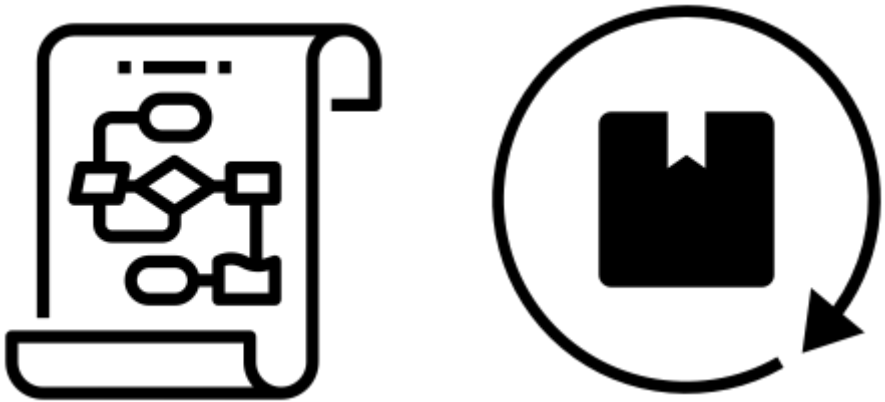
Quality Assurance (R10)

R10. The repository addresses technical quality and standards compliance, and ensures that sufficient information is available for end users to make quality-related evaluations.

NO CHANGES

Workflows (R11)

R11. Digital object management takes place according to defined workflows from deposit to access.



Workflows (R11)

R11. Digital object management takes place according to defined workflows from deposit to access.

For Quality Assurance (R10) to be achieved, it is necessary to avoid ad hoc actions and to deliver consistency of practice for all digital objects and across repository functions. This requires that workflows be defined, documented, and change-managed. Workflows may be specified in a mixture of standard operating procedures, business process descriptions and diagrams that guide normal practice and provide mechanisms for handling exceptions.

This Requirement confirms that all workflows are documented. You can include a diagram to illustrate this. It should be noted if there are different workflows for different levels of security mentioned in the Legal and Ethical (R04) response statement. Workflows may include qualitative and quantitative checking of outputs, but any detail on checks and compliance should be addressed under Quality Assurance (R10).

Evidence

R11. Digital object management takes place according to defined workflows from deposit to access.

Evidence needed in response statement:

- Workflows/business process descriptions covering the curation levels performed.
- How workflows are adjusted for different types of data and metadata.
- Decision handling within the workflows.
- Change management of workflows.
- Ability to track workflow execution, with mechanisms to handle exceptions.

Examples

A recommended workflow is available on our website for depositors to follow, and it is their responsibility to ensure that these steps are taken.

This reference (link here) shows a detailed break-down and diagram of the data ingest workflow, including various pathways for different data types.

On an annual basis, workflows are reviewed and updated to align with any changes in best practices or expectations.

A data curator supports the depositor through the data ingestion workflow, tracking completion of steps and any specific comments along the way.

Changes between 2023-2025 and 2026-2028

Workflows (R11)

R11. Digital object management takes place according to defined workflows from deposit to access.

NO CHANGES.

Discovery and Identification (R12)

R12. The repository enables users to discover the digital objects and refer to them in a persistent way through proper citation.

Discovery and Identification (R12)

R12. The repository enables users to discover the digital objects and refer to them in a persistent way through proper citation.

Effective data and metadata sharing discovery is key to resource discovery. Once discovered, digital objects should be referenceable through full citations, including persistent identifiers (PIDs) to help ensure that they can be accessed into the future.

Applicants should describe their use of a third party persistent identifier system, or document their own approach to ensuring that identifiers remain globally unique and persistent. The use of a third party to support PID creation and resolution is not sufficient; applicants should describe how they ensure that identifiers continue to resolve to the correct data or metadata over time, including the version rules that guide when a new identifier is created for a digital object. Applicants that do not have a persistent identifier solution cannot achieve “Implemented: the requirement has been fully implemented by the repository” for this requirement.

Evidence

R12. The repository enables users to discover the digital objects and refer to them in a persistent way through proper citation.

Evidence needed in response statement:

- The search facilities offered by the repository.
- The standards that a searchable metadata catalogue complies with.
- The approach to ensuring that identifiers are unique and persistent.
- Machine harvesting of the metadata.
- Repository, or repository data and metadata, inclusion in disciplinary or generic registries of resources.
- Recommended data citations.

Examples

Available datasets are only allocated persistent identifiers upon depositor request to support their own published research or funder requirements.

A search interface allows for datasets to be discovered by keywords, geographical area, variable type, contributing individuals/organizations, and more.

A data citation is provided for each dataset according to the Data Citation Guidelines for Earth Science Data (reference link).

Persistent identifiers are applied to datasets using DataCite DOIs, with contributing party PIDs (e.g., ORCIDs, RORs) included when available.

Changes between 2023-2025 and 2026-2028

Discovery and Identification (R12)

R12. The repository enables users to discover the digital objects and refer to them in a persistent way through proper citation.

NO CHANGES

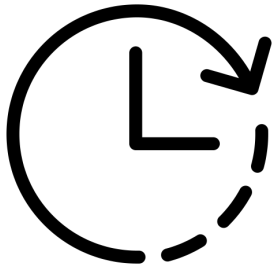
ReUse (R13)

R13. The repository enables reuse of the digital objects over time, ensuring that appropriate information is available to support understanding and use.

ReUse (R13)

R13. The repository enables reuse of the digital objects over time, ensuring that appropriate information is available to support understanding and use.

Trustworthy digital repositories must ensure that data and metadata continue to be **understood** and **used effectively** into the future despite changes in technology and the Designated Community's knowledge base.



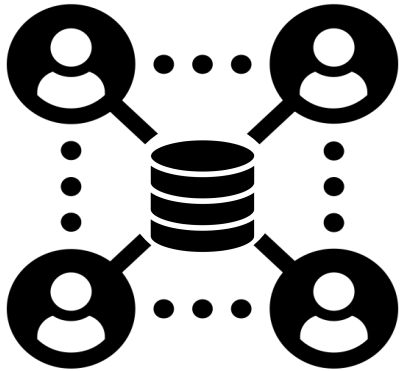
Depositors must be **ensured** that their data will remain **relevant** over time, following the most recent standards and norms of their field. Users should be able to find, understand, and use data **without problem** no matter when it was originally deposited.

Evidence

R13. The repository enables reuse of the digital objects over time, ensuring that appropriate information is available to support understanding and use.

Evidence needed in response statement:

- The ways in which the repository engages with their Designated Community of users to identify their needs.
- The data formats, metadata schemas, controlled vocabularies and ontologies used to support reuse, and how these meet the community needs.
- The metadata and documentation provided at the point of access to support understandability and reuse appropriate to the Designated Community. This may include information specific to data type, e.g. manuals, calibration records, photos, protocols.
- Measures to ensure that data and metadata remain understandable.
- Management of changes to data, metadata, documentation or other information that supports reuse.



Examples

"The repository does not support versioning of records."

"The repository actively monitors the relevant standards and norms in the Designated Community via a yearly survey."

"The repository provides a list of preferred file formats suitable for long term preservation and works together with the depositor to make sure all files adhere to these."

"The repository uses Dublin Core for all metadata."

Changes between 2023-2025 and 2026-2028

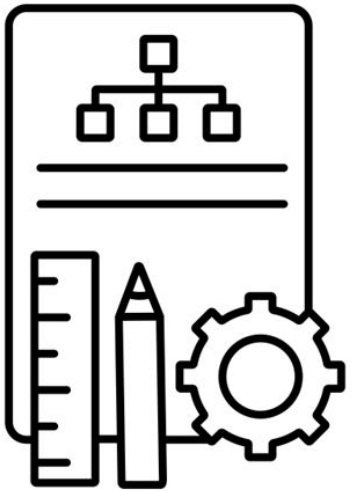
ReUse (R13)

R13. The repository enables reuse of the digital objects over time, ensuring that appropriate information is available to support understanding and use.

NO CHANGES

Storage & Integrity (R14)

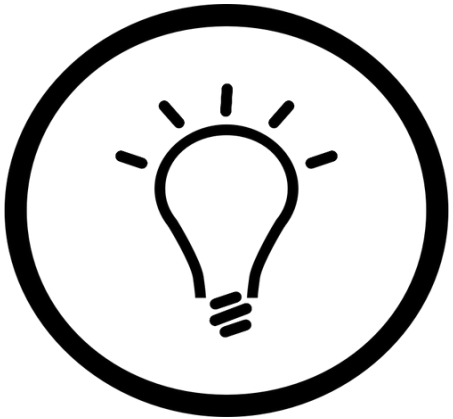
R14. The repository applies documented processes to ensure data and metadata storage and integrity.



Storage & Integrity (R14)

R14. The repository applies documented processes to ensure data and metadata storage and integrity.

The repository must store **data** and **metadata** to enable the curation and preservation of the digital objects. The measures to ensure that unintentional or unauthorised changes can be detected and correct versions restored should be detailed.



Evidence

R14. The repository applies documented processes to ensure data and metadata storage and integrity.

Required: Existence of **documented procedures** for each of the storage locations to

- Verify that a digital object has not been altered or corrupted from deposit to use (e.g., fixity checks);
- Ensure that data and metadata are only deleted as part of an approved and documented process;
- Handle and monitor deterioration of storage media.

!

Storage and integrity measures are not part of Technical Infrastructure (R15) or Security (R16) requirements. Management of intentional changes to the data and metadata should be covered under Provenance & Authenticity (R07).

Examples

"The repository uses checksums for all data."

"Fixity for the archival storage is implemented on storage and on object level. Data is stored and backed-up automatically and the media are automatically monitored for block-level integrity."

"When a new or amended deposit moves from the Ingest to the Archival Storage team a checksum (MD5) is generated for each file with the Archival Information Package (AIP)."

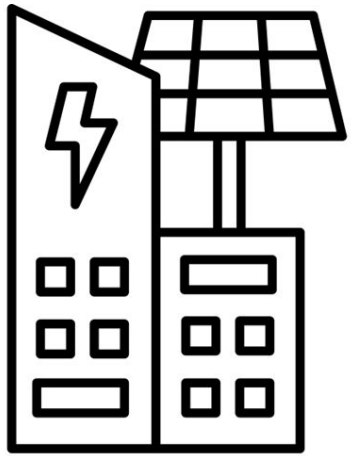
Changes between 2023-2025 and 2026-2028

Storage & **Integrity (R14).** **The repository applies documented processes to ensure data and metadata storage and integrity.**

NO CHANGES

Technical Infrastructure (R15)

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

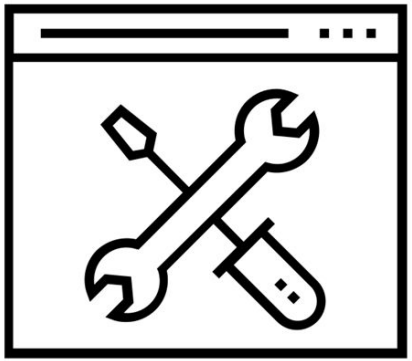


Technical Infrastructure (R15)

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

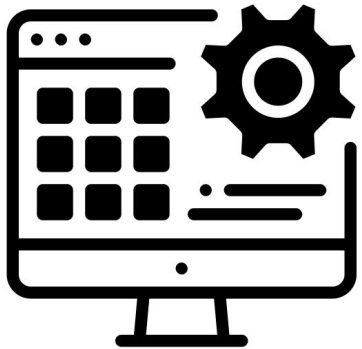
Trustworthy digital repositories must ensure that their infrastructure and services are **reliable**, **stable** and that **availability** is maximized.

Depositors and users must be ensured that **hardware** and **software** used are relevant and appropriate to their **needs**.



Evidence

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



Evidences in response statement :.

The approach for IT service management and the functions implemented (e.g. systems documentation, configuration management database, code/software repositories, version control, disaster recovery), and processes in place to manage and track changes.

Evidence

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

Other evidences in response statement :

- The description of international, community or other technical infrastructure standards in place and how compliance is monitored.
- The details of community supported, open source, or locally developed software.
- The measures taken to monitor availability, bandwidth, and connectivity.

Examples

"The repository has 5 servers at its disposal 3 of which are in a so called primary server room the remaining 2 are in a so called backup server room."

"The repository is based on a Fedora Commons repository 3. It runs on Red Hat Enterprise Linux. Services to the Designated Community such as deposition and dissemination front-ends are implemented as separate services. For institutional depositors, there is a machine-machine deposit interface, based on the SWORD 2.0 protocol."

"Standards and classifications in use include the following: DDI Data Documentation Initiative (version 2.5), ELSST (European Language Social Science Thesaurus) and ISO27001 for Information Security."

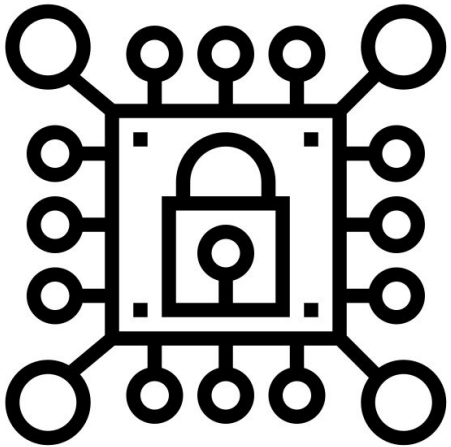
Changes between 2023-2025 and 2026-2028

Technical Infrastructure **(R15).** The repository is managed on well-supported operating systems and other core infrastructural software and hardware appropriate to the services it provides to its Designated Community..

NO CHANGES

Security (R16)

R16. The repository protects the facility and its data, metadata, products, services, and users.



Security (R16)

R16. The repository protects the facility and its data, metadata, products, services, and users.

Trustworthy digital repositories should perform a risk analysis on potential **threats**, **failures**, or **damage scenarios**. They must ensure that **measures** measures are in place to **mitigate** these risks based on their impact and probability.

Depositors and users must be ensured that a security **plan** which complies with industry standards is in place and their **assets** are protected.

Evidence

R16. The repository protects the facility and its data, metadata, products, services, and users.

Evidences in response statement :

- The I/T security system, employees with roles related to security (e.g. security officers), and any risk analysis approach in use or security-specific standards implemented.
- Measures in place to protect

The facility. How the premises where digital objects are held are secured

The access to systems. Any authentication and authorization procedures.

The access to the different data and metadata and environments

Examples

"A central detection and automatic neutral-gas extinguishing system covers fire safety in addition to the machine-room layout, which is designed to provide fire protection for more than one hour. The four rooms are monitored separately with multiple sensors."

"The solution utilizes only secure interfaces such as TLS 1.2 or above. All data in transit and at rest is encrypted with at least AES-256 or equivalent. The solution supports secure encrypted data storage both on and offsite which includes secure key management."

"The repository has an IT operations handbook that also described disaster recovery procedures and responsibilities. This handbook is in line with the ISO 27001 information security standard and is audited by the head office of the repository."

Maintenance Group

- CoreTrustSeal Maintenance WG Established
  - https://www.rd-alliance.org/groups/coretrustseal-maintenance-wg
- Join
  - Contribute to future revisions
  - Champion CoreTrustSeal
  - Support inclusion & improvement
- Other involvement
  - RDA/WDS Certification of Digital Repositories IG
  - RDA/WDS TRUST Principles Outreach and Adoption WG
  - Community-based catalogue of requirements for trustworthy Technical Repository Service Providers WG

Vprašanja?

Za pomoč pri pripravi prijav smo vam na voljo: maja.dolinar@fdv.uni-lj.si