Draft Change Log: CoreTrustSeal Requirements 2023-2025

Introduction

To maintain alignment with practice and to ensure the requirements meet community needs, the CoreTrustSeal Requirements and supporting guidance are subject to feedback and revision every three years. The new Requirements will be in place from 2023-2025, all existing certifications under previous requirements remain valid until due for renewal.

The CoreTrustSeal mission continues to be provision of a low barrier to entry 'core' level of requirements that is broadly applicable to repository data service providers that ensure the long term preservation of the digital objects they curate for the benefit of a defined designated community.

This draft change log document accompanies the draft release (2022-06) of the revised CoreTrustSeal Requirement for 2023-2025. It describes the changes implemented based on Board proposals and community feedback. The Requirements remain in draft and open for comment on significant issues or errors until the 15th of July, 2022. A final version of the Requirements will be released in September 2022, followed by a revised Extended Guidance document and supporting Glossary.

The changes proposed by the Board based on their experience of certifying against the Requirements were overwhelmingly supported by community feedback. The Guidance has been editorially reviewed for additional clarity, to minimise perceived overlap between Requirements, and with an international audience in mind. Many of the excellent proposals received during the feedback period have been incorporated into the Guidance where they were within the scope of a 'core' Requirements set. Some proposals were not incorporated due to being too challenging for the broad range of repositories, or too domain or disciplinary specific to be included in the guidance. There were some proposals for which there is not yet sufficient community consensus for integration; some of these will form part of future CoreTrustSeal work to identify and address community priorities for clarification. These areas for future work include additional alignment with the FAIR Data Principles, definitions of 'levels of preservation' and the differing expectations of specialist and generalist repositories.

Synopsis of Changes

The diagram below provides an overview of changes to the short Requirements text and to the structure of CoreTrustSeal. This is intended to provide an easy reference point for those renewing their CoreTrustSeal applications, and to support comparison between assessments undertaken against different versions of the requirements. The remainder of this document follows the latest CoreTrustSeal Requirements text and structure.

CoreTrustSeal retains a 'core' level focus and expects the evidence necessary to achieve CoreTrustSeal to remain stable. Requirement names have been revised for clarity. Integrity measures are united with Storage under Storage & Integrity (R14).

The CoreTrustSeal Compliance levels have been simplified to:

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

Applicants may still find it useful to use the additional previous compliant levels during internal self-assessments: “The Repository has not considered this yet” and “the repository has a theoretical concept”.

In cases where the scope was too narrowly focussed on ‘data’, the use of the term ‘digital object’ has been expanded and used, alongside “data and metadata”.

In R0. Context the previous repository typology has been replaced by a free text option and a request to select either ‘specialist’ or ‘generalist’. Specialist repositories are asked to clarify their specialist scope.

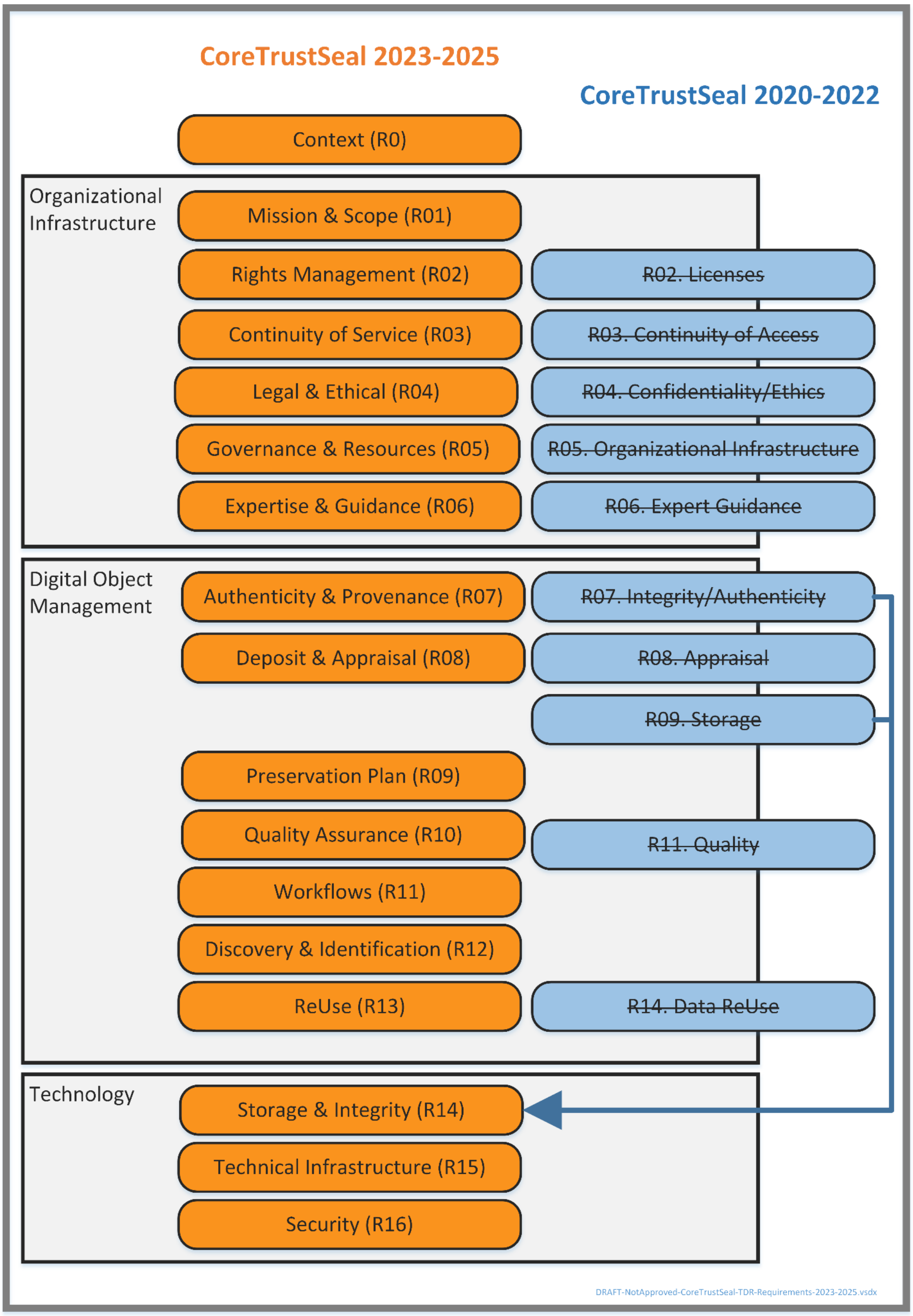
CoreTrustSeal 2023-2025
CoreTrustSeal 2020-2022
Context (R0)
Organizational Infrastructure
Mission & Scope (R01)
Rights Management (R02)
~~R02. Licenses~~
Continuity of Service (R03)
~~R03. Continuity of Access~~
Legal & Ethical (R04)
~~R04. Confidentiality/Ethics~~
Governance & Resources (R05)
~~R05. Organizational Infrastructure~~
Expertise & Guidance (R06)
~~R06. Expert Guidance~~
Digital Object Management
Authenticity & Provenance (R07)
~~R07. Integrity/Authenticity~~
Deposit & Appraisal (R08)
~~R08. Appraisal~~
~~R09. Storage~~
Preservation Plan (R09)
Quality Assurance (R10)
~~R11. Quality~~
Workflows (R11)
Discovery & Identification (R12)
ReUse (R13)
~~R14. Data ReUse~~
Technology
Storage & Integrity (R14)
Technical Infrastructure (R15)
Security (R16)
DRAFT-NotApproved-CoreTrustSeal-TDR-Requirements-2023-2025.vsdx

Diagram: Synopsis of Changes to Short Requirements Text and Structure

Organizational Infrastructure

Mission & Scope (R01)

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

```
Was: 1. Mission/Scope. R1. The repository has an explicit mission to provide access
to and preserve data in its domain.
```

Rights Management (R02)

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

```
Was: 2. Licenses. R2. The repository maintains all applicable licenses covering data
access and use and monitors compliance.
```

Updated to reflect the fact that rights management goes beyond the traditional signing of a license agreement at the point of deposit or access and includes all the measures necessary to manage the permission, prohibitions and obligations of all actors involved in managing data and metadata. Many digital objects have some rights attached even if there is no license artifact as traditionally understood.

Continuity of Service (R03)

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

```
Was: 3. Continuity of access. R3. The repository has a continuity plan to ensure
ongoing access to and preservation of its holdings.
```

This change more accurately reflects the scope of the requirement as covering ongoing services offered by the repository including access but also measures to ensure ongoing preservation. Avoids possible confusion with Access in the sense used by the FAIR Principles.

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.

```
Was: 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.
```

This change highlights that many data protection measures are legally as well as ethically governed. This was already covered in the guidance text but is made more explicit. There is a stronger focus on evidence that demonstrates the applicants understanding of the legal and ethical framework they work within. References to ‘discipline’ have been adjusted to support a wider range of applicants. There is clearer separation of general guidance from that related to digital objects with a disclosure risk.

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.

Was: 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.

This change more accurately reflects the scope of the Requirement. Potential overlap is avoided by adjusting references to qualifications and expertise that are more appropriate to Expertise and Guidance (R06) below.

Expertise & Guidance (R06)

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

Was: 6. Expert guidance. R6. The repository adopts mechanism(s) to secure ongoing expert guidance and feedback (either in-house, or external, including scientific guidance, if relevant).

This requirement will now include any guidance on internal or external expertise previously included under Governance & Resources (R05). The reference to scientific guidance is removed from the long requirement text and included in the guidance.

Digital Object Management

Provenance and authenticity (R07)

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

Was: 7. Data integrity and authenticity

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

This change focusses the requirement on measures to manage planned change. It was clear from previous applications that the topic of integrity was addressed primarily in technical terms. Integrity measures are now addressed alongside storage under Technical and Security, see Storage & Integrity (R14). The Board proposes to retain the R07 focus on authenticity and to address integrity measures alongside storage (see R09) under the Technology subsection of CoreTrustSeal.

Deposit & Appraisal (R08)

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

Was: 8. Appraisal. R8. The repository accepts data and metadata based on defined criteria to ensure relevance and understandability for data users.

This change reflects the focus on the appraisal and assessment of data and metadata at the point they are offered to a repository. Re-appraisal of digital objects over time is included under Preservation Plan (R09)

Preservation plan (R09)

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

Was: 10. Preservation plan. R10. The repository assumes responsibility for long-term preservation and manages this function in a planned and documented way.

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.

Was: 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.

Repository quality assurance is often related to 'standards compliance'. The requirement is intended to demonstrate that the repository provides data and metadata of sufficient 'technical quality'. This should be sufficient to allow users to make assessments about their 'scientific quality'. References to 'expertise' are removed to avoid overlap with Expertise & Guidance (R06)

Workflows (R11)

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

Was: 12. Workflows. R12. Archiving takes place according to defined workflows from ingest to dissemination.

The language of the Requirement has been updated to reflect that most commonly used within the applicant community.

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.

Was: 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.

Reuse (R13)

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

Was: 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.

Information Technology & Security

Storage & Integrity (R14)

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

Was: 9. Documented storage procedures R9. The repository applies documented processes and procedures in managing archival storage of the data.

It was clear from previous applications that the topic of storage was addressed primarily in technical terms. This change moves Storage into the Information Technology and Security sub-section and unites it with integrity (previously included under R07) to cover the avoidance of unintended changes to data and metadata.

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.

Was: 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.

Security (R16)

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

Was: 16. Security. R16. The technical infrastructure of the repository provides for protection of the facility and its data, products, services, and users.