DRAFT: NOT YET APPROVED

[DRAFT] CoreTrustSeal Trustworthy Data Repositories Requirements 2023-2025

Table of Contents

CoreTrustSeal Resources

https://www.coretrustseal.org/apply/

https://www.coretrustseal.org/why-certification/frequently-asked-questions/

CoreTrustSeal Requirements v03.00 2023-2025

> The full normative CoreTrustSeal Requirements and Guidance. Stable for the period 2023-2025.

CoreTrustSeal Extended Guidance v03.00 2023-2025

> The full CoreTrustSeal Requirements text with extended guidance including comments and discussion. May be periodically updated during the period 2023-2025.

CoreTrustSeal Glossary v03.00 2023-2025

> Definitions of key terms used in the CoreTrustSeal Requirements.

Background & General Guidance

The *CoreTrustSeal Requirements* describe the characteristics required to be a trustworthy repository for digital data and metadata. Each Requirement is accompanied by Guidance text describing the response statements and evidence that applicants must provide to enable an objective review. Applicants must respond to all of the Requirements.

Compliance Levels

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.

Compliance levels are an indicator of the applicant's self-assessed progress, but reviewers judge compliance against response statements and supporting evidence.

A reviewer may reduce a compliance level to ‘in progress’ and provide an explanation to the applicant in feedback. All requirements assessed as ‘in progress' must be supported by a statement from the applicant about the actions and timescales planned to reach ‘implemented’. A reviewer will not increase a self-assessed ‘in progress’ compliance level to ‘implemented’. Certification may be granted if some requirements are ‘in progress’. When CoreTrustSeal is renewed, reviewers will expect to see a move from 'in progress' to 'implemented' or clear explanations as to why this is not possible.

Supporting Evidence Links and Missing Information/Evidence

Response statements provided by applicants must be supported by links to public evidence online. Final versions of successful applications are public documents. This level of transparency is important, as the certification process does not include a site visit by an auditor. Links should be verified immediately before submitting applications.

Those reading applications (Reviewers, and eventually the public) should be able to understand the response statements without detailed reading of linked evidence. When longer documents are presented as evidence, or the same evidence is used to support more than one Requirement, the applicant must refer specifically to which sections are relevant and quote/summarise the information in their response.

Internal Information, Sensitive Information & Confidentiality

No sensitive information disclosure is required to acquire CoreTrustSeal. If evidence cannot be made public it is possible to share this confidentially during the certification process.

CoreTrustSeal certification does not require supporting evidence to be made public that is confidential, commercially sensitive, or poses a security risk. Applicants may have internal business information that contains both sensitive information *and* relevant evidence for the CoreTrustSeal. Such evidence can be submitted confidentially to the reviewers[1] and the documents named and described in the application. Over time, applicants should separate relevant evidence from confidential materials, and assure a public version is made available for the next review.

If documentation does not yet exist, is in progress, or is currently for internal use only, then a date of public availability should be stated in the application. Certification may be approved based on these assurances. Applicants are expected to provide the public documentation when they renew their certification.

Use of English, and non-English Language Documentation

All responses must be in English. If links to non-English evidence are provided, then an English summary must be included in the response statement. This summary can be brief for certain types of documents (e.g. a reference to a list of preferred formats), but should be longer for others (e.g. a Preservation Policy document).

Full English translations of linked evidence are not required.

Certification Validity & Renewal

CoreTrustSeal certification is valid for three years from the date of certification. An organisation with well-managed business processes and records should be able to reapply with minimal revisions. More significant revisions may be required if:

- the organisation, its data collection, technical infrastructure or Designated Community changes significantly
- the CoreTrustSeal Requirements are updated in ways that impact the applicant

The CoreTrustSeal Requirements are subject to review and revision every three years. This does not affect a successful applicant until they seek renewal.

[1] Contact the CoreTrustSeal Secretariat via info@coretrustseal.org

Application structure and length

It is not possible to cover every possible repository scenario in the Guidance or Extended Guidance and some guidance or questions may not be locally applicable. Applicant responses should refer to the issues raised in the Guidance text and provide responses based on their local context. Final evaluation of a Requirement depends on the completeness and quality of the response. Reviewers are looking for clear, open statements of evidence specific to the applicant. It is understood that the length of response statements will vary, but the overall application should provide a focussed narrative describing the supporting evidence.

Requirements

R0. Background Information & Context

This section provides the information necessary for reviewers to fully assess the applicants response statements. It is important to the entire application that the correct options are selected and that sufficiently detailed responses are provided.

***(1) Re3data Identifier*[2]. I**

Response

***(2) Repository type*.** lSelect a repository type:

- **Generalist repository**
- **Specialist repository**
    - Specialist repositories are asked to provide their domain(s) and/or discipline(s).

Response

(3) Overview. Provide a short overview of key characteristics of the repository, reflecting the repository type selected. This should include information about the scope and size of data collections, data types and formats. Further contextual information may also be added.

Response

(4) Designated Community. A clear definition of the Designated Community demonstrates that the applicant understands the scope, knowledge base, and methodologies—including preferred software/formats—of the group(s) of users at whom the curation and preservation measures are primarily targeted. The definition should be specific so that reviewers can assess whether that community is being served in the responses to other requirements.

Response

[2] https://www.re3data.org/

(5) Levels of Curation.

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 during ingest, enhancement of documentation and metadata

D. Data-level curation – as in C above, but with additional editing of deposited data

Response

Guidance

A repository must demonstrate that it assures long-term accessibility and understandability of data as the needs of the Designated Community change. This is less likely to be possible at curation levels A or B, because without normalising submitted file formats to a common preservation format, it may be difficult to perform format migrations in the future depending on the heterogeneity of the collection. Similarly, lack of rich metadata and documentation may pose a risk concerning the continued usability of the data.

It is recognised that a repository may offer different levels of curation to different digital objects. It is important that this is clear to depositors, users, and to CoreTrustSeal Reviewers.

More than one option (A, B, C, or D) of the level (or extent) of curation can be selected, depending on the type of data and curation terms agreed with the depositor. For each level selected add some concise information on how the respective levels are reached e.g. automatic checks of metadata, intellectual checks and editing of documentation, file format identification, transformation to preservation file formats, etc..

When a repository performs curation at more than one level, further information should be added on the proportion of the data in the collection curated to the respective levels. In this case, applicants should take care that responses to the Requirements state any relevant differences in workflows or employed measures for each selected curation level.

All levels of curation assume (1) initial deposits are retained unchanged and that edits are only made on copies of those originals, (2) metadata that enables the Designated Community to understand and use the data independently (i.e., without having to consult the original creator) is present at deposit or added by the repository, and (3) ongoing measures for active preservation are in place for the greater part of the collection(s).

Annotations/edits must fall within the terms of the license agreed with the data depositor and be clearly within the skillset of those undertaking the curation. Thus, the repository will be expected to demonstrate that any such annotations/edits are undertaken and documented by appropriate experts and that the integrity of all original copies is maintained.

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

Response

Guidance

If the applicant is entirely responsible for all decisions and takes all relevant actions related to meeting each of the 16 Requirements then this section can be left blank. If for one or more requirements the applicant is supported by another organization in making decisions or taking actions, that organisation, the role it plays, and its relationship with the applicant should be listed here.

It is understood that repositories may be structured in different ways. It is important that repository certification is associated with a clearly defined organisation. The structure of the applicant organisation is addressed under Governance & Resources (R05).

If a repository function and/or supporting evidence that is covered by the CoreTrustSeal is not under the direct control of the applicant, then the relevant host organisation, partner or other third party should be listed here. Describe the function or service they provide, the nature of the relationship or agreement (contractual, Service Level Agreement, Memorandum of Understanding, etc.) and whether they have any relevant certifications. Appropriate qualifications or certifications, including but not limited to the CoreTrustSeal, are preferred but not required. Explaining what types of agreement are in place, or why these may not be practical, helps ensure transparency. It is not expected that applicants share commercial or otherwise sensitive details of relationships (see: Internal Information, Sensitive Information & Confidentiality).

Such relationships may include, but are not limited to: cooperation or federation with other repositories, any services provided by an institution the applicant is part of, storage provided by others as part of multi-copy redundancy, or organisations that may undertake some responsibility for data, metadata and services in a service continuity or succession situation.

The listed organisations should then be clearly referenced under each relevant Requirement.

Because outsourced functions will usually still have some level of shared responsibility the applicant must provide appropriate evidence for Requirements that are not outsourced, and for the parts of the data lifecycle that they control.

Though a wide range of services and functions may be outsourced, a CoreTrustSeal 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.

This can be a complex area to define and describe, but such details are essential to ensure a comprehensive review process.

(7) Applicants renewing their CoreTrustSeal certification: summary of significant changes since last application. CoreTrustSeal certification has an expectation of continuous improvement over time. Repositories undergoing recertification should highlight briefly any significant changes including to technical systems, Designated Community or funding during the previous three years. This could include any steps taken to move from 'In Progress' to 'Implemented' Requirements since the last certification.

Response

Organisational Infrastructure

Mission & Scope (R01)

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

Self-Assessed Compliance Level:

Response

Guidance

Repositories take responsibility for the curation of digital objects, and for ensuring that materials are held in the appropriate environment for appropriate periods of time. 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.

The response statement and evidence should include references to the following items:

- The mission to actively preserve and provide access to digital objects
- The level of approval that the mission has received.

Evidence for this Requirement could include an approved public mission statement, roles mandated by funders, or a policy statement signed off by a governing board.

Rights Management (R02)

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

Self-Assessed Compliance Level:

Response

Guidance

The repository manages, and communicates to relevant stakeholders, all rights (permissions, prohibitions, obligations) covering data and metadata deposit, storage, preservation, access, and use.

This requirement relates to the system, methods and artefacts (e.g. licenses, agreements, terms and conditions, and related policies and procedures) in place for rights management.

The repository must obtain all necessary rights from the depositor, and demonstrate that there are sufficient controls in place to ensure they are applied and monitored.

The response statement and evidence should include references to the following items:

- The overall rights management approach to deposited files, data and metadata.
- The rights to copy, transform, and store digital objects for preservation, as well as provide access to them
- Conditions of use (e.g. intellectual property rights, distribution, intended use, protection of sensitive data, etc.).
- Deposit and access agreements or licenses.
- How rights metadata is managed for humans (e.g. license documents/files) or machines.
- Monitoring of compliance at deposit, during curation/preservation, and during access and reuse. Describe any circumstances where compliance monitoring is not possible.
- Measures in place if non-compliance is detected.

Data and metadata, including ‘open data’, will usually have some rights attached even if there is no signed license artefact or formal agreement in place. This could include obligations such as citation and attribution of data and metadata used, or making secondary analysis openly available. If all data and metadata are made available without any conditions of access or use then this should be made clear in the response statement.

Rights negotiations and transfer should be described under Deposit & Appraisal (R08). Any ethical codes of conduct, privacy measures, or legislation that influence rights management should be described under Legal & Ethical (R04).

Continuity of Service (R03)

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

Self-Assessed Compliance Level:

Response

Guidance

The repository must have measures in place to address the risks inherent in changing circumstances, including in mission and/or scope. This Requirement covers the stable management of repository services over time (business continuity) and the response when services have problems (disaster recovery). It also includes preparations for handover of digital objects and services to another repository (succession planning). The deposit, storage, preservation, and access services offered by the repository to depositors and users are all in scope.

The response statement and evidence should include references to the following items:

- The functions and services offered by the repository to depositors and users.
- The approach to rapid changes of circumstance and long-term planning.

- The options for relocation or transition of the activity to another repository. For example, the case of cessation of funding due to an unexpected withdrawal of funding, or a shift of host institution interests.
- The repository approach to managing policies, procedures and other business information over time.

Even though succession agreements may be hard to achieve it is important to acknowledge the possibility that a repository will cease to function or exist. If there is no formal, written agreement between the repository and a successor then the compliance level cannot be higher than “In Progress: the repository is in the implementation phase”.

Any technical aspects of business continuity, and disaster and succession planning should be covered in R15 (Technical 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.

Self-Assessed Compliance Level:

Response

Guidance

This requirement relates to repository awareness and processes around legal and ethical issues, including privacy and confidentiality, that impact the creation, curation, and use of digital objects.

To maintain the trust of those who agree to have their digital objects held by the repository, evidence should demonstrate practices that reflect the legal status and sensitivity of digital objects, including guidance for depositors and users.

The response statement and evidence should include references to the following items:

- How the repository identifies and manages relevant legal and ethical standards that impact operations.
- Compliance with specific legal and/or ethical discipline or domain standards.
- Information requested from depositors to confirm that data collection or creation was carried out in accordance with legal and ethical criteria in the relevant geographical location or discipline (e.g. Ethical Review Committee/Institutional Review Board or Data Protection legislation).
- Any data or metadata with disclosure risk e.g. depositor/user information, personal, cultural, or environmental information

For applicants that hold data or metadata with disclosure risk include references to the following items:

- 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.

The management of related rights and compliance checks should be covered under Rights (R02). Measures to protect digital objects should be addressed under Security (R16).

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.

Self-Assessed Compliance Level:

Response

Guidance

This Requirement reflects a need for transparency of financing, governance, responsibilities, and decision making. Evidence should demonstrate that the repository has a clear system of governance and sufficient human and financial resources to carry out its mission.

The response statement and evidence should include references to the following items:

- Descriptions and diagrams of governance bodies, groups and hierarchies.
- Timescales for provision and renewal of funding for operational costs and recruitment; it is understood that permanent, ongoing funding cannot be perfectly quantified or guaranteed.
- 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.

The availability of appropriate expertise is covered under Expertise (R06) below.

Expertise & Guidance (R06)

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

Self-Assessed Compliance Level:

Response

Guidance

A repository must identify the skills necessary to deliver the services it offers, and source and maintain those skills either as internal resources or through external engagement. An effective repository strives to accommodate evolutions in data types, data volumes, and data rates, as well as to adopt the most effective new technologies in order to remain valuable to its Designated Community.

The response statement and evidence should include references to the following items:

- That guidance and expertise reflects the scientific scope of the repository, if relevant.
- 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, including any relevant affiliations (e.g. national or international bodies), is appropriate to the mission.
- In-house advisers, or external advisory committees that include technical, curation, data science, data security, and disciplinary experts
- How the repository communicates with experts for advice
-

Digital Object Management

Provenance and authenticity (R07)

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

Self-Assessed Compliance Level:

Response

Guidance

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.

The response statement and evidence should include references to the following items:

- 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.

Deposit & Appraisal (R08)

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

Self-Assessed Compliance Level:

Response

Guidance

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.

The response statement and evidence should include references to the following items:

- Any documented deposit process that includes steps to ensure that data and metadata are sufficient for long-term preservation.
- A collection development policy 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.
- 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.

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.

Preservation plan (R09)

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

Self-Assessed Compliance Level:

Response

Guidance

The repository, depositors, and Designated Community need to understand the level of responsibility undertaken for the long-term preservation of data and metadata. Procedures must be documented and their completion assured.

The response statement and evidence should include references to the following items:

- 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.
- 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.

The rights of the repository, including the right to preserve, are covered under Rights Management (R02). Bit level integrity is covered under Storage and Integrity (R14) and is not considered sufficient for preservation. Acceptable file formats at deposit should be covered under Deposit and Appraisal (R08). Measures to ensure that file formats, schemas and content are appropriate to the Designated Community should be covered under Reuse (R13).

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.

Self-Assessed Compliance Level:

Response

Guidance

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.

The response statement and evidence should include references to the following items:

- 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.
- 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.

This Requirement refers to data and metadata quality standards and assurance during curation. Selection criteria are covered during Deposit and Appraisal (R8). Measures to ensure that digital objects remain fit for purpose over time are covered under Preservation Plan (R09).

Workflows (R11)

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

Self-Assessed Compliance Level:

Response

Guidance

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.

The response statement and evidence should include references to the following items:

- 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.

This Requirement confirms that all workflows are documented. 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).

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.

Self-Assessed Compliance Level:

Response

Guidance

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.

The response statement and evidence should include references to the following items:

- 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.

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.

Reuse (R13)

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

Self-Assessed Compliance Level:

Response

Guidance

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. This Requirement evaluates the measures taken to ensure that data and metadata are reusable.

The response statement and evidence should include references to the following items:

- 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.

Responses to this Requirement should focus on engagement with the Designated Community, identification of their needs and specifying how their needs are met.

Information Technology & Security

Storage & Integrity (R14)

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

Self-Assessed Compliance Level:

Response

Guidance

In addition to maintaining 'archival' copies of digital objects, repositories need to store data and metadata from the point of deposit, during curation and preservation, and for access by users. For each storage location, measures should be in place to ensure that unintentional or unauthorised changes can be detected and correct versions of data and metadata recovered.

The response statement and evidence should include references to the following items:

- Processes and documents to ensure that the repository staff have a clear understanding of all storage locations and how they are managed.
- The repository's strategy for multiple copies.
- The risk management techniques used to inform the strategy.
- Procedures for handling and monitoring deterioration of storage media.
- Procedures to ensure that data and metadata are only deleted as part of an approved and documented process.

- Any checks (i.e. fixity checks) used to verify that a digital object has not been altered or corrupted from deposit to use.

Storage and integrity measures should be covered here (R14) and not as part of Technical Infrastructure (R15) or Security (R16) responses. Details of how intentional changes to the data and metadata are logged should be covered under Provenance & Authenticity (R07).

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.

Self-Assessed Compliance Level:

Response

Guidance

Repositories must operate on reliable and stable core infrastructure that maximises service availability. The details of technical infrastructure will vary widely across repositories. Responses and evidence should focus on demonstrating that the repository solution, including hardware and software is well managed and appropriate to the needs of the repository functions and the Designated Community of users.

The response statement and evidence should include references to the following items:

- The repository software used for deposit, curation, preservation and access management. Whether it is community supported, open source, or locally developed.
- Any IT service management approach followed and the functions this approach specifies (e.g. systems documentation, software inventories, code repositories, infrastructure development planning).
- Any international, community or other technical infrastructure standards in place and how compliance is monitored.
- The version control systems used for repository generated software
- Measures taken to ensure that availability, bandwidth, and connectivity are sufficient to meet the needs of the Designated Community.
- Processes in place to monitor and manage the need for technical change, including in response to the changing needs of Preservation (R10), and Reuse (R13) by the Designated Community.

Technical aspects of business continuity, disaster recovery and succession planning are relevant here, but their management should be covered under Continuity of Service (R03). This requirement excludes Security (R16) measures and Storage & Integrity (R14).

File formats and metadata schema information should be referenced under Deposit & Appraisal (R08) and Reuse (R13). Standards that are not technical or security focussed should be referenced under Quality Assurance (R10).

Security (R16)

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

Self-Assessed Compliance Level:

Response

Guidance

The repository should analyze potential threats, assess risks, and create a consistent security system. It should consider damage scenarios based on malicious actions, human error, or technical failure that pose a threat to the repository and its data, metadata, products, services, and users. It should measure the likelihood and impact of such scenarios, decide which risk levels are acceptable, and determine which measures should be taken to counter the threats to the repository and its Designated Community. This should be an ongoing process.

The response statement and evidence should include references to the following items:

- The levels of security required for different data and metadata and environments, and how these are supported.
- The IT security system, employees with roles related to security (e.g. security officers), and any risk analysis approach in use.
- Measures in place to protect the facility. How the premises where digital objects are held secured
- Any security-specific standards the repository references or complies with
- Any authentication and authorization procedures employed to securely manage access to systems in use.

Responses should not cover Storage and Integrity (R14) measures or the wider Technical Infrastructure (R15).

Applicant Feedback

We welcome feedback on the CoreTrustSeal Requirements and the Certification procedure.

Response