Relationship between OAIS, ISO 16363, CTS, FAIR and TRUST

# Introduction

This concept paper is an attempt to clarify the relationship between the concepts of OAIS[[1]](#footnote-2) and ISO 16363[[2]](#footnote-3), compared to CoreTrustSeal[[3]](#footnote-4), FAIR principles[[4]](#footnote-5) and TRUST principles[[5]](#footnote-6). It assumes familiarity with OAIS and ISO 16363. OAIS and ISO 16363 do not prescribe things related to domain specific customs or implementations.

# OAIS and ISO 16363,

OAIS and ISO 16363 focus on the ability to preserve, in the sense defined in OAIS, digitally encoded information. Preservation is defined in terms of usability/understandability over time therefore the OAIS Information Model is of central importance. Representation Information is a key part of the Information Model concerned with understandability. To be more specific about how much Representation Information is needed, OAIS requires the repository to define a Designated Community. OAIS conformance is defined in terms of the Information Model and the Mandatory Responsibilities.

Some important points to remember are:

* OAIS can apply whether or not what is being preserved is junk from some points of view;
* OAIS applies whether or not the repository is open access (i.e. free of cost or other access barriers);
* a specific taxonomy for “metadata” is defined in order to be able to discuss which specific types of metadata, and how much of each, is needed for preservation;
* OAIS defines preservation in a way which allows one test whether preservation is being carried out properly.
* OAIS specifies how a Designated Community is defined and what its role is.

# CoreTrustSeal

The 16 CoreTrustSeal requirements are much more general.

|  |  |
| --- | --- |
| **CTS Requirement** | **Relationship to OAIS/ISO 16363** |
| R1. The repository has an explicit mission to provide access to and preserve data in its domain. | ISO 16363  3.1.1**. THE REPOSITORY SHALL HAVE A STATEMENT THAT REFLECTS A COMMITMENT TO THE PRESERVATION OF, LONG TERM RETENTION OF, MANAGEMENT OF, AND ACCESS TO DIGITAL INFORMATION** |
| R2. The repository maintains all applicable licenses covering data access and use and monitors compliance. | OAIS:  AIP must have Access Rights Information: The information that identifies the access restrictions pertaining to the Content Data Object, including the legal framework, licensing terms, and access control. It contains the access and distribution conditions stated within the Submission Agreement, related to both preservation (by the OAIS) and final usage (by the Consumer). It also includes the specifications for the application of rights enforcement measures.  ISO 16363  3.4.3 THE REPOSITORY SHALL HAVE AN ONGOING COMMITMENT TO ANALYZE AND REPORT ON RISK, BENEFIT, INVESTMENT, AND EXPENDITURE (INCLUDING ASSETS, LICENSES, AND LIABILITIES).  3.5.1 The repository shall have and maintain appropriate contracts or deposit agreements for digital materials that it manages, preserves, and/or to which it provides access.  3.5.2 The repository shall track and manage intellectual property rights and restrictions on use of repository content as required by deposit agreement, contract, or |
| R3. The repository has a continuity plan to ensure ongoing access to and preservation of its holdings. | ISO 16363  3.1.2.1 The repository shall have an appropriate, formal succession plan, contingency plans, and/or escrow arrangements in place in case the repository ceases to operate or the governing or funding institution substantially changes its scope. |
| R4. The repository ensures, to the extent possible, that data are created, curated, accessed, and used in compliance with disciplinary and ethical norms. |  |
| 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. | ISO 16363  3.1 GOVERNANCE AND ORGANIZATIONAL VIABILITY  3.2.1 THE REPOSITORY SHALL HAVE IDENTIFIED AND ESTABLISHED THE DUTIES THAT IT NEEDS TO PERFORM AND SHALL HAVE APPOINTED STAFF WITH ADEQUATE SKILLS AND EXPERIENCE TO FULFIL THESE DUTIES.  3.2.1.3 The repository shall have in place an active professional development program that provides staff with skills and expertise development opportunities.  . |
| R6. The repository adopts mechanism(s) to secure ongoing expert guidance and feedback (either in-house, or external, including scientific guidance, if relevant). |  |
| R7. The repository guarantees the integrity and authenticity of the data. | ISO 16363  3.3.5 THE REPOSITORY SHALL DEFINE, COLLECT, TRACK, AND APPROPRIATELY PROVIDE ITS INFORMATION INTEGRITY MEASUREMENTS.  4.2.9 THE REPOSITORY SHALL PROVIDE AN INDEPENDENT MECHANISM FOR VERIFYING THE INTEGRITY OF THE REPOSITORY COLLECTION/CONTENT. |
| R8. The repository accepts data and metadata based on defined criteria to ensure relevance and understandability for data users. | ISO 16363  3.1.3 The repository shall have a Collection Policy or other document that specifies the type of information it will preserve, retain, manage, and provide access to.  4.2.5 THE REPOSITORY SHALL HAVE ACCESS TO NECESSARY TOOLS AND RESOURCES TO PROVIDE AUTHORITATIVE REPRESENTATION INFORMATION FOR ALL OF THE DIGITAL OBJECTS IT CONTAINS.  4.2.5.2 The repository shall have tools or methods to determine what Representation Information is necessary to make each Data Object understandable, as exemplified by the associated Preservation Objectives, to the Designated Community. |
| R9. The repository applies documented processes and procedures in managing archival storage of the data. | ISO 16363  4.4.2 THE REPOSITORY SHALL HAVE CONTEMPORANEOUS RECORDS OF ACTIONS AND ADMINISTRATION PROCESSES THAT ARE RELEVANT TO STORAGE AND PRESERVATION OF THE AIPS. |
| R10. The repository assumes responsibility for long-term preservation and manages this function in a planned and documented way. | ISO 16363  OAIS  – Negotiate for and accept appropriate information from information Producers.  – Obtain sufficient control of the information provided to the level needed to ensure Long Term Preservation.  3.5.1.3 The repository shall have written policies that indicate when it accepts preservation responsibility for contents of each set of submitted data objects |
| 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. | OAIS:  – Make the preserved information available to the Designated Community and enable the information to be disseminated as copies of, or as traceable to, the original submitted Content Information with evidence supporting its Authenticity.  ISO 16363  3.2.1.2 The repository shall have the appropriate number of staff to support all functions and services.  3.2.1.3 The repository shall have in place an active professional development program that provides staff with skills and expertise development opportunities.  4.2.5 The repository shall have access to necessary tools and resources to provide authoritative Representation Information for all of the digital objects it contains.  In particular the following aspects must be checked.  4.2.5.1 The repository shall have tools or methods to identify the file type of all submitted Data Objects.  4.2.5.2 The repository shall have tools or methods to determine what Representation Information is necessary to make each Data Object understandable, as exemplified by the associated Preservation Objectives, to the Designated Community.  4.2.5.3 The repository shall have access to the requisite Representation Information. |
| R12. Archiving takes place according to defined workflows from ingest to dissemination. | OAIS and ISO 16363  4.1.2 THE REPOSITORY SHALL CLEARLY SPECIFY THE INFORMATION THAT NEEDS TO BE ASSOCIATED WITH SPECIFIC CONTENT INFORMATION AT THE TIME OF ITS DEPOSIT.  4.1.3 THE REPOSITORY SHALL HAVE ADEQUATE SPECIFICATIONS ENABLING RECOGNITION AND PARSING OF THE SIPS.  4.1.4 THE REPOSITORY SHALL HAVE MECHANISMS TO APPROPRIATELY VERIFY THE DEPOSITOR OF ALL MATERIALS.  4.1.5 THE REPOSITORY SHALL HAVE AN INGEST PROCESS WHICH VERIFIES EACH SIP FOR COMPLETENESS AND CORRECTNESS.  4.1.6 THE REPOSITORY SHALL OBTAIN SUFFICIENT CONTROL OVER THE DIGITAL OBJECTS TO PRESERVE THEM.  4.1.7 THE REPOSITORY SHALL PROVIDE THE PRODUCER/DEPOSITOR WITH APPROPRIATE RESPONSES AT AGREED POINTS DURING THE INGEST PROCESSES.  4.1.8 THE REPOSITORY SHALL HAVE CONTEMPORANEOUS RECORDS OF ACTIONS AND ADMINISTRATION PROCESSES THAT ARE RELEVANT TO CONTENT ACQUISITION.  4.6.1 THE REPOSITORY SHALL COMPLY WITH ACCESS POLICIES.  4.6.1.1 The repository shall log and review all access management failures and anomalies.  4.6.2 THE REPOSITORY SHALL FOLLOW POLICIES AND PROCEDURES THAT ENABLE THE DISSEMINATION OF DIGITAL OBJECTS THAT ARE TRACEABLE TO THE ORIGINALS, WITH EVIDENCE SUPPORTING THEIR AUTHENTICITY.  4.6.2.1 The repository shall record and act upon problem reports about errors in data or responses from users. |
| R13. The repository enables users to discover the data and refer to them in a persistent way through proper citation. | ISO 16363  4.2.4 THE REPOSITORY SHALL HAVE AND USE A CONVENTION THAT GENERATES PERSISTENT, UNIQUE IDENTIFIERS FOR ALL AIPS  4.2.4.1 The repository shall uniquely identify each AIP within the repository.  4.2.4.1.1 The repository shall have unique identifiers.  4.2.4.1.2 The repository shall assign and maintain persistent identifiers of the AIP and its components so as to be unique within the context of the repository.  4.2.4.1.3 Documentation shall describe any processes used for changes to such identifiers.  4.2.4.1.4 The repository shall be able to provide a complete list of all such identifiers and do spot checks for duplications.  4.2.4.1.5 The system of identifiers shall be adequate to fit the repository’s current and foreseeable future requirements such as numbers of objects.  4.2.4.2 The repository shall have a system of reliable linking/resolution services in order to find the uniquely identified object, regardless of its physical location.  4.5.2 THE REPOSITORY SHALL CAPTURE OR CREATE MINIMUM DESCRIPTIVE INFORMATION AND ENSURE THAT IT IS ASSOCIATED WITH THE AIP.  4.5.3 THE REPOSITORY SHALL MAINTAIN BI-DIRECTIONAL LINKAGE BETWEEN EACH AIP AND ITS DESCRIPTIVE INFORMATION.  4.5.3.1 The repository shall maintain the associations between its AIPs and their descriptive information over time. |
| 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. | OAIS and ISO 16363 with specific reference to the Designated Community  4.2.5 THE REPOSITORY SHALL HAVE ACCESS TO NECESSARY TOOLS AND RESOURCES TO PROVIDE AUTHORITATIVE REPRESENTATION INFORMATION FOR ALL OF THE DIGITAL OBJECTS IT CONTAINS.  4.2.5.1 The repository shall have tools or methods to identify the file type of all submitted Data Objects.  4.2.5.2 The repository shall have tools or methods to determine what Representation Information is necessary to make each Data Object understandable to the Designated Community.  4.2.5.3 The repository shall have access to the requisite Representation Information.  4.2.5.4 The repository shall have tools or methods to ensure that the requisite Representation Information is persistently associated with the relevant Data Objects. |
| 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. | ISO 16363  5.1.1.1.1 The repository shall have hardware technologies appropriate to the services it provides to its designated communities.  5.1.1.1.2 The repository shall have procedures in place to monitor and receive notifications when hardware technology changes are needed.  5.1.1.1.3 The repository shall have procedures in place to evaluate when changes are needed to current hardware.  5.1.1.1.4 The repository shall have procedures, commitment and funding to replace hardware when evaluation indicates the need to do so.  5.1.1.1.5 The repository shall have software technologies appropriate to the services it provides to its designated communities. |
| R16. The technical infrastructure of the repository provides for protection of the facility and its data, products, services, and users. | ISO 16363  5.1.1 THE REPOSITORY SHALL IDENTIFY AND MANAGE THE RISKS TO ITS PRESERVATION OPERATIONS AND GOALS ASSOCIATED WITH SYSTEM INFRASTRUCTURE.  5.1.1.1 The repository shall employ technology watches or other technology monitoring notification systems.  5.1.1.1.1 The repository shall have hardware technologies appropriate to the services it provides to its designated communities.  5.1.1.1.2 The repository shall have procedures in place to monitor and receive notifications when hardware technology changes are needed.  5.1.1.1.3 The repository shall have procedures in place to evaluate when changes are needed to current hardware.  5.1.1.1.4 The repository shall have procedures, commitment and funding to replace hardware when evaluation indicates the need to do so.  5.1.1.1.5 The repository shall have software technologies appropriate to the services it provides to its designated communities.  5.1.1.1.6 The repository shall have procedures in place to monitor and receive notifications when software changes are needed.  5.1.1.1.7 The repository shall have procedures in place to evaluate when changes are needed to current software.  5.1.1.1.8 The repository shall have procedures, commitment and funding to replace software when evaluation indicates the need to do so.  5.1.1.2 The repository shall have adequate hardware and software support for backup functionality sufficient for preserving the repository content and tracking repository functions.  5.1.1.3 The repository shall have effective mechanisms to detect bit corruption or loss.  5.1.1.3.1 The repository shall record and report to its administration all incidents of data corruption or loss, and steps shall be taken to repair/replace corrupt or lost data.  5.1.1.4 The repository shall have a process to record and react to the availability of new security updates based on a risk-benefit assessment.  5.1.1.5 The repository shall have defined processes for storage media and/or hardware change (e.g., refreshing, migration).  5.1.1.6 The repository shall have identified and documented critical processes that affect its ability to comply with its mandatory responsibilities.  5.1.1.6.1 The repository shall have a documented change management process that identifies changes to critical processes that potentially affect the repository's ability to comply with its mandatory responsibilities.  5.1.1.6.2 The repository shall have a process for testing and evaluating the effect of changes to the repository's critical processes. |

# FAIR

|  |  |
| --- | --- |
|  | OAIS/ISO 16363 |
| To be Findable: |  |
| F1. (meta)data are assigned a globally unique and persistent identifier | ISO 16363  Note these identifiers are unique within the repository but not necessarily globally unique.  4.2.4 THE REPOSITORY SHALL HAVE AND USE A CONVENTION THAT GENERATES PERSISTENT, UNIQUE IDENTIFIERS FOR ALL AIPS  4.2.4.1 The repository shall uniquely identify each AIP within the repository.  4.2.4.1.1 The repository shall have unique identifiers.  4.2.4.1.2 The repository shall assign and maintain persistent identifiers of the AIP and its components so as to be unique within the context of the repository.  4.2.4.1.3 Documentation shall describe any processes used for changes to such identifiers.  4.2.4.1.4 The repository shall be able to provide a complete list of all such identifiers and do spot checks for duplications.  4.2.4.1.5 The system of identifiers shall be adequate to fit the repository’s current and foreseeable future requirements such as numbers of objects.  4.2.4.2 The repository shall have a system of reliable linking/resolution services in order to find the uniquely identified object, regardless of its physical location. |
| F2. data are described with rich metadata (defined by R1 below) | OAIS:  Section 4.3 Information Model |
| F3. metadata clearly and explicitly include the identifier of the data it describes | This is possible in terms of “metadata” related to finding relevant data (see above - Package Description, Provenance Information, Context Information).  However OAIS does not require a bi-directional link between data and “metadata” in general. The link from data to “metadata” is required. However, the link from metadata to data is impractical in general for example where “metadata” applies to billions of, possibly remote, data objects. |
| F4. (meta)data are registered or indexed in a searchable resource | See above. |
| To be Accessible: | OAIS has only a small amount to say about accessibility, except where it is consistent with the Access Rights Information, and with the requirement that a member of the Designated Community can get the information needed to be able to make a judgement about Authenticity. FAIR does not mention either of these concerns. |
| A1. (meta)data are retrievable by their identifier using a standardized communications protocol | This is implicit in OAIS and ISO 16363 where the “metadata” is itself being preserved. |
| A1.1 the protocol is open, free, and universally implementable |  |
| A1.2 the protocol allows for an authentication and authorization procedure, where necessary |  |
| A2. metadata are accessible, even when the data are no longer available |  |
| To be Interoperable: |  |
| I1. (meta)data use a formal, accessible, shared, and broadly applicable language for knowledge representation. | OAIS provides more detailed requirements for Representation Information for understandability by the Designated Community  But there are no restrictions in OAIS/ISO 16363. |
| I2. (meta)data use vocabularies that follow FAIR principles | Interoperability requires more than vocabularies. |
| I3. (meta)data include qualified references to other (meta)data | This may be the same as Representation Information Network. |
| To be Reusable: |  |
| R1. meta(data) are richly described with a plurality of accurate and relevant attributes | OAIS provides more detailed requirements for Representation Information and, to a lesser extent for Provenance Information. Fixity Information, Reference Information and Access Rights Information. |
| R1.1. (meta)data are released with a clear and accessible data usage license | 3.5.2 THE REPOSITORY SHALL TRACK AND MANAGE INTELLECTUAL PROPERTY RIGHTS AND RESTRICTIONS ON USE OF REPOSITORY CONTENT AS REQUIRED BY DEPOSIT AGREEMENT, CONTRACT, OR LICENSE.  For “metadata” also is implicit in OAIS and ISO 16363 where the “metadata” is itself being preserved. |
| R1.2. (meta)data are associated with detailed provenance | Data needs Provenance Information.  For “metadata” this is the case in OAIS and ISO 16363 where the “metadata” is itself being preserved, because “metadata” is Information.. |
| R1.3. (meta)data meet domain-relevant community standards | No restriction in OAIS/ISO 16363 on which standards to use. In any case standards will change over time.. |

# TRUST Principles

|  |  |
| --- | --- |
| TRUST principles | OAIS/ISO 16363 |
| **Transparency** |  |
| In order to select the most appropriate repository for a particular use case, all potential users benefit from being able to easily find and access information on the scope, target user community, policies, and capabilities of the data repository. Transparency in these areas offers an opportunity to learn about the repository and consider its suitability for users’ specific requirements, including data deposition, data preservation, and data discovery. |  |
| To be compliant with this principle, repositories should ensure that, at a minimum, the mission statement and scope of the repository are clearly stated. | ISO 16363  3.1.1 THE REPOSITORY SHALL HAVE A STATEMENT THAT REFLECTS A COMMITMENT TO THE PRESERVATION OF, LONG TERM RETENTION OF, MANAGEMENT OF, AND ACCESS TO DIGITAL INFORMATION.  3.1.2 THE REPOSITORY SHALL HAVE A PRESERVATION STRATEGIC PLAN THAT DEFINES THE APPROACH THE REPOSITORY WILL TAKE IN THE LONG-TERM SUPPORT OF ITS MISSION |
| In addition, the following aspects should be transparently declared: |  |
| Terms of use, both for the repository and for the data holdings. | ISO 16363  3.5.2 THE REPOSITORY SHALL TRACK AND MANAGE INTELLECTUAL PROPERTY RIGHTS AND RESTRICTIONS ON USE OF REPOSITORY CONTENT AS REQUIRED BY DEPOSIT AGREEMENT, CONTRACT, OR LICENSE. |
| Minimum digital preservation timeframe for the data holdings. | OAIS  No requirement to specify minimum timeframe in OAIS |
| Any pertinent additional features or services, for example the capacity to responsibly steward sensitive data. | OAIS  Unspecified in OAIS other than to say that the archive may offer other services.  ISO 16363  3.5.2 THE REPOSITORY SHALL TRACK AND MANAGE INTELLECTUAL PROPERTY RIGHTS AND RESTRICTIONS ON USE OF REPOSITORY CONTENT AS REQUIRED BY DEPOSIT AGREEMENT, CONTRACT, OR LICENSE. |
| Clearly communicating repository policies and, in particular, the terms of use for data holdings, informs users about any limitations that may restrict their use of the data or the repository. Likewise, being able to easily assess whether a repository can handle sensitive data in a responsible manner would also inform their decision on whether to utilize the available data services. | ISO 16363  3.5.2 THE REPOSITORY SHALL TRACK AND MANAGE INTELLECTUAL PROPERTY RIGHTS AND RESTRICTIONS ON USE OF REPOSITORY CONTENT AS REQUIRED BY DEPOSIT AGREEMENT, CONTRACT, OR LICENSE |
| **Responsibility** |  |
| TRUSTworthy repositories take responsibility for the stewardship of their data holdings and for serving their user community. | OAIS  Mandatory Responsibilities |
| Responsibility is demonstrated by: |  |
| Adhering to the designated community’s metadata and curation standards, along with providing stewardship of the data holdings e.g. technical validation, documentation, quality control, authenticity protection, and long-term persistence. | OAIS does not demand use of Designated Community’s standards. |
| Providing data services e.g. portal and machine interfaces, data download or server-side processing. |  |
| Managing the intellectual property rights of data producers, the protection of sensitive information resources, and the security of the system and its content. | 3.5.2 THE REPOSITORY SHALL TRACK AND MANAGE INTELLECTUAL PROPERTY RIGHTS AND RESTRICTIONS ON USE OF REPOSITORY CONTENT AS REQUIRED BY DEPOSIT AGREEMENT, CONTRACT, OR LICENSE. |
| Repository users should have confidence that data depositors are prompted to provide all metadata compliant with the community norms, as this greatly enhances the discoverability and usefulness of the data. Knowing that a repository verifies the integrity of available data and metadata assures potential users that the data holdings are more likely to be interoperable with other relevant datasets. Both depositors and users must have confidence that the data will remain accessible over time, and thus can be cited and referenced in scholarly publications. | OAIS  – Ensure that the information to be preserved is Independently Understandable to the Designated Community. In particular, the Designated Community should be able to understand the information without needing special resources such as the assistance of the experts who produced the information.  – Follow documented policies and procedures which ensure that the information is preserved against all reasonable contingencies, including the demise of the Archive, ensuring that it is never deleted unless allowed as part of an approved strategy. There should be no ad-hoc deletions.  – Make the preserved information available to the Designated Community and enable the information to be disseminated as copies of, or as traceable to, the original submitted Content Information with evidence supporting its Authenticity. |
| Responsibility may be clarified through some legal means (right to preserve) or may take the form of voluntary compliance with some norm (ethical standards). | OAIS:  – Negotiate for and accept appropriate information from information Producers.  – Obtain sufficient control of the information provided to the level needed to ensure Long Term Preservation.  ISO 16363  3.5.1.3 The repository shall have written policies that indicate when it accepts preservation responsibility for contents of each set of submitted data objects. |
| **User Focus** |  |
| A TRUSTworthy repository needs to focus on serving its target user community. Each user community likely has differing expectations from their community repositories, depending in part on the community’s maturity regarding data management and sharing. A TRUSTworthy repository is embedded in its target user community’s data practices, and so can respond to evolving community requirements. We take a broad view of ‘user community’ as these could include users depositing or accessing data; those accessing data holdings computationally; and indirect stakeholders such as funders, journal editors, other institutional partners or citizens. | OAIS  – Determine, either by itself or in conjunction with other parties, which entities should become the Designated Community, that is, the communities that should be able to understand the information provided. Definition of the Designated Community includes a determination of their Knowledge Base.  – Ensure that the information to be preserved is Independently Understandable to the Designated Community. In particular, the Designated Community should be able to understand the information without needing special resources such as the assistance of the experts who produced the information.  – Follow documented policies and procedures which ensure that the information is preserved against all reasonable contingencies, including the demise of the Archive, ensuring that it is never deleted unless allowed as part of an approved strategy. There should be no ad-hoc deletions.  – Make the preserved information available to the Designated Community and enable the information to be disseminated as copies of, or as traceable to, the original submitted Content Information with evidence supporting its Authenticity. |
| Use and reuse of research data is an integral part of the scientific process, and therefore TRUSTworthy repositories should enable their community to find, explore, and understand their data holdings with regard to potential (re)use. Repositories should encourage users to fully describe data at the time of deposition and facilitate feedback on any issues with the data (e.g. quality or fitness for use) that may become apparent after the data have been made available. | OAIS  – Determine, either by itself or in conjunction with other parties, which entities should become the Designated Community, that is, the communities that should be able to understand the information provided. Definition of the Designated Community includes a determination of their Knowledge Base.  – Ensure that the information to be preserved is Independently Understandable to the Designated Community. In particular, the Designated Community should be able to understand the information without needing special resources such as the assistance of the experts who produced the information.  – Follow documented policies and procedures which ensure that the information is preserved against all reasonable contingencies, including the demise of the Archive, ensuring that it is never deleted unless allowed as part of an approved strategy. There should be no ad-hoc deletions.  – Make the preserved information available to the Designated Community and enable the information to be disseminated as copies of, or as traceable to, the original submitted Content Information with evidence supporting its Authenticity. |
| Repositories have a vital role in applying and enforcing the target user community norms and standards as compliance facilitates data interoperability and reusability. Data standards that TRUSTworthy repositories should enforce include metadata schema, data file formats, controlled vocabularies, ontologies, and other semantics where these exist in the user community. A TRUSTworthy repository may demonstrate adherence to this principle by: | OAIS:  – Determine, either by itself or in conjunction with other parties, which entities should become the Designated Community, that is, the communities that should be able to understand the information provided. Definition of the Designated Community includes a determination of their Knowledge Base.  – Ensure that the information to be preserved is Independently Understandable to the Designated Community. In particular, the Designated Community should be able to understand the information without needing special resources such as the assistance of the experts who produced the information.  – Follow documented policies and procedures which ensure that the information is preserved against all reasonable contingencies, including the demise of the Archive, ensuring that it is never deleted unless allowed as part of an approved strategy. There should be no ad-hoc deletions.  – Make the preserved information available to the Designated Community and enable the information to be disseminated as copies of, or as traceable to, the original submitted Content Information with evidence supporting its Authenticity |
| Implementing relevant data metrics and making these available to users. |  |
| Providing (or contributing to) community catalogues to facilitate data discovery. |  |
| Monitoring and identifying evolving community expectations and responding as required to meet these changing needs. |  |
| **Sustainability** |  |
| Ensuring sustainability of a TRUSTworthy repository is necessary to ensure uninterrupted access to its valuable data holdings for current and future user communities. Continued access to data is dependent upon the ability of the repository to provide services over time, and to respond with new or improved services to meet evolving user community requirements. |  |
| A TRUSTworthy repository may demonstrate the sustainability of its holdings by: |  |
| Planning sufficiently for risk mitigation, business continuity, disaster recovery, and succession. | OAIS  – Follow documented policies and procedures which ensure that the information is preserved against all reasonable contingencies, including the demise of the Archive, ensuring that it is never deleted unless allowed as part of an approved strategy. There should be no ad-hoc deletions. |
| Securing funding to enable ongoing usage and to maintain the desirable properties of the data resources that the repository has been entrusted with preserving and disseminating. |  |
| Providing governance for necessary long-term preservation of data so that data resources remain discoverable, accessible, and usable in the future. |  |
| **Technology** |  |
| A repository depends on the interaction of people, processes, and technologies to support secure, persistent, and reliable services. Its activities and functions are supported by software, hardware, and technical services. Together, these provide the tools to enable the delivery of the TRUST Principles. |  |
| A TRUSTworthy repository may demonstrate the fitness of its technological capabilities by: |  |
| Implementing relevant and appropriate standards, tools, and technologies for data management and curation. | 5.1.1 THE REPOSITORY SHALL IDENTIFY AND MANAGE THE RISKS TO ITS PRESERVATION OPERATIONS AND GOALS ASSOCIATED WITH SYSTEM INFRASTRUCTURE.  5.1.1.1 The repository shall employ technology watches or other technology monitoring notification systems.  5.1.1.1.1 The repository shall have hardware technologies appropriate to the services it provides to its designated communities.  5.1.1.1.2 The repository shall have procedures in place to monitor and receive notifications when hardware technology changes are needed.  5.1.1.1.3 The repository shall have procedures in place to evaluate when changes are needed to current hardware.  5.1.1.1.4 The repository shall have procedures, commitment and funding to replace hardware when evaluation indicates the need to do so.  5.1.1.1.5 The repository shall have software technologies appropriate to the services it provides to its designated communities.  5.1.1.1.6 The repository shall have procedures in place to monitor and receive notifications when software changes are needed.  5.1.1.1.7 The repository shall have procedures in place to evaluate when changes are needed to current software.  5.1.1.1.8 The repository shall have procedures, commitment and funding to replace software when evaluation indicates the need to do so.  5.1.1.2 The repository shall have adequate hardware and software support for backup functionality sufficient for preserving the repository content and tracking repository functions.  5.1.1.3 The repository shall have effective mechanisms to detect bit corruption or loss.  5.1.1.3.1 The repository shall record and report to its administration all incidents of data corruption or loss, and steps shall be taken to repair/replace corrupt or lost data.  5.1.1.4 The repository shall have a process to record and react to the availability of new security updates based on a risk-benefit assessment.  5.1.1.5 The repository shall have defined processes for storage media and/or hardware change (e.g., refreshing, migration).  5.1.1.6 The repository shall have identified and documented critical processes that affect its ability to comply with its mandatory responsibilities.  5.1.1.6.1 The repository shall have a documented change management process that identifies changes to critical processes that potentially affect the repository's ability to comply with its mandatory responsibilities.  5.1.1.6.2 The repository shall have a process for testing and evaluating the effect of changes to the repository's critical processes. |
| Having plans and mechanisms in place to prevent, detect, and respond to cyber or physical security threats. | 5.1.1 THE REPOSITORY SHALL IDENTIFY AND MANAGE THE RISKS TO ITS PRESERVATION OPERATIONS AND GOALS ASSOCIATED WITH SYSTEM INFRASTRUCTURE.  5.2.1 THE REPOSITORY SHALL MAINTAIN A SYSTEMATIC ANALYSIS OF SECURITY RISK FACTORS ASSOCIATED WITH DATA, SYSTEMS, PERSONNEL, AND PHYSICAL PLANT.  5.2.2 THE REPOSITORY SHALL HAVE IMPLEMENTED CONTROLS TO ADEQUATELY ADDRESS EACH OF THE DEFINED SECURITY RISKS.  5.2.3 THE REPOSITORY STAFF SHALL HAVE DELINEATED ROLES, RESPONSIBILITIES, AND AUTHORIZATIONS RELATED TO IMPLEMENTING CHANGES WITHIN THE SYSTEM. |

1. See <http://public.ccsds.org/publications/archive/650x0m2.pdf> [↑](#footnote-ref-2)
2. See <https://public.ccsds.org/Pubs/652x0m1.pdf> [↑](#footnote-ref-3)
3. See <http://www.coretrustseal.org> [↑](#footnote-ref-4)
4. <https://www.go-fair.org/fair-principles/> [↑](#footnote-ref-5)
5. <https://www.nature.com/articles/s41597-020-0486-7> [↑](#footnote-ref-6)