Broadening the Umbrella of Trust: Modular and Inheritable Certification for Repositories, Services, and Software Packages

Final outputs of the Research Data Alliance Technical Repository Service Providers Working Group for community consultation

Table of Contents

Authors 2
Affiliations 2
ORCID 2
INTRODUCTION 3
Why we need to broaden the umbrella of trust for repository certification 3
Brief History of Repository Evaluation 4
Challenges and Deficiencies in the Current Repository Certification Landscape 6
WG Objectives 7
Methods 8
Identification and Analysis of Sources of Attributes 8
Inclusion and Exclusion Criteria 9
Mapping Methods 10
Community Feedback Mechanism 10
Results 10
TRSP WG Attribute Inventory 10
Main Findings: Attribute Profiles 11
Gap Analysis 12
Certification models and their scope 14
Novel approaches to repository certification 15
Moving modular certification from theory to practice 16
Alignment with the European EDEN and FIDELIS Projects 16
DISCUSSION 17
Expected challenges 18

Strengths and limitations 19
Recommendations for moving forward with modular certification 20
CONCLUSION 22
References 23
Annexes 28
Annexure A: Scope and Status of Landscape Analysis 28
Annexure B: TRSP Results and Recommendations 30
B.1 Major concerns with existing repository certification approaches to be addressed 30
B.2: Approaches to Appraisal/ Assessment and Certification 31
B.3 Major Gaps in Assessment of Services 32
B.4 Normative and Informative Characteristics 33
B.5 Resolving Conflicts in Characteristics 33
Annexure C: Verifying Assessments 34
Annexure D: Community Consultation and Collaboration 38
D.1 Community Consultation Processes 38
D.2 Collaboration with the EOSC EDEN and FIDELIS Projects 38
D.3 Formal Feedback 40

Authors

Lauren Maxwell[1,2], Allyson Lister[3], Dieuwertje Bloemen[4], Olivier Rouchon[5], Wim Hugo[6], on behalf of the Research Data Alliance (RDA) Technical Repository Service Providers (TRSPs) Working Group

Affiliations

[1]Heidelberg Institute of Global Health (HIGH), Faculty of Medicine and University Hospital, Heidelberg University, Heidelberg, Germany
[2]Ecraid Foundation, Utrecht, Netherlands
[3]Oxford e-Research Centre (OeRC), Department of Engineering Science, University of Oxford, Oxford, United Kingdom
[4]KU Leuven, Leuven, Belgium
[5]CINES (Centre Informatique National de l'Enseignement Supérieur), Montpellier, France
[6]DANS (Data Archiving and Networked Services), Netherlands

ORCID

Lauren Maxwell: https://orcid.org/0000-0002-0777-2092
Allyson Lister: https://orcid.org/0000-0002-7702-4495
Dieuwertje Bloemen: https://orcid.org/0000-0003-4041-6855
Olivier Rouchon: https://orcid.org/0000-0002-1816-5546
Wim Hugo: https://orcid.org/0000-0002-0255-5101

INTRODUCTION

Why we need to broaden the umbrella of trust for repository certification

Community-developed criteria for identifying “trustworthy” data repositories are essential to centring investment, both financial and data, on repositories that meet core service criteria. The Community-based catalogue of requirements for trustworthy Trusted Repository Service Providers (TRSP) Research Data Alliance (RDA) Working Group (WG) was established to address a critical gap in the global research ecosystem: existing certification frameworks, such as CoreTrustSeal, Nestor, and ISO, have defined what constitutes a trustworthy repository through a binary approach to certification that only covers a subset of repositories and excludes most technical service providers on which repositories increasingly depend. Many generalist or domain-specific repositories meet some, but not all, of the criteria required for certification, yet the binary, all-or-nothing certification model does not offer a way to recognise partial compliance, improvement trajectories, or the contributions of outsourced services such as bit-level preservation. The absence of modularity may also make full certification more difficult and resource-intensive, because each repository must assemble and document evidence for the complete set of requirements, including criteria that may already be fulfilled and evidenced by external services or shared software packages. In practice, this can require repositories to repeat substantially similar assessment work for each certification application rather than reusing previously verified evidence. Emerging research outputs, including code, workflows, and semantic artefacts, fall outside of existing certification schemes.

Modular certification allows for the certification of the elements or criteria for which the applicant demonstrates the requisite maturity or performance level. The certification of software or attributes that are applied by different repositories could then be “inherited” by those repositories, reducing the burden of certification for those shared attributes or software approaches. Inheritance through the reuse of that component would allow a repository to reuse verified evidence for a certification criterion when that criterion is fulfilled by a certified external service or software package on which the repository depends. For example, where a repository uses a service provider or software package that has already been assessed for specific preservation, provenance, security, or interoperability criteria, the repository could reference that assessment in its own application rather than demonstrating the same criteria independently. The repository would remain responsible for showing that it uses the component in a way that does not undermine the certified characteristics and for providing evidence for the criteria that remain under its direct control.

Modular certification and the inheritance of modular certification provide a way to recognise and support repository best practice without compromising long-established, community-based expectations, broadening the umbrella of trust. To respond to the limitations of binary certification and evaluate what modular certification would need to entail, the RDA TRSP WG mapped the attributes and functions of repositories, including governance, sustainability, technical infrastructure, preservation capabilities, metadata practices, and service

dependencies, against criteria in existing trusted repository schemas. This mapping made visible where expectations, capabilities, and certification criteria aligned or diverged. We see this as the first step towards enabling modular assessments, delegating verification of service components, and building more inclusive pathways to defining repository trustworthiness.

By creating a community-validated catalogue of requirements applicable to repositories and the service providers that support them, and beginning the dialogue on modular certification and the inheritance of certification of attributes and software across repositories, the WG outputs support the extension of the umbrella of trust to a broader set of infrastructures, enable the evaluation of incremental improvement, and offer the research community more precise, granular information for selecting trustworthy repositories and services. Modular certification may also simplify future certification efforts. Repositories could progressively build a portfolio of verified modules, carry forward valid evidence of compliance, and update only the components affected by changes in their services, software, policies, or organisational arrangements. Shared services and software packages could likewise be assessed once for clearly defined criteria and reused across multiple repository applications, reducing duplication while allowing certification authorities to focus their review on repository-specific responsibilities and the integration of the inherited components. Emerging evaluation frameworks, such as OSTrails Assess-IF [1], can aid modular, community-specific, and machine-actionable certification, while integrations with existing resources can improve and inform trustworthiness evaluation.

Brief History of Repository Evaluation

The Open Archival Information System Reference Model (OAIS-RM) provides a conceptual framework for the long-term preservation of digital information, defining core archival functions such as ingest, archival storage, data management, preservation planning, access, and administration, as well as the structure of information packages (SIP, AIP, DIP) [2]. OAIS-RM does not itself certify repositories, but it has served as the foundational model for repository audit and certification approaches such as TRAC, ISO 16363, nestor, Data Seal of Approval, and, indirectly, CoreTrustSeal. OAIS-derived certification frameworks focus primarily on organisational governance, sustainability, documented workflows, preservation planning, risk management, and the repository's ability to maintain and provide access to digital objects over time. These approaches typically treat repositories as holistic entities and generally define whether a repository meets a set of requirements as a binary outcome. Table 1 provides a short history of the assessment and certification approaches derived from OAIS-RM [2].

Table 1. History of OAIS-RM-based repository assessment and certification

Timeline	Event	Description	Reference
2002 2012 2024	OAIS-RM	The Reference Model for an Open Archival Information System (OAIS-RM) provided the first widely adopted conceptual framework defining archival functions (Ingest, Archival Storage, Data Management, Administration, Preservation Planning, Access) and information packages (SIP, AIP, DIP).	[2,3]

Timeline	Event	Description	Reference
2005-2007	TRAC	Developed by the Online Computer Library Center (OCLC) and the Centre for Research Libraries (CRL), Trustworthy Repositories Audit & Certification (TRAC) introduced the first formal checklist-based audit criteria for digital repositories. TRAC mapped OAIS concepts into measurable organisational, technical, and financial criteria.	[4]
2006-2009	nestor	nestor developed a German catalogue of criteria for trustworthy digital archives, aligned with OAIS and TRAC, contributing to harmonisation efforts in Europe.	[5]
2012, 2025	ISO 16363	ISO 16363 transformed OAIS-RM and TRAC into an international ISO standard for auditing digital repositories and established a formal third-party certification pathway via audits by qualified auditors. A second edition, ISO 16363:2025, was published in March 2025.	[6,7]
2008-2018	Data Seal of Approval	Originally developed by Data Archiving and Networked Services (DANS) in the Netherlands, the Data Seal of Approval (DSA) introduced a community-driven, self-assessment model focused on practical, accessible requirements for research data repositories. Self-assessments could be verified by reviewers and led to certification if accepted.	[8]
2011–2018	World Data System (WDS)	The ICSU WDS developed its own certification framework for member data centres, focusing on governance, data quality, and service reliability.	[9]
2015-2018	Convergence, RDA	Recognising fragmentation, DSA and WDS aligned criteria via the RDA.	[10-12]
2017	CoreTrustSeal	CoreTrustSeal (CTS) was formed by merging the DSA and WDS certifications. It combined criteria into a single set of 16 requirements and became the de facto global baseline certification for research data repositories.	[13]
2020	TRUST Principles	Developed, published, and maintained partly through RDA-based collaboration, the TRUST Principles summarise the main characteristics of OAIS-RM-focused trustworthy repositories.	[14]

OAIS-RM=Open Archival Information System Reference Model

In contrast, non-OAIS-based approaches to repository evaluation generally emphasise different dimensions or components of trustworthiness, such as scientific impact, metadata interoperability, FAIR alignment, policy compliance, or domain-specific community value. For example, initiatives such as ELIXIR Core Data Resources assess the scientific quality and impact of specific data resources rather than auditing repository preservation processes. FAIRsharing and OpenAIRE assessments focus on standards alignment and technical interoperability. These alternative approaches may be inclusion-based rather than audit-based and are often more context-specific, discipline-driven, or function-targeted than OAIS-

based certification approaches, and are fundamentally more modular. Select non-OAIS-based approaches to repository certification are described in Table 2.

Table 2. Timeline of select alternatives to OAIS-RM-based assessment

Timeline	Event	Description	Reference
2017	ELIXIR CDR	ELIXIR developed the Core Data Resources (CDR) framework to identify life-science data resources of fundamental importance to the European research ecosystem.	[15]
2019	FAIRsharing	FAIRsharing confirms alignment between standards, policies, and data resources, and records metadata quality and FAIR status for research infrastructures and other resources.	[16]
2019	OpenAIRE	OpenAIRE evaluates repositories for inclusion in its network based on (1) Metadata interoperability, (2) Open access compliance, (3) PID usage, and (4) OAI-PMH compatibility.	[17,18]
2020	Criteria that Matter (CTM)	A collaboration between publishers and experts in the field formulated a set of criteria for repositories from a publisher's perspective.	[19]
2022	Global Biodata	Global Biodata Coalition extended the ELIXIR model globally to identify "Global Core Biodata Resources."	[20]

OAIS-RM=Open Archival Information System Reference Model

Challenges and Deficiencies in the Current Repository Certification Landscape

Current repository evaluation and certification options present a number of structural and practical challenges which provided the impetus for the formation of the RDA TRSP WG in 2023. Several of these challenges were anticipated in the RDA TRSP WG case statement [21], and confirmed and extended through TRSP WG-led community engagements [22,23]. The main areas for improvement that were identified through this process are:

- **Binary certification** indicates that an assessment and certification result is either accepted or not accepted, and, as a result, there are few or no mechanisms to reflect maturity or performance levels. Moreover (using CoreTrustSeal certification as an example), only successful certifications are published, leaving little information about repositories that applied for certification but were unsuccessful.
- **Lack of modular certification**: Modular certification allows applicant resources to be certified in part. Moving from binary certification of the repository as a whole to modular certification of the elements or criteria for which the applicant demonstrates the requisite maturity or performance level. Currently, no certification authority practises modular certification, which limits identifying repositories that meet some criteria for a trusted resource.

- **Certification cost:** Certification often involves a cost (e.g., CTS costs 3K for a 3-year certification), although fee waivers are available for repositories in low-and-middle-income countries. Ensuring repository documentation is certification-ready implies a significant investment of personnel time.
- **Certification complexity:** The evaluation and curation of the public-facing repository documentation and policies may necessitate convening different groups within a repository's structure and encoding consequential decisions into preservation plans and policies in a more explicit way. This process, while improving repository services, structure, and policies, may also require cross-functional engagement and budgetary commitments. This combined cost and complexity results in a very small percentage of repositories attempting such certification - estimated at approximately 5% of well-known repositories [24].
- **Self-assessment** (with or without some form of publicly accessible evidence and verification) is not available in a consistent and standardised manner, limiting the dissemination of information to repositories that have the resources to pursue a formal certification path.
- **Scope of Certification**: some criteria derived from OAIS-RM expect a well-defined designated community (usually discipline-specific), as well as deep curation and community-focused expertise.[1] Generalist repositories often struggle to meet these criteria. Services to repositories and software packages that enable repository functionality are not currently certifiable, as are repositories for other research outputs such as code and semantic artefacts.
- **Lack of Alignment**: There is significant divergence between OAIS-RM-based approaches and most alternatives. This creates confusion and complexity that improved alignment could reduce.

WG Objectives

The TRSP WG was convened to establish modular repository features and characteristics based on community expectations, to move beyond the limitations of current binary certification approaches. The WG identified repository functions that could be delegated to service providers and software packages, thereby improving efficiency and enabling economies of scale. The WG conceptualised a modular certification approach as an alternative to formal binary certification and began discussing decentralised, metadata-driven assessments to evaluate uncertified repositories and external services better.

We wanted to distinguish between repository attributes relevant to service providers and those that could be provided externally to the repository, and between cross-cutting services, like FAIR assessment, that could be provided across repositories. Software offerings, such as Dataverse, CKAN, DSpace, Invenio, and Figshare[2]may be used by different repositories. We wanted to understand which repository attributes and trustworthiness properties apply to them.

As such, two key WG objectives were to determine:

[1] While it is recognised that this maximises the chances that relevant expertise and technical measures to support the community with adequate quality is available, it also significantly limits choice for end users. If the argument is that all data should be published in certified disciplinary repositories, it also places significant additional demand on those repositories.

[2] These offerings range from open source repository platforms to 'software as a service'.

1. Which repository attributes are related to services and software packages
2. Which repository service attributes can be inherited across certifications (e.g., FAIR evaluation service software that is certified and then reused across different repositories will then mean that this component is certified for different repositories)

To address this, initial work focused on compiling a representative inventory of desirable repository characteristics, as reported in a separate supporting publication [22]. This effort included a mapping exercise to understand coverage and gaps in repository characterisation as indicated directly or implicitly by a large number of sources.

Methods

To support the development of modular approaches to repository certification, the TRSP WG first established a comprehensive and structured inventory of repository attributes drawn from existing certification schemes, registries, policy frameworks, and community guidance. The landscape-informed synthesis brought together attributes from established assessment models, such as CoreTrustSeal and the TRUST principles, with broader sources describing repository functions, best practices, and service dependencies. The WG systematically mapped these attributes across frameworks to identify convergence, divergence, and omissions, particularly for services and software packages not fully represented in current certification models. This methodological approach provided the analytical foundation for the WG and the larger community's assessment of where existing frameworks are sufficient, where extensions are required, and how to construct modular certification pathways that more inclusively characterise trustworthy repositories and their supporting infrastructures.

Identification and Analysis of Sources of Attributes

Numerous attribute sources describe the characteristics of repositories, archives, and the services/software packages that support them. Some sources are obvious and include registries of repositories (e.g., FAIRsharing, re3data, the European Open Science Cloud (EOSC) Resource Hub, and COAR), and several publications describe such attributes (e.g., Data Repository Attributes WG in RDA [25], Criteria that Matter, and Repository Features to Help Researchers: An invitation to a dialogue [26]). Others indirectly recommend repository attributes: the TRUST principles and the CoreTrustSeal requirements for certification discuss best practices and offer guidelines, which imply that certain attributes are available (e.g., evidence that a given policy exists and is accessible on the web). Digital preservation frameworks and archival standards provide another source of relevant characteristics, particularly for preservation functions, maturity, and how archival institutions describe themselves and their services. In addition, the DCAT-AP was explicitly created to describe 'Catalogue' (repository) properties, and schema.org provides equivalents for many repository characteristics.

Most of the sources we consulted to create an inventory of attributes and their mappings come from a landscape analysis. We identified sources iteratively through a landscape analysis supplemented by WG presentations, use cases, community discussions, and

consultation with related initiatives. These activities helped identify additional sources and assess whether the emerging inventory adequately represented different repository, archival, preservation, service, and software perspectives. The landscape analysis also considered implementation-oriented initiatives such as FAIR-IMPACT, which helped show how repository attributes can move from descriptive concepts to machine-actionable assertions linked to evidence, assessment results, and certification status [27]. While the major effort to identify attributes has concluded, the inventory remains open, and we will consider new sources if time and resources allow. Annexe A lists the current scope and status of the resources consulted.

Inclusion and Exclusion Criteria

We did not select resources used as sources of attributes on any specific basis. However, we focused on sources within the scope of the TRSP WG (certification, TRUST, and existing registries that host repository attributes). By iteratively analysing each new resource, mapping it to the inventory, and adding new attributes as needed, we created an inventory that required fewer additions with each iteration. This initial inventory and its classification were largely based on the TRUST Principles, CoreTrustSeal, POSI, Criteria that Matter, and the outputs of the Digital Repository Attributes WG in RDA.

A second round of collation involved verifying the classification, scope, and definition of the inventory using additional publications and sources, including re3data, CARE and FAIR principles, the GORC, and digital preservation considerations from NDSA and Digital Preservation Council resources.

A third round of collation involved verifying the inventory compiled by the TRSP WG with an inventory developed by the EOSC EDEN project. The project started from a different perspective: it relied on a collection of experts in a Work Package to identify and disambiguate the attributes and services that are required to support the following:

- The ‘Core Preservation Processes’ recommended for implementation by archives and repositories offering long-term preservation;
- Services and attributes identified by a panel of experts in respect of quality assurance, interoperability, and ethics and rights considerations; and
- Services and attributes identified from user stories obtained from participating use cases.

We are reasonably confident that the attributes identified in the TRSP inventory are based on a sufficiently broad sample of the landscape to represent a largely complete list. Still, there will certainly be omissions and additions in future.

A final round of input came from three public consultations at RDA Plenaries 23, 24 and 25, where, as applicable, inventories of attributes were shared with participants, who could contribute attributes or characteristics they considered missing. Appendix B presents these results.

Mapping Methods

The iterative addition of resources that directly or indirectly identify attributes created a de facto mapping among these resources, since attributes identified by more than one resource are annotated with each resource. This results in a graph-like attribute database that links the resource, either via a URL or a fragment of that URL, to an annotation and to the relevant attribute(s). The mapping is subjective, as it was often done by a single workgroup participant, sometimes two, which implies that a different analyst may classify and map an attribute differently. Future work, outside the scope of this WG, could focus on reviewing and confirming these mappings. Nevertheless, it will remain a useful resource.

The informal mapping of attributes to sources enables resource-based gap analysis. For example, it can identify which attributes are commonly associated with most resources but missing from a particular resource.

We formally determined gaps in the attribute inventory by comparing and collating it with the EOSC EDEN and FIDELIS project outputs. For those attributes identified as applicable to services and software packages, gaps will be identified, if they exist, by the organisations requested to perform a formal review - CTS, COAR, WDS, etc.

Community Feedback Mechanism

The community was asked to determine which repository attributes could be addressed through external certification of service providers, which attributes could be used for modular certification, and which could be inherited. In addition to regular feedback at open working group meetings, we engaged the wider repository stakeholder community via Mentimeter polls at RDA Plenaries in 2024 and 2025 [22,23,28]. Inheritance, in this context, means a criterion satisfied by a service or software platform can be adopted as is by a repository that uses the service or platform, removing the need for re-evaluation. Participants were also asked about the relative importance of different repository attributes. See Appendix D for a summary of past and future community engagement activities.

We will collate community consultation results and share these for comment with other stakeholders, including repository certification groups (CoreTrustSeal, nestor), the FIDELIS and EDEN projects, the World Data System, and COAR.

Results

TRSP WG Attribute Inventory

The TRSP WG, with assistance from the EOSC EDEN project, has identified and inventoried 342 repository attributes as of the time of writing.[3]. The inventory is available online, and details are in TRSP WG working documents. Figure 1 shows a subset of the inventory and its graphical representation.

[3] The EOSC EDEN and FIDELIS projects will continue to add refinements, extensions, mappings, and annotations to the inventory, in addition to future work planned for the TRSP WG.

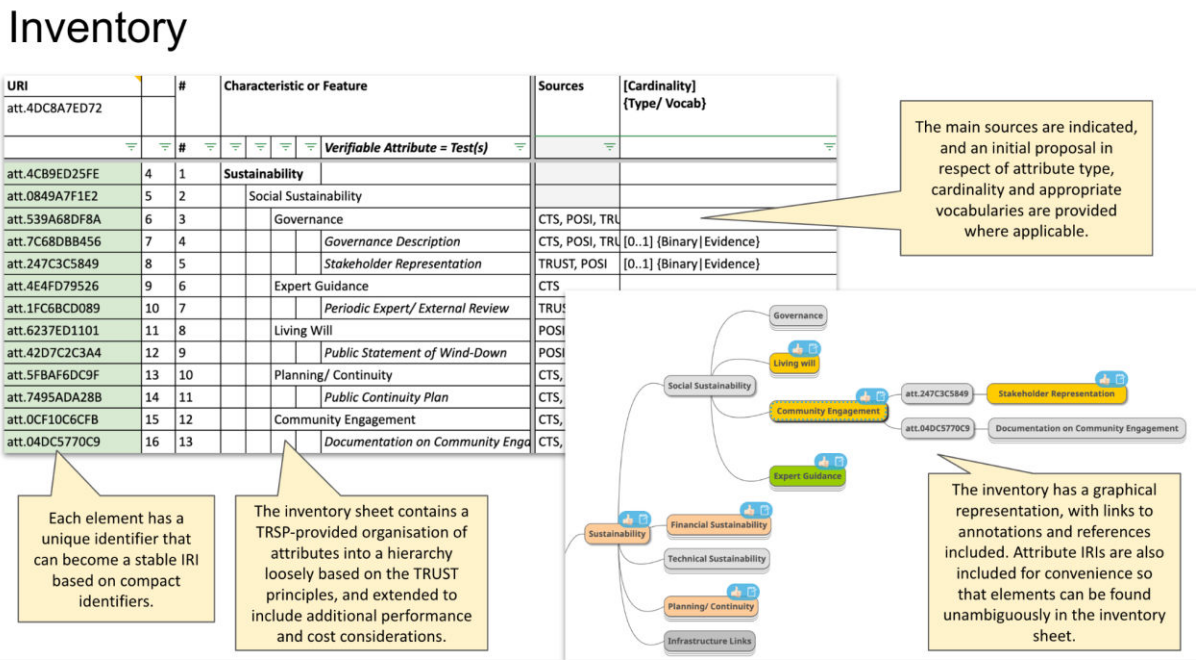


Figure 1. TRSP WG Inventory of Attributes and its Graphical Representation.

Main Findings: Attribute Profiles

The TRSP WG attribute inventory (Annexe B) facilitated the identification of subsets of attributes, i.e., profiles, applicable to three main cases: (1) services to repositories (including those supporting trustworthy repositories), (2) repository software packages such as Dataverse, DSpace, or Invenio, and (3) attributes that can be inherited from services or software packages by repositories when implemented and assessed at the level of the service or software package. The inheritance profile (3) is particularly important, as it would enable repositories to rely on verified service- or platform-level capabilities without duplicating assessment or certification efforts.

Community consultation revealed varying degrees of consensus across these profiles. Some attributes were unanimously selected or supported by a clear majority of respondents. Others were favoured by a majority but generated meaningful minority disagreement, while a third group was selected by a smaller majority yet faced little substantive opposition. Feedback also clarified an important distinction between normative attributes, which may form the basis for formal assessment or certification, and informative attributes, which support repository characterisation and selection but are less likely to serve as certification criteria. Proposed mechanisms for assessment and verification were developed and iteratively refined through RDA Plenary discussions (Annexe C). Their current formulation reflects this community input.

Most identified repository attributes could be organised within the broad structure provided by the TRUST principles. Notable exceptions included: (1) financial characteristics, including cost-recovery models, revenue sources, and major expenditure categories, which are rarely addressed explicitly in existing certification schemas, yet are important for repository transparency and selection, and (2) performance-oriented service characteristics such as

uptime, rate limits, allowable file sizes, and median time to publication, which are not commonly emphasised in the literature but were repeatedly highlighted in community consultations as critical considerations for users evaluating repository services and were also identified in a minority of the landscape references.

Gap Analysis

Gaps in criteria for repository certification were identified through a general approach driven largely by ranking concerns identified by the community (see Annexure B), and by including repository attributes not currently considered under existing certification schema but identified as necessary for assessing and certifying services and software packages.

General (structural, scope, and resource-related) gaps identified in the analysis of challenges, and confirmed by the WG, include the following, summarised here again for convenience :

- **Cost and time required for certification**: All existing formal certification pathways require considerable investment of time and money to achieve.
- **Binary nature of certification**: There is a shared perception that certification does not presently allow a gradual performance improvement.
- **Modular certification:** At present, no certification authority practises modular certification, which limits the identification of repositories that are responding to some of the criteria for a trusted resource, but not all of them.
- **Not all repositories can be certified**: Services to repositories (for example, long-term preservation services) cannot be certified in their own right, and generalist repositories are often out of scope for certification by CoreTrustSeal, nestor, and ISO.
- **No mechanism for certification of other research outputs**: In practice, the obvious omission at the current time would be software, for which certified or assessed repositories are not available. This concern falls outside the scope of the TRSP WG, but remains important to the community.

Gaps in the inventory of repository evaluation and certification criteria identified by TRSP include the specific attributes (which equate to criteria, metrics, tests, and benchmarks for which the attributes serve as evidence) [22,23,28] identified for services and software that do not correspond to CoreTrustSeal criteria for trusted repositories, listed in Table 3.

Table 3. Attributes not included in existing certification schema that were identified as important by the TRSP WG for Services and Software[4].

Attribute	Description	Scope	Inheritable
'Data is Free' att.0E0C905D2A	Identified primarily as a requirement for public infrastructure services by POSI [29], this criterion ensures that the data gathered by services is available to the community at no cost and serves as insurance should the service no longer be available. The attribute is linked to sub-attributes that provide	Services	No

[4] This table is a subset of table B.1 (Annexure B). In that table, all attributes applicable to services and software packages are listed, including those already linked to CoreTrustSeal criteria.

Attribute	Description	Scope	Inheritable
	evidence of revenue sources, the business model, and so on, which proves that revenue from data is out of scope.		
Inventory of Available Services att.532324DE1D	This is an important aspect related to services and software packages - providing both human- and machine-readable inventories of available services/ service elements and accompanying them with proper documentation. It is a prerequisite for incorporating services and/or software packages into automated workflows.	Services Platforms	Yes
Machine-Readable Policies att.03110A5773	For services, the focus is on automation. As a result, aspects such as policies and their implications should be machine-readable. Some policy provisions are expressed in licences or conditions of use and, as such, will be more useful as machine-readable, standardised resources.	Services	No
Performance Assessment att.1095E8CF4A	These aspects relate to performance assessments associated with digital services in general, not just within the research output management landscape. It covers aspects of process quality (e.g., ISO 9000), information security (ISO 27001), and service management (FitSM).	Services	No
Level of Service att.2090660301 att.2307B62BCB	This set of attributes includes aspects such as uptime and availability, and/or rate limits for services.	Services	No
Easy access to file and dataset properties att.7F7C2776AC	software packages should provide easy API access to file and dataset properties in addition to dataset metadata - for example, file sizes and checksums, file types, storage types, download links, and similar.	Platforms	No
Access to usage metrics and user feedback/ annotations att.70C4C7B218	These criteria allow end users to annotate and rate metadata and data, and provide them with links to external resources (other versions, citation metrics, web statistics...) as well as internal metrics (page views, downloads, access requests, etc.)	Platforms	No
Business Model Type att.7CBE776C7A	Transparent confirmation of the business model and how the cost of service is funded sustainably should be available.	Services	No
Median Time To Publication att.545686D0F9	The provision of turnaround time for the main service elements provided by a service, of which median time to publication is typically the most important for end users.	Services	No

TRSP=Trusted Repository Service Providers; WG=Working Group

The TRSP WG also determined, through community consultation, which attributes identified for services or software packages repositories using those services or platforms could inherit. Annexure B provides details of these relationships, and Table 4 summarises these inheritable attributes.

Table 4. Inheritable Repository Attributes Identified by the TRSP WG for Services and Software

Attribute	Description	Scope
(Full and Partial) Certification and Assessment att.371D70B854	In cases where an authority (e.g. CoreTrustSeal) certifies a service or a software package in full, i.e., for all relevant criteria, these criteria should be transferable to a repository making use of the service or software package. In the case of modular certification, individual criteria are transferable, as	Services Platforms

Attribute	Description	Scope
	described below.	
Public Continuity Plan att.7495ADA28B	In cases where services have published a continuity plan that has been certified by an authority, that certification should be carried through to repositories using such a service and aggregated with other applicable plans without the need for reassessment and certification.	Services
Applicable and appropriate (schema) att.7AD9748A7D	In cases where a service or software package implements metadata schema(s) that are applicable and appropriate to the community it serves, proof of such community focus can be transferred.	Services Platforms
Quality Control - Deposit Documentation att.00C02C55DC	Assess and certify the adequacy of deposit documentation, and verify its quality, through the repositories using the service or platform.	Services Platforms
Long-term Preservation att.570534F4B8	Long-term preservation actions and functionalities, and records of their execution performed by services or software packages, should be transferable to repositories using the service or platform.	Services Platforms
Licences att.419EE6D029	Proof of clearly documented information about licences, in human- and machine-readable formats, should be transferable to repositories if assessed and certified to be adequate for services and/ or software packages.	Services Platforms
Appropriate Licences att.4F40729393	Services or software packages may provide licences linked to defined levels of disclosure risk, and as such, be assessed and certified as adequate in this respect. Such assessment and/ or certification should be transferable to repositories making use of the service or platform.	Services Platforms
Administrative Capacity att.48E7481CDD	If a service demonstrates adequate administrative capacity to be certified in respect of fulfilment of its mandate and mission, this assessment or certification can be transferred to repositories using the service.	Services
Supported Dataset Formats att.4234565A8D	Supporting specific file (dataset) formats and documenting them in machine- and human-readable form supports end users and may satisfy assessment and certification benchmarks. In such cases, the outcome is transferable to repositories making use of the service or platform.	Services Platforms
Supported Metadata Schema att.6C03AB58B8	Supporting specific metadata schema(s) and documenting them in machine- and human-readable form supports end users and may satisfy assessment and certification benchmarks. In such cases, the outcome is transferable to repositories making use of the service or platform.	Services Platforms
Supported Persistent Identifiers att.2F993B25AD	Supporting the use of PIDs and documenting them in machine- and human-readable form supports end users and may satisfy assessment and certification benchmarks. In such cases, the outcome is transferable to repositories making use of the service or platform.	Services Platforms

TRSP=Trusted Repository Service Providers; WG=Working Group

Certification models and their scope

The TRUST principles [14], mentioned above, distil a high-level subset of the repository trustworthiness characteristics addressed in more detailed OAIS-RM-based certification frameworks, including CoreTrustSeal [13,30], nestor [5], and ISO 16363 [7].

These approaches focus on repository governance, sustainability, and succession planning, ensuring the quality and completeness of data descriptions for future discoverability, rights

management, interoperability, and reuse (mirroring FAIR criteria), with well-documented workflows and processes monitored for compliance. These aspects support an overarching goal of long-term preservation and availability of the resources entrusted to the repository.

Certification in the context of these TRUST-aligned approaches speaks to the repository's process quality and repeatability, its resource documentation and completeness, and its fitness for use and reuse by a designated community.

In contrast, the framework for **Core Data Resources** developed by ELIXIR [15] has ***scientific (content) quality*** as a foundational consideration, in addition to TRUST-aligned ones such as (1) Community served by the resource, (2) Quality of service, (3) Legal and funding infrastructure and governance, and (5) Impact and translational stories. ELIXIR assesses individual datasets for alignment with these criteria, rather than the repository holding them. Because datasets are evaluated for inclusion (effectively certification) in a multi-step, human-driven process, automation is less appropriate.

FAIR, while traditionally used to assess datasets, is applicable across all digital research objects and has been interpreted to measure database-level FAIRness. FAIRsharing's database-level FAIR benchmark operationalises FAIR through database-level characteristics and metrics [31]. Similarly, FAIREST [32] shows how an alternative implementation of FAIR can be used for repository evaluation, following other work to understand how repositories implement FAIR [33].

Our perspective, after looking at the scope of alternative approaches, is to make the question of valid and appropriate assessment criteria context-dependent. Each subset of criteria (linked to one or more characteristics or attributes) depends at least on the assessment objective, the type of resource being assessed, and the assessment granularity.

Criteria and attendant characteristics that are properly defined can be based on conceptual models developed in FAIRCORE4EOSC and OSTRAILS projects. Following these approaches results in well-defined, reusable definitions of criteria, metrics, tests, and benchmarks, referenceable with stable IRIs. The work performed by the TRSP WG to define a comprehensive inventory of repository attributes and its mappings ('profiles') directly supports such an approach.

The TRSP WG will not have enough time and resources to define standard metrics, tests, vocabularies, and benchmarks for all of the 350-odd attributes and characteristics it has identified, but should focus its remaining efforts on doing so for those attributes identified for services and software packages that are not currently in scope for practical certification, for example via CoreTrustSeal, and also offer examples of how current CoreTrustSeal criteria can be translated into metrics, tests, and benchmarks for purposes of self-evaluation and reuse.

Novel approaches to repository certification

The community consultation at Plenary 23 in Costa Rica [22] obtained input from participants regarding the mechanisms and characteristics of certification. This is discussed in detail in Annexure B.2. From the responses, we can make the following recommendations:

- Community responses strongly favoured mechanisms for consistent and public self-assessment, and a role is foreseen for automation of assessment, which will both reduce the effort of assessment for all and improve its reproducibility.
- Automation has a role if it is properly managed and monitored. This implies developing automated tests to determine or confirm the values of repository, service, and software package attributes, and to compare them with benchmarks. Clearly, AI-based assessment workflows will be useful in some cases.

A key innovation in this modular certification approach is the recognition that certification requirements can and should be community-dependent, rather than universally predefined. This mirrors recent developments in FAIR evaluation, particularly through the OSTrails Assess-IF [1] framework, which has created a shift from tools providing a universal definition of FAIRness (with such universality often limiting the applicability to individual communities) to communities transparently defining FAIR for themselves in a modular way. Our approach similarly enables any community to define and publish their own certification benchmarks as narrative documents or even machine-actionable profiles. This decentralisation fundamentally changes who performs certification: communities can compare benchmarks to identify common criteria and shared standards, fostering alignment while respecting contextual differences. By empowering communities to self-define requirements, certification costs may decrease; repositories no longer need to navigate complex, externally imposed frameworks but can instead align with criteria they've helped shape. Furthermore, when frameworks like Assess-IF and associated automated tools implement benchmarks, assessments can occur at regular intervals rather than as costly periodic events, enabling continuous compliance monitoring and reducing the burden of recertification.

Moving modular certification from theory to practice

The move from binary to modular certification requires sustained engagement from the diverse stakeholder groups that interact with the digital preservation landscape. Developing approaches to implement modular certification must include diverse disciplines and geographies to ensure adoption and build trust in a novel approach to defining trusted repositories. Implementing the WG recommendations would benefit from diverse funding sources to support collaborative development of software-based approaches, where relevant, and community adoption.

Alignment with the European EDEN and FIDELIS Projects

The EOSC EDEN and FIDELIS projects, because they align with the WG objectives to improve repository trustworthiness, will provide a preliminary test case for some WG recommendations. Specifically, EDEN will create a publicly available knowledge base (‘EDEN Registry’) that links attributes, repositories, and services based on defined relations. The registry is a project deliverable and will serve as a starting point for the FIDELIS network of repositories in EOSC. The scope of the EDEN and FIDELIS projects is narrower

(European repositories and a subset of the TRSP attributes). The registry's beta version is planned to be available in January 2027.

The EDEN project is currently mapping the TRSP inventory to DCAT-AP and schema.org, where applicable, and integrating the results of the Transparent Trustworthy Repository Attribute Metrics (TTRAM) work undertaken in the FIDELIS project [34,35]. The EDEN project is also in the process of (1) adding annotations to existing attributes where applicable, (2) defining the attributes in more detail where appropriate, (3) defining applicable vocabularies and specifying attribute cardinality for attributes important to the EDEN and FIDELIS projects, steps that will also support the movement towards implementing TRSP WG recommendations.

DISCUSSION

The TRSP RDA WG was launched to address structural limitations in existing repository certification frameworks, which have historically relied on binary, all-or-nothing models derived from OAIS-RM-aligned approaches such as CoreTrustSeal and ISO-based audit standards. While these frameworks have successfully defined core characteristics of trustworthy repositories, they exclude many generalist repositories, outsourced service providers, and software packages, and do not accommodate emerging research outputs such as code and semantic artefacts. Applicants vary from well-prepared ones that have documented policies and procedures and verified contracts; when these are not in place, certification involves considerable cost and time. Because of the documentation process and limited uptake of certification, many repositories do not pursue certification, are unaware of it, or choose not to recertify after their certification expires.

To respond to this gap, we conducted a comprehensive landscape analysis and mapping exercise, compiling an inventory of 342 repository attributes derived from certification schemas, registries, policy frameworks, and community consultations. We iteratively mapped these attributes across sources and reviewed and updated them in concert with the Horizon Europe-funded EDEN and FIDELIS projects. Through multiple public consultations and structured gap analysis, the WG identified which attributes apply to repositories, which to services and software packages, and which could be inherited across certification contexts, thereby establishing the conceptual foundation for modular, federated approaches to repository assessment.

The recommendations we developed through extensive review and comparison of certification schemas and repository attributes, along with community consultations, form the basis for the WGs' recommendations for certification authorities, repository networks, infrastructure projects, and the broader research data community. We call for (1) modular, piecewise certification pathways; (2) mechanisms for inheriting certified service or software attributes; (3) development of maturity levels and benchmarks; (4) extension of certification scope to services, software packages, and additional research outputs; and (5) consistent, publicly accessible self-assessment mechanisms supported by automation.

The EDEN and FIDELIS initiatives can serve as early implementation environments to develop the guidance and software-based approaches needed to trial these recommendations in practice. For example, the EDEN registry for repository attribute profiles, community benchmarks, and mappings to DCAT-AP and schema.org can serve as an implementation resource. Certification authorities such as CoreTrustSeal, and networks including the World Data System and COAR, should consider inheritance mechanisms and the integration of service- and software-level criteria into existing repository support services or review processes.

Expected challenges

The transition from binary, repository-level certification to modular, federated, and inheritable approaches introduces conceptual, technical, governance, and adoption challenges. **(1) Interoperability and semantic alignment**. Although the TRSP Working Group developed a comprehensive inventory of 342 attributes, consistent interpretation and implementation across communities will require precise definitions, shared vocabularies, and sustained and inclusive governance. Without careful coordination and version control, modular certification risks introducing fragmentation and end-user confusion, rather than harmonisation, and will not deliver on its goal of building trust in and uptake of repository certification. Modular attributes and their certification pathways may be difficult to share due to limited interoperability or community-specific implementation concerns. **(2) Defining benchmarks and maturity levels.** Moving beyond binary certification requires agreement on context-dependent thresholds, performance classes, and evidence requirements, all of which may vary by discipline, repository type, and infrastructure scale. Establishing who defines and maintains these benchmarks, how disagreements are resolved, and which benchmarks are community-specific and which can be defined at a higher level will be critical. **(3) The inheritance of certified attributes from services or software packages.** Clear and transparent rules must govern full and partial inheritance, how multiple services contribute to a single criterion, and how certification validity is managed when underlying services change. **(4) Automated authentication of modular components** is a key priority and challenge for moving towards implementation. Automation can reduce certification burden and increase reproducibility, but it also poses risks. Overreliance on machine-detectable indicators may privilege what is measurable over what is meaningful, and AI-based assessment workflows may introduce bias or false precision if the evidence and approach underlying the assessment are not sufficiently clear. The technical implementation of the attribute definitions in TTL, made openly available through GitHub, aims to provide a mechanism for encoding automated verification. CoreTrustSeal, for example, can use the TTL serialisation of the attributes to support automated verification of the sub-criteria in each requirement. **(5) Institutional transformation.** Adoption of the novel certification approach proposed here by existing certification authorities, such as CoreTrustSeal, will require institutional adaptation and potentially revised review processes. The conceptualisation of certification as community-defined profiles of modular components makes certification both modular and binary (i.e., components can be individually certified, but the goal remains for a repository to meet the highest standards for trustworthiness). Stakeholders accustomed to binary approaches to defining trust must also be willing to interpret graded or modular

certification outcomes. **(6) Global equity considerations.** Certification models have historically reflected well-resourced infrastructures, and although modular approaches aim to broaden participation, under-resourced repositories may struggle to produce machine-readable evidence or engage in benchmark-setting processes. **(7) Building the research community's understanding of why using trusted repositories is important.** The current situation, in which only a small fraction of repositories are certified, is driven more by a lack of understanding of the importance of the criteria used to identify trusted repositories than by the certification process itself. Continuing to build awareness of the importance of repositories in facilitating data reuse, and of the rationale for using trusted repositories as part of research data management curricula or other outreach efforts, will remain a challenge, regardless of the certification approach. **(8) Sustained engagement and funding.** The sustainability of software-based implementations and community profiles for modular certification, developed in collaboration with EDEN and FIDELIS, will depend on long-term governance, funding, and stewardship, and broad, sustained engagement.

Strengths and limitations

This work has several important strengths. To our knowledge, the TRSP WG has produced one of the most comprehensive mappings of repository attributes and certification schema inventories to date. The repository attribute mapping was grounded in multiple rounds of community consultation, including representatives from repository certification and the attribute schema. By explicitly mapping areas of convergence and divergence between OAIS-derived and alternative evaluation approaches, the work clarifies where trust expectations align and where they diverge, providing an evidence-based foundation for modular certification. Our close collaboration with the EDEN and FIDELIS projects, which were ongoing during the WG activities, strengthened the practical relevance and implementation potential of the WG recommendations.

Registry-based implementations of modular service and attribute certification, along with machine-actionable profiles, offer a way to lower the bar for certification while ensuring adherence to the core attributes and services widely used to encode the concept of trust in repositories. Introducing inheritable criteria for services and software packages can reduce duplication, lower certification burden, and recognise distributed infrastructures more fairly. Modular certification supports incremental improvement and broader inclusion, allowing generalist repositories and service providers to demonstrate compliance with relevant subsets of criteria rather than being excluded by binary thresholds.

Our work had several limitations. Community engagement, while iterative and transparent, has been largely shaped by European project collaborations and Europe-heavy RDA participation patterns. We attempted to address this bias by engaging colleagues in other geographies through RDA plenaries in other locations (e.g., Costa Rica, Australia). Closer engagement with digital preservation colleagues outside of Europe would support global representativeness and uptake. Mapping and classifying attributes involved interpretive judgment. Other groups may have grouped attributes differently, and despite our best efforts, we may have overlooked attributes important to specialist repositories or to geographies less likely to engage in RDA. The WG identified attributes, inheritance relationships, and implementation concepts, but developing actionable definitions of metrics, tests, and

benchmarks for all criteria was outside the WG's scope. Ultimately, modular certification will succeed only if certification authorities, repository networks, and infrastructure providers adopt it. Without integration into established evaluation processes, the framework risks remaining advisory rather than transformative. While the conceptualisation of different approaches to modular certification as ***self-assessment, assessment by an authority, or automated (federated) assessment*** opens the doorway to supporting more nuanced definitions of “trusted” repositories, it also raises questions about differences in the quality of the evidence to support such designations that will need to be considered by the repository community and stakeholders.

Recommendations for moving forward with modular certification

To support implementation of the TRSP WG recommendations, we recommend working with digital preservation communities to identify priorities for machine-actionable metrics, tests, and benchmarks for the most critical service- and software-related attributes, and to develop pathways for translating existing CoreTrustSeal guidance into reusable components suitable for modular assessment and self-assessment.

Collaboration with EDEN and FIDELIS, which will continue until December 2027, should focus on developing and piloting repository and community profiles of modular attributes, including inheritance logic and context-specific benchmarks. The WG should also continue engaging with certification authorities, repository networks, and service providers to identify funding opportunities for co-designing pilot inheritance and verification workflows applicable to federated assessment models, self-certification, and third-party review.

The following 20 recommendations summarise the WG’s findings from the extensive literature review and community consultations described above. Recommendations cover overarching principles and scope, including metrics, benchmarking, and inheritance, as well as implementation and future research.

R1: Adopt a gradual approach to gathering, presenting, and refining evidence as part of the transition towards modular assessment and certification.

R2: Introduce modular, or piecewise, assessment and certification to address concerns arising when repositories cannot meet or demonstrate all certification criteria.

R3: Define levels of maturity or performance that can be used as benchmarks within modular assessment and certification.

R4: Develop a flexible, modular set of criteria that are defined consistently and interoperably, independent of the application context.

R5: Extend the scope of certification to include services and software packages.

R6: Enable generalist repositories to obtain certification for the criteria that they cover, rather than requiring them to meet criteria outside their scope.

R7: Develop and publish detailed definitions, including metrics, tests, and benchmarks, for all criteria mapped to CoreTrustSeal and for the additional service- and software package-related criteria identified by the TRSP WG.

R8: Make criteria relating to service turnaround times, such as time to publication, transparently available to end users, while recognising that turnaround times depend on the time and effort required to appraise and curate deposits, which are currently undertaken predominantly by humans.

R9: Evaluate self-assessments against open community benchmarks to improve consistency, while recognising the challenge of compiling and curating benchmarks across multiple communities.

R10: Recognise that benchmarks are context-dependent and that each context may require a different profile. Explore implementation through the EOSC EDEN and FIDELIS projects, including functionality for creating and maintaining context-specific profiles comprising defined sets of attributes and benchmark values.

R11: Encourage certification authorities to consider the inheritance of criteria already certified for services and software packages as a mechanism for reducing the certification burden on repositories.

R12: Apply the following generic cases when considering the inheritance of certified criteria:

- When a service or software package is fully certified, all matching criteria may be transferred to a repository using that service or platform, provided that the repository's implementation does not undermine the modularly certified elements.
- When a service or software package acts as a full proxy for a defined set of repository criteria—for example, by providing long-term preservation services for several repositories or implementing self-documenting provenance records—those criteria may be transferred to the repository without modification.
- When multiple services or software packages contribute to one or more criteria, assess the repository based on the aggregate of the contributing certifications or assessments.

R13: Focus the remaining work of the TRSP WG, inter alia, on elaborating and refining the guidelines and benchmarks for assessing the service- and software package-related attributes presented in Annexure B.

R14: Engage relevant communities in developing tests and benchmarks for the additional service- and software package-related attributes identified by the TRSP WG.

R15: Evaluate and transform current CoreTrustSeal guidance into a set of tests and benchmarks suitable for self-assessment, assessment by a certification authority, and automated assessment.

R16: Propose that CoreTrustSeal consider adding service- and software package-related criteria to its certification process after appropriate guidelines have been developed with input from the community and the TRSP WG.

R17: Recommend that the EDEN project include the combined community benchmarks and tests in the publicly available EDEN/FIDELIS registry of repository certification approaches.

R18: Advocate for and foster further work within RDA to address modular certification and the associated assessment challenges.

R19: Consider the development of automation frameworks, including approaches based on Assess-IF and the Compliance Assessment Toolkit conceptual model, as a potential follow-up topic for an RDA Working Group.

R20: Support further research and development on the role of automation in assessment, particularly the use of AI-based assessment and the identification and management of biases introduced through automation.

CONCLUSION

In collaboration with EDEN, FIDELIS, and the broader repository certification community, the TRSP WG will identify opportunities to translate the attribute inventory and recommendations into interoperable software frameworks and community profiles that support federated, modular certification. This includes community-informed, federated approaches to defining machine-actionable metrics, tests, and benchmarks for prioritised attributes; formalising community profiles; and enabling assessment workflows that can be conducted as self-certification, third-party authority certification, or automated evaluation.

References

1. OSTrails Consortium. FAIR testing interoperability framework (FAIR-IF / Assess-IF) [Internet]. OSTrails technical documentation; 2024 [cited 2026 Oct 6]. Available from: https://docs.ostrails.eu/en/latest/architecture/fair-if.html
2. Consultative Committee for Space Data Systems. Reference model for an open archival information system (OAIS). Recommended practice CCSDS 650.0-M-2. Issue 2. Washington (DC): CCSDS; 2012. Available from: https://public.ccsds.org/pubs/650x0m2.pdf
3. Consultative Committee for Space Data Systems. Reference model for an open archival information system (OAIS). Recommended practice CCSDS 650.0-M-3. Issue 3. Washington (DC): CCSDS; 2024. Published as ISO 14721:2025. Available from: https://ccsds.org/Pubs/650x0m3.pdf
4. Center for Research Libraries, OCLC Online Computer Library Center. Trustworthy repositories audit and certification (TRAC): criteria and checklist. Version 1.0. Chicago (IL): Center for Research Libraries; 2007 Feb. OCLC:85786759. Available from: https://digitalcollections.crl.edu/search?ln=en&p=oclc:85786759
5. nestor Working Group Trusted Repositories, Certification. Catalogue of criteria for trusted digital repositories. Version 2. Frankfurt am Main: nestor c/o Deutsche Nationalbibliothek; 2009. urn:nbn:de:0008-2010030806. Available from: http://nbn-resolving.de/urn:nbn:de:0008-2010030806
6. International Organization for Standardization. ISO 16363:2012. Space data and information transfer systems: audit and certification of trustworthy digital repositories. 1st ed. (withdrawn). Geneva: ISO; 2012. Available from: https://www.iso.org/standard/56510.html
7. International Organization for Standardization. ISO 16363:2025. Space data and information transfer systems: audit and certification of trustworthy digital repositories. 2nd ed. Geneva: ISO; 2025. Available from: https://www.iso.org/standard/87472.html
8. CoreTrustSeal. Data Seal of Approval synopsis (2008–2018) [Internet]. n.d. [cited 2026 Sep 24]. Available from: https://www.coretrustseal.org/about/history/data-seal-of-approval-synopsis-2008-2018/
9. CoreTrustSeal. WDS regular member certification (2011–2018) [Internet]. n.d. [cited 2026 Sep 24]. Available from: https://www.coretrustseal.org/about/history/wds-regular-member-certification-2011-2018/
10. Rickards L, Vardigan M, Diepenbroek M, Dillo I, Genova F, L'Hours H, et al. DSA–WDS Partnership Working Group catalogue of common procedures for certification. Version 1.2. Research Data Alliance; 2016. Available from: https://doi.org/10.15497/RDA00019
11. L'Hours H, Kleemola M, de Leeuw L. CoreTrustSeal: from academic collaboration to sustainable services. IASSIST Q. 2019;43(1):1–17. Available from: https://doi.org/10.29173/iq936
12. Repository Audit and Certification DSA–WDS Partnership Working Group. DSA–WDS Partnership: catalogue of common requirements. Version 2.3. DSA, ICSU–

WDS, RDA; 2016. Available from: https://doi.org/10.15497/RDA00021

13. CoreTrustSeal Standards and Certification Board. CoreTrustSeal requirements 2023–2025. Version 01.00. Zenodo; 2022. Available from: https://doi.org/10.5281/zenodo.7051012
14. Lin D, Crabtree J, Dillo I, Downs RR, Edmunds R, Giaretta D, et al. The TRUST Principles for digital repositories. Sci Data. 2020;7(1):144. Available from: https://doi.org/10.1038/s41597-020-0486-7
15. Durinx C, McEntyre J, Appel R, Apweiler R, Barlow M, Blomberg N, et al. Identifying ELIXIR core data resources [version 2; peer review: 2 approved]. F1000Res. 2017;5(ELIXIR):2422. Available from: https://doi.org/10.12688/f1000research.9656.2
16. Sansone SA, McQuilton P, Rocca-Serra P, Gonzalez-Beltran A, Izzo M, Lister AL, et al.; FAIRsharing Community. FAIRsharing as a community approach to standards, repositories and policies. Nat Biotechnol. 2019;37(4):358–67. Available from: https://doi.org/10.1038/s41587-019-0080-8
17. OpenAIRE. OpenAIRE guidelines [Internet]. n.d. [cited 2026 Sep 24]. Available from: https://guidelines.openaire.eu/en/latest/
18. Hugo W, Manghi P. Case study: principles for high-quality data sources in OpenAIRE encoded in CAT. Zenodo; 2025. Available from: https://doi.org/10.5281/zenodo.15534446
19. Sansone SA, McQuilton P, Cousijn H, Cannon M, Chan WM, Callaghan S, et al. Data repository selection: criteria that matter. Zenodo; 2020. Available from: https://doi.org/10.5281/zenodo.4084763
20. Global Biodata Coalition. Global core biodata resources: concept and selection process. Zenodo; 2022. Available from: https://doi.org/10.5281/zenodo.7468719
21. RDA TRSP Working Group. Community-based catalogue of requirements for trustworthy technical repository service providers: working group case statement. Version 1.0. Research Data Alliance; 2024. Available from: https://www.rd-alliance.org/wp-content/uploads/2024/07/Case-Statement-Community-based-catalogue-of-requirements-for-trustworthy-Technical-Repository-Service-Providers-Working-Group-Case-Statement-v1.0.pdf
22. Hugo W, Lister A, Maxwell L, Ramamurthy M. TRSP WG: results of community consultation 1. Presented at: RDA 23rd Plenary; 2024 Nov 12-14; San José, Costa Rica. Zenodo; 2026. Available from: https://doi.org/10.5281/zenodo.23183439
23. Hugo W, Lister A, Maxwell L, Ramamurthy M. TRSP WG: results of community consultation 2. Presented at: RDA 24th Plenary (virtual); 2025 Apr 7-11. Zenodo; 2026. Available from: https://doi.org/10.5281/zenodo.18542662
24. Key C, Llebot C, Boock M. Building a trustworthy data repository: CoreTrustSeal certification as a lens for service improvements. J eScience Librariansh. 2023;12(3):e761. Available from: https://doi.org/10.7191/jeslib.761
25. Witt M, Cannon M, Lister A, Segundo W, Shearer K, Yamaji K, Research Data Alliance Data Repository Attributes Working Group. RDA common descriptive attributes of research data repositories. Version 1.0. Research Data Alliance; 2024. Available from: https://doi.org/10.15497/RDA00103

26. Cannon M, Graf C, McNeice K, Chan WM, Callaghan S, Carnevale I, et al. Repository features to help researchers: an invitation to a dialogue [preprint]. Zenodo; 2021. Available from: https://doi.org/10.5281/zenodo.4683794
27. Huber R, Ulrich R, L'Hours H, Hugo W, Neidiger C, Parkes O, et al. M5.8: pilot for exposing repository trustworthiness status and FAIR data and code assessment outcomes in generic and disciplinary registries and portals [project milestone]. Version 1.0. Zenodo; 2024. Available from: https://doi.org/10.5281/zenodo.13861127
28. Hugo W, Lister A, Maxwell L, Ramamurthy M. TRSP WG: results of community consultation 3. Presented at: RDA 25th Plenary; 2025 Oct 14-16; Brisbane, Australia. Zenodo; 2026. Available from: https://doi.org/10.5281/zenodo.18549061
29. Bilder G, Lin J, Neylon C. The principles of open scholarly infrastructure. Version 1.0. 2020. Available from: https://doi.org/10.24343/C34W2H
30. CoreTrustSeal Standards and Certification Board. CoreTrustSeal requirements 2026-2028. Version 01.00. Zenodo; 2025. Available from: https://doi.org/10.5281/zenodo.17660463
31. FAIRsharing. Database-level FAIRness [Internet]. n.d. [cited 2026 Oct 6]. Available from: https://fairsharing.gitbook.io/fairsharing/fair-assistance/database-level-fairness
32. d'Aquin M, Kirstein F, Oliveira D, Schimmler S, Urbanek S. FAIREST: a framework for assessing research repositories. Data Intell. 2023;5(1):202–41. Available from: https://doi.org/10.1162/dint_a_00159
33. Maxwell L, Shreedhar P, Dauga D, McQuilton P, Terry RF, Denisiuk A, et al. FAIR, ethical, and coordinated data sharing for COVID-19 response: a scoping review and cross-sectional survey of COVID-19 data sharing platforms and registries. Lancet Digit Health. 2023;5(10):e712–e736. Available from: https://doi.org/10.1016/S2589-7500(23)00129-2
34. Conzett P, Duvaud S, Jouneau T, Kallio J, Klemetsen T, Recker J, et al. Digital repository capabilities and characteristics mapping spreadsheet [dataset]. Zenodo; 2025. Available from: https://doi.org/10.5281/zenodo.17471457
35. Kleemola M, Kaartinen H, Bäckman S, Conzett P, Duvaud S, Parkes O, et al. D5.1: harmonised matrix of repository functions, activities and characteristics. Zenodo; 2025. Available from: https://doi.org/10.5281/zenodo.17973113
36. Confederation of Open Access Repositories. Next generation repositories: behaviours and technical recommendations of the COAR Next Generation Repositories Working Group. Zenodo; 2017. Available from: https://doi.org/10.5281/zenodo.1215014
37. Strecker D, Axtmann A, Bertelmann R, Cousijn H, Elger K, Ferguson LM, et al. Metadata schema for the description of research data repositories: version 4.0. re3data; 2023. 33 p. Available from: https://doi.org/10.48440/re3.014
38. Thurston M, Lister A, Granell R, Batista D, McQuilton P, Rocca-Serra P, et al. FAIRsharing application: schema. Zenodo; 2025. Available from: https://doi.org/10.5281/zenodo.17045694
39. FAIRsharing. Database conditions [Internet]. n.d. [cited 2026 Sep 24]. Available from: https://fairsharing.gitbook.io/fairsharing/additional-information/database-

conditions

40. Confederation of Open Access Repositories. COAR community framework for good practices in repositories. Version 2. Zenodo; 2022. Available from: https://doi.org/10.5281/zenodo.7108101
41. European Commission, Directorate-General for Research and Innovation; Hellström M, Heughebaert A, Kotarski R, et al. A persistent identifier (PID) policy for the European Open Science Cloud (EOSC). Luxembourg: Publications Office of the European Union; 2020. Available from: https://data.europa.eu/doi/10.2777/926037
42. Carroll SR, Garba I, Figueroa-Rodríguez OL, Holbrook J, Lovett R, Materechera S, et al. The CARE Principles for Indigenous Data Governance. Data Sci J. 2020;19:43. Available from: https://doi.org/10.5334/dsj-2020-043
43. SEMIC. DCAT application profile for data portals in Europe (DCAT-AP). Version 3.0.1. European Commission; 2025. Available from: https://semiceu.github.io/DCAT-AP/releases/3.0.1
44. Schema.org. Dataset. In: Schema.org vocabulary [Internet]. n.d. [cited 2026 Jan 31]. Available from: https://schema.org/Dataset
45. National Digital Stewardship Alliance. Levels of digital preservation [Internet]. n.d. [cited 2026 Sep 24]. Available from: https://ndsa.org/publications/levels-of-digital-preservation/
46. Digital Preservation Coalition. Digital Preservation Coalition rapid assessment model (DPC RAM). Version 3. DPC; 2024. Available from: http://doi.org/10.7207/dpcram24-03
47. Digital Preservation Coalition. Core requirements for a digital preservation system. In: DPC procurement toolkit [Internet]. 2022 [cited 2026 Sep 24]. Available from: https://www.dpconline.org/digipres/implement-digipres/procurement-toolkit/procurement-toolkit-core-requirements
48. Woodford C, Treloar A, Leggott M, Payne K, Jones S, Lopez Albacete J, et al. The Global Open Research Commons International Model. Version 1. Research Data Alliance; 2023. Available from: https://doi.org/10.15497/RDA00099
49. Braukmann R, Kvamme T, Kleemola M, Dolinar M, Alfredsson I. D16 landscape workshop and report. Version 1.0. Zenodo; 2023. Available from: https://doi.org/10.5281/zenodo.5554457
50. Frank RD. Constructing risk in trustworthy digital repositories. J Doc. 2024;80(6):1508–27. Available from: https://doi.org/10.1108/JD-08-2023-0157
51. RDA/WDS Trust Principles Outreach and Adoption Working Group [Internet]. Research Data Alliance; n.d. [cited 2026 Sep 24]. Available from: https://www.rd-alliance.org/groups/rdawds-trust-principles-outreach-and-adoption-working-group/activity
52. OAPEN. ERC open access requirements for FP7, Horizon 2020 and Horizon Europe grants [Internet]. n.d. [cited 2026 Sep 24]. Available from: https://www.oapen.org/article/13934224-erc-oa-requirement
53. Barbosa S, Curtin L, Cousijn H. Generalist repository ecosystem initiative introductory brochure. Zenodo; 2023. Available from: https://doi.org/10.5281/zenodo.8350509

54. FAIRsFAIR. 5_4_prototype [software repository]. GitHub; 2024 [cited 2026 Oct 6]. Available from: https://github.com/FAIRsFAIR/5_4_prototype
55. Hugo W, Steinhoff W, Turner D, Buys M, Zamani T. FAIRCORE4EOSC D2.1: compliance assessment specification [project deliverable]. Zenodo; 2023. Available from: https://doi.org/10.5281/zenodo.10067253
56. EOSC EDEN and FIDELIS [Internet]. n.d. [cited 2026 Sep 24]. Available from: https://eden-fidelis.eu/

Annexes

Annexure A: Scope and Status of Landscape Analysis

Table A1. Resources Consulted in the Landscape Analysis to Identify Attributes

Label	Source of Information
COAR [36]	COAR (n.d.), Next Generation Repositories. https://ngr.coar-repositories.org/
re3data.org [37]	Strecker, D., Axtmann, A., Bertelmann, R., Cousijn, H., Elger, K., Ferguson, L. M., Fichtmüller, D., Jones, C., Lindenmann, I., Neidiger, C., Nguyen, T. B., Pal, J. K., Pampel, H., Petras, V., Schnepf, E., Semrau, A., Ulrich, R., Upmeier, A., Vierkant, P., Wang, H., Weickert, G., Weisweiler, N. L., Williams, S. C., Witt, M., Wright, S. J. (2023): Metadata Schema for the Description of Research Data Repositories: version 4.0, re3data, 33 p. https://doi.org/10.48440/re3.014
FAIRsharing [38,39]	Thurston, M., Lister, A., Granell, R., Batista, D., McQuilton, P., Rocca-Serra, P., & Sansone, S.-A. (2025). FAIRsharing Application: Schema. Zenodo. https://doi.org/10.5281/zenodo.17045694 FAIRsharing database metadata (https://fairsharing.gitbook.io/fairsharing/additional-information/database-conditions)
COAR [40]	Confederation of Open Access Repositories. (2022). COAR Community Framework for Good Practices in Repositories, Version 2 (Version 2). Zenodo. https://doi.org/10.5281/zenodo.7108101
TRUST [14]	Lin, D., Crabtree, J., Dillo, I. et al. The TRUST Principles for digital repositories. Sci Data 7, 144 (2020). https://doi.org/10.1038/s41597-020-0486-7
DRAWG [25]	Witt, M., Cannon, M., Lister, A., Segundo, W., Shearer, K., Yamaji, K., & Research Data Alliance Data Repository Attributes Working Group. (2024). RDA Common Descriptive Attributes of Research Data Repositories (1.0). Zenodo. https://doi.org/10.15497/RDA00103
CTM [19]	Sansone, S.-A., McQuilton, P., Cousijn, H., Cannon, M., Chan, W. M., Callaghan, S., Carnevale, I., Cranston, I., Edmunds, S., Everitt, N., Ganley, E., Graf, C., Hrynaszkiewicz, I., Khodiyar, V., Leary, A., Lemberger, T., MacCallum, C., McNeice, K., Murray, H., … Threlfall, J. (2020). Data Repository Selection: Criteria That Matter. Zenodo. https://doi.org/10.5281/zenodo.4084763
CTS [13]	CoreTrustSeal Standards and Certification Board. (2022). CoreTrustSeal Requirements 2023-2025 (V01.00). Zenodo. https://doi.org/10.5281/zenodo.7051012
EOSC PID [41]	European Commission, Directorate-General for Research and Innovation, Hellström, M., Heughebaert, A., Kotarski, R., et al., A Persistent Identifier (PID) policy for the European Open Science Cloud (EOSC), Publications Office, 2020 https://data.europa.eu/doi/10.2777/926037
POSI [29]	Bilder G, Lin J, Neylon C (2020), The Principles of Open Scholarly Infrastructure, retrieved 08-11-2024, https://doi.org/10.24343/C34W2H
CARE [42]	Carroll, S.R., Garba, I., Figueroa-Rodríguez, O.L., Holbrook, J., Lovett, R., Materechera, S., Parsons, M., Raseroka, K., Rodriguez-Lonebear, D., Rowe, R., Sara, R., Walker, J.D., Anderson, J. and Hudson, M. (2020) 'The CARE Principles for Indigenous Data Governance', Data Science Journal, 19(1), p. 43. Available at: https://doi.org/10.5334/dsj-2020-043
DCAT-AP [43]	SEMIC. (2023). DCAT application profile for data portals in Europe (DCAT-AP), version 3.0.1. Publications Office of the European Union.

Label	Source of Information
	https://semiceu.github.io/DCAT-AP/releases/3.0.1
schema.org [44]	Schema.org. (n.d.). Dataset. In Schema.org vocabulary. Retrieved January 31, 2026, from https://schema.org/Dataset
NDSA [45]	Levels of Digital Preservation. https://ndsa.org/publications/levels-of-digital-preservation/
DPC RAM [46]	Digital Preservation Coalition (2024). Digital Preservation Coalition Rapid Assessment Model (DPC RAM). Version 3. http://doi.org/10.7207/dpcram24-03
DPC CRPS [47]	Digital Preservation Coalition (2022). Core requirements for a digital preservation system. Part of the DPC Procurement Toolkit. Mapping also available to DPC RAM. https://www.dpconline.org/digipres/implement-digipres/procurement-toolkit/procurement-toolkit-core-requirements
GORC [48]	Woodford, C., Treloar, A., Leggott, M., Payne, K., Jones, S., Lopez Albacete, J., Madalli, D., Genova, F., Dharmawardena, K., Chibhira, N., Åkerström, W. N., Macneil, R., Nurnberger, A., Pfeiffenberger, H., Tanifuji, M., Zhang, Q., Jones, N., Sesink, L., Wood-Charlson, E., & RDA GORC International Model WG. (2023). The Global Open Research Commons International Model, Version 1 (1.0). Zenodo. https://doi.org/10.15497/RDA00099
CESSDA [49]	Braukmann, R., Kvamme, T., Kleemola, M., Dolinar, M., & Alfredsson, I. (2023). D16 Landscape Workshop and Report (Version 1.0). Zenodo. https://doi.org/10.5281/zenodo.5554457
RISK [50]	Frank, R.D. (2024), "Constructing risk in trustworthy digital repositories", Journal of Documentation, Vol. 80 No. 6, pp. 1508-1527. https://doi.org/10.1108/JD-08-2023-0157
TRUST WG [51]	RDA/WDS Trust Principles Outreach and Adoption WG, https://www.rd-alliance.org/groups/rdawds-trust-principles-outreach-and-adoption-working-group/activity
ELIXIR [15]	Durinx C, McEntyre J, Appel R et al. Identifying ELIXIR Core Data Resources [version 2; peer review: 2 approved]. F1000Research 2017, 5(ELIXIR):2422 https://doi.org/10.12688/f1000research.9656.2
ERC-HE [52]	OAPEN, 2024. ERC Open Access requirements for FP7, Horizon 2020 and Horizon Europe grants. https://www.oapen.org/article/13934224-erc-oa-requirement
GREI [53]	Sonia, Lisa, & Helena. (2023). Generalist Repository Ecosystem Initiative Introductory Brochure. Zenodo. https://doi.org/10.5281/zenodo.8350509
ISO [6]	International Organization for Standardization. Audit and certification of trustworthy digital repositories. 2012. https://www.iso.org/standard/56510.html

Annexure B: TRSP Results and Recommendations

B.1 Major concerns with existing repository certification approaches to be addressed

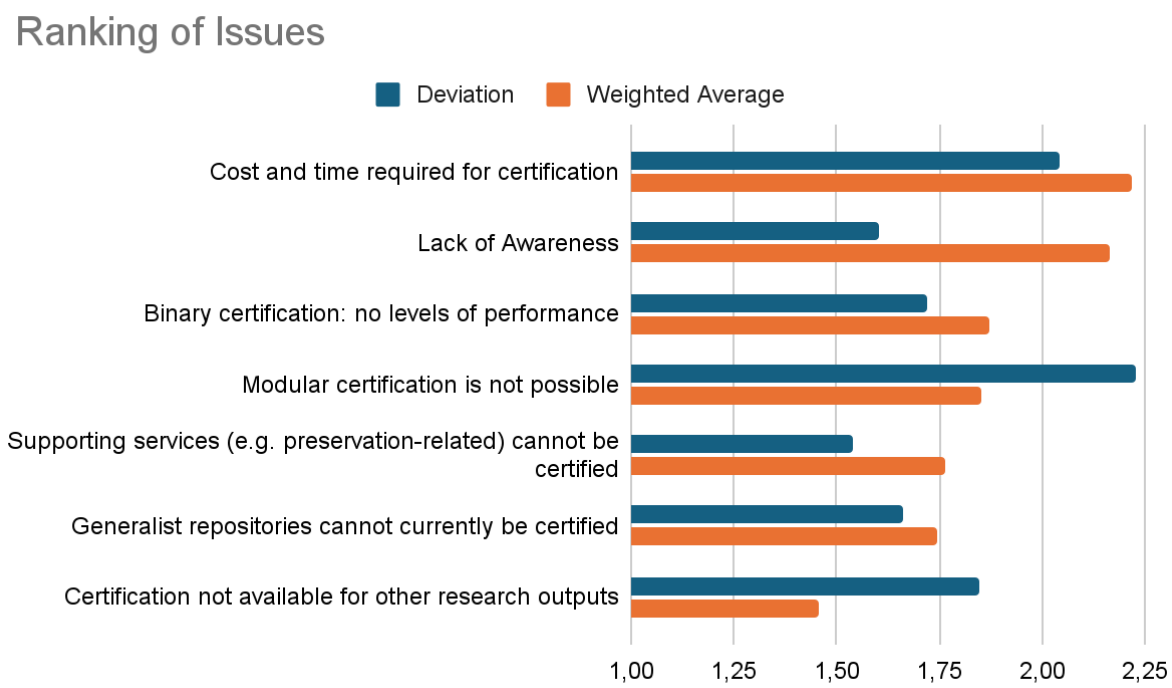


Figure B1. Ranking of issues identified by WG participants in Plenary 22.

Plenary 22 gathered community input on the major issues to be addressed, summarised in Figure B1. The main concerns were:

- **Cost and time required for certification**: all existing formal certification pathways required considerable investment of time and money to achieve, focused on a periodic event. While one could argue that a minimum level of care should be present in gathering and presenting evidence, these resource requirements also create a barrier to entry. *A gradual approach to gathering, presenting, and refining evidence may form part of the solution, as would modular (piecewise) assessment or certification, which was also highlighted as a major concern.*
- **Binary nature of certification**: respondents shared the perception that certification did not presently allow a gradual improvement in performance, and that one either conformed to the benchmark set by the certification authorities, or did not. *Defining maturity levels as benchmarks will go a long way toward addressing this concern.*
- **Some actors in the landscape cannot be certified**: Services to repositories (for example, long-term preservation services) cannot be certified in their own right, and generalist repositories are out of scope for certification by CoreTrustSeal, nestor, and ISO. On the one hand, generalist repositories often do not exhibit the required designated community focus or curation expertise, but on the other hand, they are in

widespread use without any mechanism for assessing quality or selecting the most suitable repository.

- **No mechanism for certification of other research outputs**: in practice, the obvious omission at the current time would be software, for which certified or assessed repositories are not available. This concern falls outside the scope of the TRSP WG, but remains important to the community. *Advocate and foster work in RDA to address this issue.*

B.2: Approaches to Appraisal/ Assessment and Certification

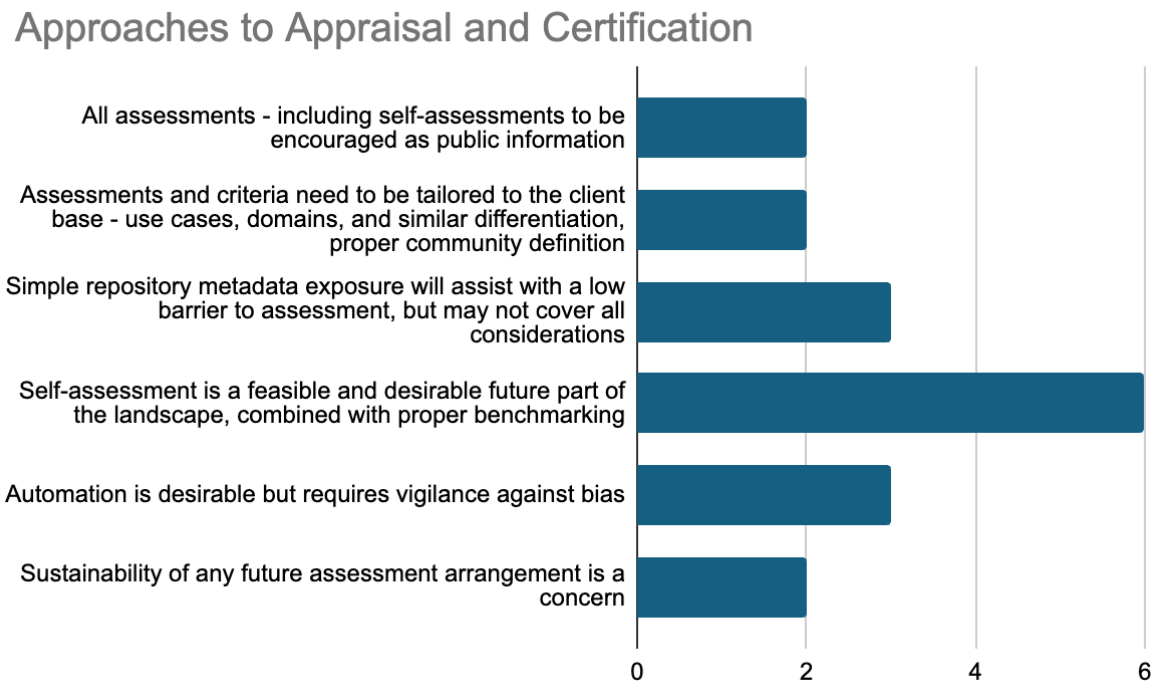


Figure B2. Community Ranking of Options and Characteristics of Appraisal and Certification in Plenary 22

Based on the community ranking in Figure B2, we conclude that:

- Self-assessment is a viable future option, provided that such assessments are also made public and can serve as a basis for appraisal of repository suitability for specific end user needs. *Self-assessment is more consistent when evaluated against a set of open community benchmarks, which may be challenging to compile and curate across multiple communities. Benchmarks are context-dependent, and each context will have a potentially different set. This aspect may interest and inform implementation possibilities in the EOSC EDEN and FIDELIS projects.*
- Automation has a role if it is properly managed and monitored. *This implies development of automated tests to determine or confirm the values associated with repository, service, and software package attributes, and comparing them to benchmarks. There is a danger of biases (more assessments available for machine-readable attribute sets, less focus on attributes that cannot be assessed automatically). Clearly, AI-based assessment workflows will be useful in some cases.*

B.3 Major Gaps in Assessment of Services

The first public engagement, held at the virtual plenary P22, identified and ranked several service characteristics that current repository certification or assessment approaches may not include or adequately emphasise. These are shown in Figure B3.

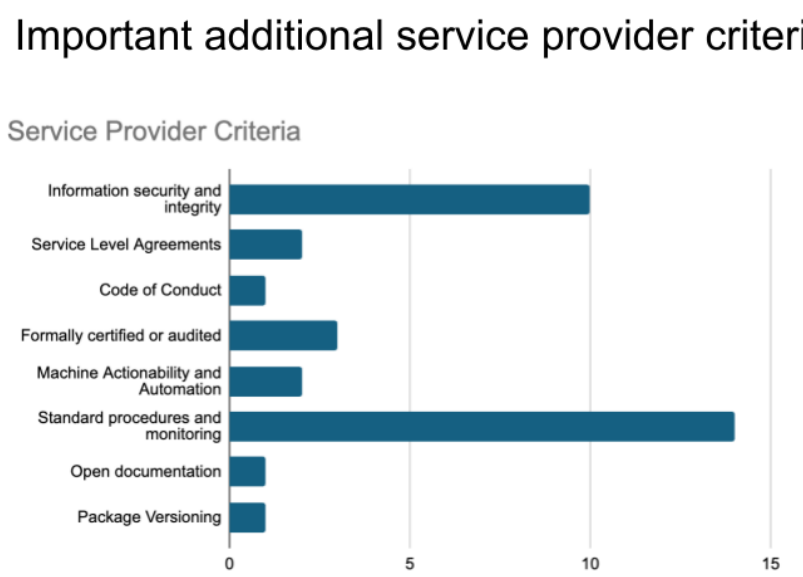


Figure B3. Criteria that apply to service providers in addition to repository criteria [22]

While all of these characteristics appear to be applicable, the most commonly identified ones deal with (1) Information security and integrity, and (2) documented procedures that are monitored for compliance. These are also explicitly included in the highly ranked characteristics confirmed in Community Consultation 2 [23]. *Service characteristics should be extended to include these two considerations.*

Figure B4 shows additional considerations raised in Community Consultation 1 that were not initially identified in preparation for the event, but identified and added by participants. The most important ones include (1) High-quality service documentation, and (2) turnaround time for processes such as submission and publication. *The latter is a complex objective, and while it is identified as a service characteristic to be shared transparently with the community, it is not easy to achieve in practice, since proper appraisal and curation of submitted content require time and effort. Automation of curation services becomes important in this context.*

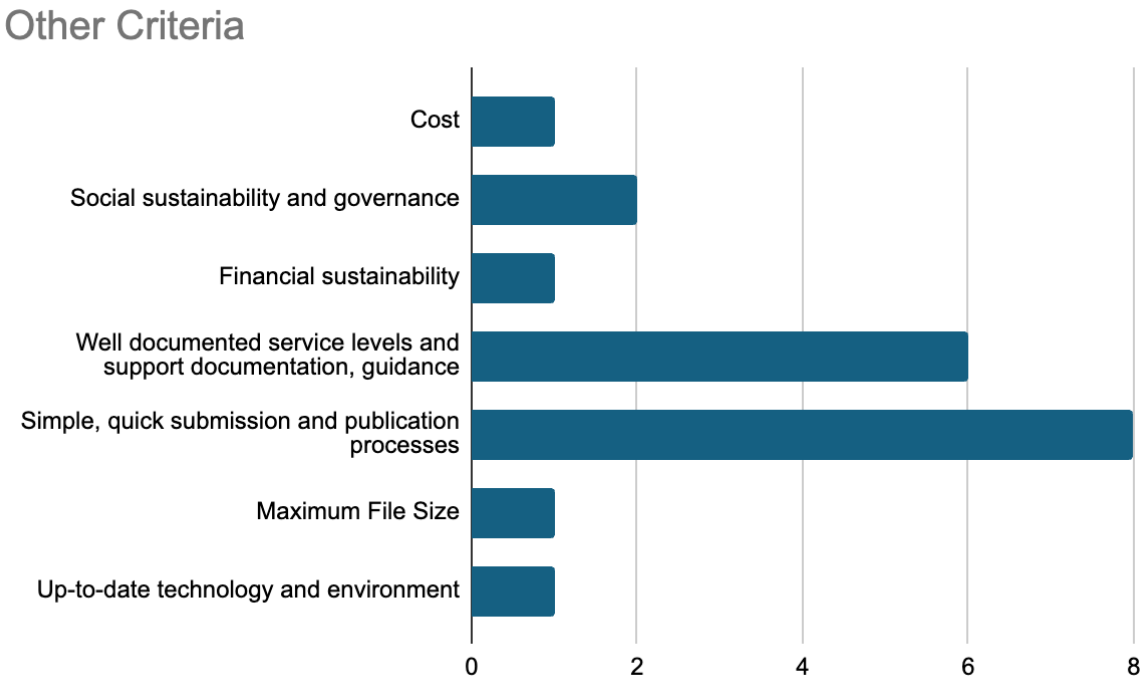


Figure B4. Additional criteria that apply to service providers as identified by participants [22]

B.4 Normative and Informative Characteristics

Community feedback at P22 identified that some characteristics are used to assess a repository or service, while others are used to transparently characterise a repository or service without judgment. At Plenary 24, the following was discussed and confirmed by the participants:

- **Normative characteristics** are used in assessments and certification, and can be specified and/ or standardised in respect of criteria, metrics, tests, benchmarks and performance levels, and assessment rubrics.
- **Informative characteristics** are used to select an appropriate repository or service based on end-user needs, and will be appraised differently in each case. Standardising these criteria makes it possible to select services objectively and potentially rank them.
- When an individual, project, institution, or community selects an appropriate repository or service:
    - They can mix and match normative and informative criteria
    - They can define their own metrics, tests, and benchmarks

B.5 Resolving Conflicts in Characteristics

Community Consultations 1 and 2 [22,23] focused on finalising the characteristics of services and software packages, and the results were presented for final confirmation in the third Community Consultation at Plenary 25 in Brisbane [28].

Annexure C: Verifying Assessments

Figure C1 describes the typical options available for verification of attributes ('asserted values' as defined by FAIR-IMPACT [27,54]).

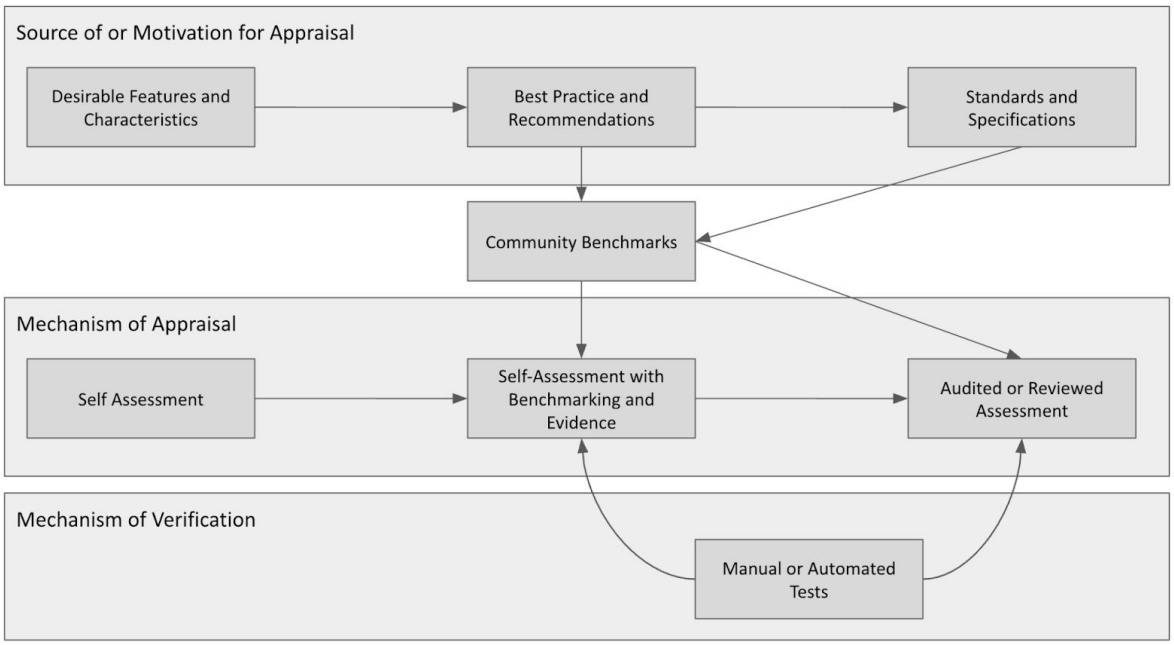


Figure C1. Mechanisms of Verification in Performance Appraisal

In the figure, the sources of and motivation for appraisal and its associated content is categorised as follows:

- The most broadly scoped source would be informal but widely recognised desirable features and characteristics of repositories. There are many sources of these attributes - for example, attributes defined by GORC, or the attributes defined by DRAWG.
- There are best practices and recommendations in respect of attributes, their definitions, and more importantly, what constitutes broadly accepted norms for the values of these attributes or the content of documentation provided as evidence that an attribute is available. As an example
    - An attribute may describe the metadata harvesting service(s) offered by a repository.
    - The attribute may be defined as ideally providing local API URLs for standardised API implementations, for example, by referencing a registry containing entries for common implementations such as OAI-PMH, a SPARQL endpoint, and CS/W.
    - Best practice or a recommendation might indicate that OAI-PMH is preferred for a specific context.

- Community benchmarks may further constrain the acceptable values for an attribute, for example by indicating that in order to be a part of the FIDELIS Network, an API endpoint for an OAI-PMH service must be indicated.
- Verifying the assertion that a specific endpoint has been implemented can be done via one of three mechanisms:
    - ***Self-assessment***, which does not require any additional verification of the assertion.
    - Self-assessment with ***public benchmarking and evidence***, for example by providing evidence that an OAI-PMH endpoint is functional by publishing availability data.
    - ***Assessment by a third party***, which involves audit or review of an assertion.
- The mechanism whereby an assertion can be verified can be one of several, which vary in respect of reproducibility. These mechanisms were analysed and defined in detail in the FAIRCORE4EOSC Compliance Assessment Model [55], and the options are defined in more detail below. Some of these verification mechanisms involve manual or automated tests and a metric. In the case of OAI-PMH endpoint verification, these might be:
    - A metric that measures whether the asserted endpoint conforms to the OAI-PMH specification, and whether it is available for harvesting with a minimum uptime.
    - Tests that determine OAI-PMH specification compliance.
    - Tests that determine availability.
    - The benchmark could be:
        - Specification compliance: Go/ No Go, i.e. the metric fails if the endpoint is not specification-compliant.
        - If it is compliant, the second part of the benchmark determines if availability is equal to or exceeds a norm, for example 98% uptime on a moving annual basis.

Not all attributes are verified by reproducible and properly documented tests, and the options described in Table C1 have been identified in the FAIRCORE4EOSC CAT Model. Suggested refinements are shown in purple text.

Table C1. Metric Typology and Typical Benchmarks

Metric Type	Description	Approach to Metric Definition	Typical Benchmark
Open Review	No guidelines are present, and reviewers make a completely subjective and independent conclusion about performance.	The metric is undocumented, the reviewer makes a subjective 'measurement' of performance	The assessor determines whether performance is acceptable or not based on tacit knowledge and experience.
Guided Review	Guidance on how to approach assessment of compliance is available	The metric is documented in the sense that the assessor is advised on which considerations are in scope for a subjective evaluation of performance, and the expected result is not always	The assessor determines whether performance across the typical considerations is acceptable or not based on knowledge and experience and interpretation of the guideline.

Metric Type	Description	Approach to Metric Definition	Typical Benchmark
		documented.	
Benchmarked Review	As for guided review, but it is possible to select a level of compliance by matching with described performance or examples	The metric is documented in the sense that the assessor is advised on which considerations apply to a subjective evaluation of performance ~~and the result is not always documented~~. It is possible to map a subjective assessment to a defined level of performance or maturity	The benchmark describes which of the considerations are considered to be important, non-negotiable, or optional, and the assessment is made by the assessor based on experience and mapping of subjective considerations to the benchmarks - which may describe recommended or best practices.
Subjective Ranking	Assessment by assigning a ranking to a compliance claim or description (subjectively). Often employed when assessment is competitive - for example for grant applications.	The metric is documented in the sense that the assessor is presented with one or more considerations and ranks them subjectively.	The assessor determines whether performance across the typical considerations is acceptable or not based on tacit knowledge and experience.
Binary	True or false, for example by determining whether there is evidence supporting a compliance claim	The metric is documented, based on reproducible tests, and it is clear what will constitute a true or false result when considering performance across one or more tests.	The benchmark determines whether performance is acceptable, but it is often a trivial case - true being acceptable ('Pass'), and false being unacceptable ('Fail'). A benchmark may be more applicable in cases of multiple tests for the same metric.
Measured or Computed Value	Measuring objectively using an instrument and/ or a method (test), result is a defined variable - for example 'number of employees'	The metric is documented, including reproducible tests, and it is clear how a value will be computed for performance across one or more tests.	The benchmark determines whether performance is acceptable, often with a mapping to benchmark categories.
Composite Assessment	Aggregation of a collection/ hierarchy of weighted and normalised measures. Includes ranking, multicriteria analysis, and analytic hierarchy methods.	A mechanism is provided whereby a metric is composed of other metrics and/ or tests, and the combination of results is based on some form of weighted aggregation. Simple methods sum the results over several tests and/ or metrics and implicitly weight all equally.	The benchmark determines whether performance is acceptable, often with a mapping to benchmark categories.

Metric Type	Description	Approach to Metric Definition	Typical Benchmark
Objective Ranking	Ranking against peers through quantitative methods, e.g. pairwise comparison	The test method assumes that all instances of a population are measured together, or measurements for all exist. By comparing an individual instance against each other instance and selecting the best performing instance, an objective ranking is obtained. Pairwise comparisons are also often combined for more than one assessor or observer.	The benchmark determines whether performance is acceptable, often with a mapping to benchmark categories.
Classification	Supervised or unsupervised classification based on ML mechanisms or heuristics	A number of test values or characteristics of a subject are combined into a classification heuristic, often by developing such a heuristic from learning examples. Neural networks for classification are one example of such an approach.	The benchmark determines whether performance is acceptable, often with a mapping to benchmark categories.

Not all of these approaches produce reproducible outcomes, and while reproducibility (by a third party) is ideal, it may not be necessary in all circumstances. Transparency (how an outcome was reached) may also be required in many instances. With these considerations in mind, some approaches listed above are less appropriate.

Moreover, not all approaches are automatable or machine-actionable, and because scalability is a major bottleneck in quality assurance processes, automated approaches are more attractive.

Based on these considerations, Table C2 summarises our classification of the approaches in Table C1.

Table C2. Metric Typology and Design Considerations

Metric Type	Reproducibility	Transparency	Automation
Open Review	Low	Low	No
Guided Review	Low	Low	No
Benchmarked Review	Medium	Medium	No
Subjective Ranking	Medium	Medium	No
Binary	High	High	Yes
Measured or Computed Value	High	High	Yes
Composite Assessment	High	High	Yes
Objective Ranking	Medium	High	Maybe
Classification	High[5]	Medium	Yes

[5] Depending on model quality and training

Annexure D: Community Consultation and Collaboration

D.1 Community Consultation Processes

The TRSP working group has identified three profiles (subsets) of the inventory of attributes described in Annexure B. These are:

1. Attributes that are applicable to **service providers to repositories**. Examples of such services include long-term preservation services (as offered by Arkivum and others), FAIR assessment (e.g., F-UJI, FAIR-EVA, Fair Champion, …)
2. Attributes that are applicable to **software packages used by repositories** - such as Dataverse, CKAN, DSpace, and Invenio.
3. Attributes that apply to one of the categories above, but can be **transferred to the repository** using the service or platform once an assessment or certification is available for the attribute (‘inherited’).

The community consultation process involved three rounds of engagement at RDA plenaries, as follows:

1. At the P22 (virtual), we asked the participants to assist with identification of the main concerns that the community had in respect of existing certification options, scope, and processes.
2. At the P23 in San José, Costa Rica, where the community provided a first round of allocation of attributes to the three profiles that the TRSP has defined, and we identified, in interactive sessions, whether the scope of attributes identified, landscape analysis inputs, and classification were adequate or required extensions.[22]
3. At the P24 (virtual), the consultation focused on confirming the allocation of attributes to the profiles [23].
4. At the P25 in Brisbane, Australia, the final recommendations and profiles based on the previous engagements were shared for comment and refinement, and remaining conflicts between the three sets of attributes (profiles) were resolved by consensus [28].

D.2 Collaboration with the EOSC EDEN and FIDELIS Projects

The EOSC EDEN project [56] (grant agreement nr.101188015) seeks to enhance digital preservation strategies at the European and national levels. EDEN will create a comprehensive framework for identifying which data are candidates for digital preservation. This involves setting standards and protocols for long-term data preservation, based on an assessment of data usage, quality, and its benefits to science and society.

In addition to providing a framework for making informed digital preservation decisions, the

EOSC EDEN project aims to develop a model for re-appraising data throughout its lifecycle. The model's usability and practicality will be assessed through relevant communities (early adopters), which will also help develop tools and services to automate certain preservation actions. The re-appraisal model will support the digital preservation framework by ensuring preservation efforts remain relevant over time.

EOSC aims to develop a web of FAIR (Findable, Accessible, Interoperable, Reusable) data and services for science in Europe. The FIDELIS project [56] (grant agreement no. 101188078) will enhance the sustainability of EOSC by establishing a European network of healthy, vibrant and self-sustaining trustworthy digital repositories (TDRs) while fostering harmonisation and interoperability across repositories. It will provide a framework to support repositories in becoming and remaining trustworthy and FAIR-enabling over time. FIDELIS also contributes to upskilling repositories and expanding the TDR network by offering a series of training and financial support programmes.

The EDEN project will use the TRSP WG Attribute inventory to populate and cross-reference an attribute registry that is linked to repositories and services via 'profiles.' The conceptual model proposes a structure that has three sets of profiles:

- A ***standard profile***, which highlights the minimum mandatory characteristics that should be exposed by a repository, whether these must be public, may be public, or must not be public (i.e. private).
- One or more ***community profiles***, which can extend the standard profile properties and add scope constraints, but not remove constraints. The CoreTrustSeal criteria, for example, can be encoded as such a collection of characteristics. For this to be possible, a community profile must also include properties such as benchmarks and indicate the verification mechanism.
- One or more ***repository (actor) profiles***, which advertise characteristics available for a repository or service, including aspects such as whether they are publicly or privately available, and how frequently these are updated. These profiles can also add properties to the standard profile and constrain the scope of applicable characteristics.

Assessments and appraisals, including those required for compliance assessment, can be formulated from these three sets of profiles.

Table D2.1 describes the scope of contributions from the TRSP WG, and the EDEN and FIDELIS projects.

Table D2.1. Scope of Contributions

Initiative	Standard Profiles	Community Profile(s)	Profiles	Main Attributes
TRSP WG	Trustworthy Repositories, Services, Software	TRUST, POSI, CTS, FAIRsharing, re3DATA, GORC, DPC, FAIR, EOSC	None	Cardinality, Description, Annotations, Normative/ Informative, Inheritable,

Initiative	Standard Profiles	Community Profile(s)	Profiles	Main Attributes
		PID Policy, CTM, DRAWG, CARE, NDSA, TRSP		References
EOSC EDEN	None	schema.org EDEN Project DCAT-AP CPP	Adds specific service profiles, FIDELIS Network	Linked URIs, Annotations, References
EDEN FIDELIS	None	TTRAM	Adds FIDELIS Network repositories	FIDELIS Benchmark Values, Semantics of FIDELIS-related attributes

D.3 Formal Feedback

Formal feedback has been requested from the following projects and organisations:

- CoreTrustSeal
- World Data System
- FAIRSharing
- Re3data
- COAR
- EOSC EDEN project
- EOSC FIDELIS project
- RDA/WDS Certification of Digital Repositories IG