DPC RAM & CoreTrustSeal: Initial Analysis

Introduction

This paper consists of an initial response to the first version of the Digital Preservation Coalition's (DPC[1]) Rapid Assessment Model[2] (RAM) released in September 2019. This is not a detailed critical analysis of this archive maturity self-assessment based on the DPC adaptation of Adrian Brown's approach[3]. The RAM is new and explicitly subject to further testing and revision based on the experience of DPC members. With the exception of the discussion of maturity levels and the conclusion this paper predominantly follows the structure of the RAM paper[4].The intention is to provide an initial 'compare and contrast' between two sets of criteria which, though related, have different purposes and scopes.

Jenny Mitcham and Paul Wheatley from the DPC provided detailed and thoughtful clarifications and feedback on the first draft, many of which have been used to amend and improve the text. This text will be used as input for discussion of the RAM at the CoreTrustSeal[5] Board and into the FAIRsFAIR project which is looking at the application of maturity to the CoreTrustSeal requirements with a particular focus on identifying how repositories can enable the FAIR[6] data principles.

If well adopted and consistently applied it might go beyond a beneficial self-assessment tool and offer an opportunity for analysis of what different practitioners consider 'appropriate' evidence. Alongside the ongoing CoreTrustSeal certifications this could help lead to a more concrete understanding of what the data management, repository, archiving and preservation practitioners (and their users) consider 'best practice'.

[1] https://www.dpconline.org/
[2] https://www.dpconline.org/our-work/dpc-ram
[3] http://www.facetpublishing.co.uk/title.php?id=047555#.XZX8OUZKiUk
[4] https://www.dpconline.org/docs/miscellaneous/our-work/dpc-ram/2006-dpc-ram-v-1-0/file
[5] https://www.coretrustseal.org/
[6] https://www.nature.com/articles/sdata201618

Introduction 1
Resources 3
Digital Preservation Coalition Rapid Assessment Model 3
Overview 3
Origins and Acknowledgements 3
Explanation of terms 3
Guiding Principles 4
How to Use This Model 5
Benefits of Use 6
Benefits for DPC Members 6
Note on Scope 7
RAM and CoreTrustSeal 7
A. Organizational viability 8
B. Policy and strategy 8
C. Legal basis 9
D. IT capability 9
E. Continuous improvement 9
F - Community 10
G. Acquisition, transfer and ingest 10
H. Bitstream Preservation 11
I. Content preservation 11
J - Metadata management 12
K - Discovery and access 12
Maturity Levels 13
Conclusions 16

Resources

https://www.dpconline.org/blog/a-dpc-maturity-model-for-digital-preservation
https://www.dpconline.org/our-work/dpc-ram
https://www.dpconline.org/docs/miscellaneous/our-work/dpc-ram
Which includes:
https://www.dpconline.org/docs/miscellaneous/our-work/dpc-ram/2006-dpc-ram-v-1-0/file
https://www.dpconline.org/docs/miscellaneous/our-work/dpc-ram/2005-dpc-ram-worksheet/file
(direct download of worksheet)
https://www.coretrustseal.org/wp-content/uploads/2017/01/20180629-CTS-Extended-Guidance-v1.1.pdf

Digital Preservation Coalition Rapid Assessment Model

Overview

- "Designed to enable a rapid benchmarking of an organization's digital preservation capability whilst remaining agnostic to solutions and strategy"
- "Enable organizations to monitor their progress as they develop and improve their preservation capability and infrastructure and to set future maturity goals"
- "DPC Members will also be offered the opportunity to share their results and compare their progress with other members of the Coalition"
- "Providing DPC staff with an efficient, continuous and standardized approach to capturing information on member needs and issues."

Origins and Acknowledgements

"*Primarily based on Adrian Brown's Digital Preservation Maturity Model. It was also informed by the NDSA Levels of Preservation, the Digital Preservation Capability Maturity Model (DPCMM), the Assessing Organisational Readiness (AOR) Toolkit and the CoreTrustSea*l." DPC RAM was created in conjunction with the Nuclear Decommissioning Authority.

Explanation of terms

The Guiding Principles include the statement "*Many of the existing maturity models target particular domains (e.g. data repositories as in the CoreTrustSeal)*" but the 'explanation of terms' section notes that "*The term 'Digital Archive' is used throughout the DPC RAM to refer to a facility where content in digital form with enduring value is stored and managed for long term Preservation*", which also seems to be a reasonable definition of a candidate for the CoreTrustSeal.

“The term ‘Organization’ is used through the DPC RAM to refer to the unit of an organization that is being measured. Typically this will be a specific section of an organization that has a remit to manage and preserve digital content, but in some instances it may be appropriate to look at the organization as a whole. Each institution using this model will need to establish first which part of their organization they are measuring.”

For internal self-assessments it may be sufficient for participants to have a general understanding of the intended scope but for more formal and external assessments it’s particularly important to understand the scope of the applicant, The CoreTrustSeal seeks to ensure that the right parts of the organisation (and only those parts) are certified as ‘trustworthy’. But organisational boundaries can be hard to define, especially in the realm of organisational archives, university hosted repositories and complex preservation partnerships which may include third party vendors of software and services.

The self-assigned organization boundary for RAM simplifies things for the self-assessor but could reduce comparability of results across digital archives. The DPC acknowledges this but their priority is to encourage use by their members by making it flexible.

Guiding Principles

This section opens by contrasting the RAM with CoreTrustSeal (too repository focussed), the NDSA Levels (too tech focussed) or the DPCMM (too focussed on open formats and migration). The RAM is intended to apply across all organisational missions, scales and approaches. But how this differs from the CoreTrustSeal is not fully defined.

“This model aims to be:
- *Applicable for organizations of any size and in any sector*
- *Applicable for all content of long-term value*
- *Preservation strategy and solution agnostic*
- *Based on existing good practice*
- *Simple to understand and quick to apply”*

The breadth of the aims here suggests that there are two primary reasons for changing terms and definitions used for items A to K:
1 To align with updated good practice.
2. To make it simpler to understand or quicker to apply.

But the DPC can also see the potential to broaden its scope in response to ongoing use, e.g. if changes might make it more applicable for web archiving or software preservation

The ‘comments’ section acknowledges that the maturity level examples will be more dynamic as they “*may be updated and enhanced over time in line with developments in the field and in response to feedback from DPC Members and the wider digital preservation community*.”

How to Use This Model

“This model should be used as a rapid benchmarking tool, enabling a quick and simple assessment which can be applied frequently with minimal effort and consultation across an organization”.

The outcomes of real world application may differ from the testing process. The results of a maturity self-assessment can have implications for reputations or create demands for expenditure. Both of these factors could reduce speed and increase the demand for consultation in future applications of the RAM.

The footnote to this statement says: “*Early testing of the model suggests that the basic assessment can be carried out in less than two hours by someone with good knowledge of digital preservation and how it is applied in their own organization. For others it may take longer, particularly if multiple stakeholders need to be consulted. Setting future goals and priorities is likely to be a longer process*”

It would be useful to monitor how many candidates identify a single person with “good knowledge of digital preservation and how it is applied in their own organization” and the scale of those organisations. Beyond ‘early testing’ it will be interesting to see how consistent and comparable the outcomes of a two hour process are. It might be assumed that organisations which are already somewhat managed/optimal have the culture and information management systems in place to make the assessment process more rapid.

“It is expressly not a strict and comprehensive certification tool that might provide a "deep dive" assessment”

This acknowledges the differences between a formal certification process and the RAM, which DPC see as more aligned with something like the NDSA levels in terms of how people will use and apply it internally. DPC are adding some formality to the RAM assessment by coordinating and encouraging the assessment periodically and collecting the results, but are not certifying the results.
It would be useful to explore what DPC would consider sufficient to be ‘strict’, ‘comprehensive’ or ‘deep dive’ and to look at whether the CoreTrustSeal meets those expectations.

“*This should be an honest and realistic assessment*“

The CoreTrustSeal acknowledges that there will always be limitations to an evaluation process which does not directly inspect a repository and the objects it holds. Part of the CoreTrustSeal mitigation for this is to ensure transparency through public self-assessment statements with evidence links. “Trust” in the self-assessor remains a feature of the DPC RAM.

Benefits of Use

“Are there any gaps in our organization’s preservation capabilities? “

> Implies that these gaps can be identified by applying the model.

“How close is our organization to reaching the level of preservation maturity we would like?”

> The self-assessor can set internal targets for improvement, but the model does not assign any minimum levels for preservation maturity.

“What should the priorities be for improving our organization’s preservation capability?”

> Implies that the model helps with prioritisation, presumably by seeking to attain the next preservation level. A priority column was removed from the release version of the RAM as it was causing confusion during testing. In ‘What to do after DPC RAM’ users of the model are encouraged to prioritise and schedule actions as a follow on exercise (https://www.dpconline.org/our-work/dpc-ram/what-to-do-after-dpc-ram)

“What support and resources do we need in order to help our organization move forward?”

> This segues into the benefits of DPC membership, but may underplay the complexity of addressing gaps and prioritisation, especially for readers who are not DPC members and therefore do not have access to the password protected ‘level up’ content.

Benefits for DPC Members

“How does my organization’s digital preservation maturity compare with that of the wider DPC membership?
How does my organization’s digital preservation maturity compare with that of similar institutions within the DPC?”

There are challenges to effective comparison of results without an understanding of the digital archive’s collection (digital object characteristics) or of the community it serves. In their online form the DPC ask for some basic information on the type of content, size of content, size of organisation and scope of the assessment to support easier comparison.

Note on Scope

"This model specifically excludes IT security issues. Whilst considered extremely important from a capability and resilience standpoint, it is an area that is already well-served by existing IT security guidance (for example the ISO/IEC 27000 family of standards). It was also felt that the results of an assessment against such criteria could in itself be sensitive or confidential."

To exclude something from a preservation assessment that is 'extremely important from a capability and resilience standpoint' is a significant choice. Given the increased attack surface presented by complex, networked IT systems in the internet age it seems hard to evaluate IT capability (D. Information Technology "capabilities for supporting digital preservation activities") without a security component. Though without relevant contextual questions about the data collections (e.g. presence or absence of personal data) it would be challenging to design security maturity levels.

The results of such a self-assessment could indeed be sensitive or confidential. The CoreTrustSeal requirements may be used to self-assess against the security criteria (R16). Though applications are confidential until successful the CoreTrustSeal Board are unlikely to receive applications from organisations whose self-assessments suggests their information security is insufficient to protect their data. There is an acknowledged weakness in agreeing minimum (technical) standards for data protection. It's not convincing to say that existing IT security guidance serves digital archives regardless of their mission, scale and approach. Reaching and maintaining an ISO27000 level of information security is complex, and any ISO-compliant audit and certification regime is costly. The CoreTrustSeal does not claim to have identified ideal practice for core information security assessments so perhaps there is room for cooperation with the DPC even if this is outside the RAM process.

RAM and CoreTrustSeal

Though the RAM overview says that the "model provides a set of **organizational**, **technical** and **functional** criteria" these terms aren't clarified and the criteria aren't mapped to them.

The top tiers for the 11 criteria within the RAM are:
Organizational capabilities, Service capabilities

For CoreTrustSeal[7] top tiers for the 16 Requirements are:
Organisational Infrastructure, Digital Object Management, Technology
CoreTrustSeal also asks some specific context questions (R0: repository type, designated community definition, level of curation, outsource partners). There are some related questions in the DPC RAM online form, but these aren't integrated into the criteria document.

[7] https://www.coretrustseal.org/why-certification/requirements/
https://public.ccsds.org/pubs/652x0m1.pdf

A. Organizational viability

“Governance, organizational structure, staffing and resourcing of digital preservation activities”

A strong alignment with:

> **R5. Organizational infrastructure** “The repository has adequate funding and sufficient numbers of qualified staff managed through a clear system of governance to effectively carry out the mission.”

But nothing explicit to support:

> **R3. Continuity of access**. “The repository has a continuity plan to ensure ongoing access to and preservation of its holdings”

Which addresses business continuity, disaster recovery and succession planning.

And it doesn’t go as far as:

> **R1. Mission/Scope** “The repository has an explicit mission to provide access to and preserve data in its domain”.

B. Policy and strategy

“Policies, strategies, and procedures which govern the operation and management of the digital archive”

Policies and strategies are implied or explicitly required as evidence across multiple CoreTrustSeal requirements but not addressed at the top level. Procedures are addressed through:

> **R12. Workflows.** Archiving takes place according to defined workflows from ingest to dissemination.

RAM examples for ‘optimized’ include ‘policy, strategy and procedure is proactively monitored and updated to reflect internal changes, changes in other policies, or other external factors’. But this could be considered as a more basic requirement for any ‘managed’ change in response to internal and external, technical and community factors i.e. preservation. It’s also a dependency for continuous improvement (E).

C. Legal basis

“Management of contractual, licensing, and other legal rights and responsibilities relating to acquiring, preserving and providing access to digital content (e.g. licencing, copyright, terms and conditions of use, data protection regulation).”

A strong alignment with:

> **R2. Licenses**. “The repository maintains all applicable licenses covering data access and use and monitors compliance”

In CoreTrustSeal there’s also an element of ‘right to preserve’ under preservation plan. But current and future revisions of CoreTrustSeal aim to contain all rights issues under R2.

One RAM example of 4-Optimized is “*The organization engages with and inputs into legal and judicial processes that create regulation*”. This may be hard for a smaller scale organisation to meet, but the DPC makes it clear that bulleted examples are not intended to be universally applicable.

D. IT capability

“Information Technology capabilities for supporting digital preservation activities.”

A strong alignment with:

> **R15. Technical infrastructure**. “The repository functions on well-supported operating systems and other core infrastructural software and is using hardware and software technologies appropriate to the services it provides to its Designated Community.”

CoreTrustSeal also includes security, which is explicitly excluded by the RAM.

> **R16. Security.** “The technical infrastructure of the repository provides for protection of the facility and its data, products, services, and users.”

E. Continuous improvement

“Processes for the assessment of current digital preservation capabilities, the definition of goals and the monitoring of progress.”

Continuous improvement over time, including responsiveness to changes in community best practice are assumed by the CoreTrustSeal. This can be addressed by making the guidance more explicit over time (e.g. the expectation of persistent identifier use becomes stronger as PID systems become available). But there are no specific CoreTrustSeal Requirements which test the concept of continuous improvement.

None of the RAM maturity levels for continuous improvement refers to meeting the needs of data users though they are noted in some examples elsewhere e.g. K. Discovery and Access: "The user community is proactively consulted to establish and anticipate needs and expectations." In contrast the designated community aspect of the CoreTrustSeal means reviewers are always seeking evidence which demonstrates responsiveness to changes in the data users' needs.

The inclusion of E continuous improvement as a top tier criterion also calls into question the interpretation of 'Optimizing' (the top maturity tier), which in many maturity approaches (e.g. CMMI[8]) includes an expectation of continuous improvement. This doesn't mean that the decision isn't valid or that the two can't co-exist, but might benefit from some explanation to self-assessors (see Maturity Levels below).

F - Community

"Engagement with and contribution to the wider digital preservation community."

A strong alignment with:

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

The CoreTrustSeal requirement goes beyond an expectation that the applicant interact with the 'preservation' community and explicitly includes expertise in the data themselves.

G. Acquisition, transfer and ingest

Processes to acquire or transfer content and ingest it into a digital archive.

A strong alignment with:

> **R8. Appraisal.** The repository accepts data and metadata based on defined criteria to ensure relevance and understandability for data users.

Transfer and Ingest are assured through:

> **R12. Workflows.** Archiving takes place according to defined workflows from ingest to dissemination.

[8] https://cmmiinstitute.com/learning/appraisals/levels

H. Bitstream Preservation

“Processes to ensure the storage and integrity of digital content to be preserved.”

A strong alignment with:

> **R9. Documented Storage Procedures.** The repository applies documented processes and procedures in managing archival storage of the data.

With the integrity aspect addressed alongside authenticity (provenance) in:

> **R7. Data Integrity & Authenticity.** The repository guarantees the integrity and authenticity of the data.

The CoreTrustSeal uses R7 to address the management of intended changes through authenticity (provenance) and the avoidance of unintended change through integrity measures. R9 refers to the curation teams’ expertise in ensuring appropriate storage processes during deposit, curation and access, which are supported by **technical infrastructure (R15)**. The term bit-stream ‘preservation’ is common within preservation-focussed circles, but in most data management and technical infrastructure terms it’s the basic assurance of integrity for data in movement (transfer) or at rest (storage).

I. Content preservation

“Processes to preserve the meaning or functionality of the digital content and ensure its continued accessibility and usability over time.”

As the primary duty of a trustworthy digital repository content preservation is addressed across several CoreTrustSeal requirements. The evaluation, assurance, and communication of content preservation is sought at **Appraisal (R7)**, during curation (**R11. Data Quality**) and **Data Reuse (R14).**

It might be important to explore the intended scope of ‘usable’ in the RAM to identify whether it includes ensuring data remain understandable. There is no reference to data users and most, if not all examples could be undertaken through a fully automated process once file format risks are identified. Content preservation mentions “meaning or functionality” but none of the provided examples explore the implications of “meaning”.

J - Metadata management

“Processes to create and maintain sufficient metadata to support preservation, management and use of preserved digital content.”

The CoreTrustSeal assumes that the description, and management of data is dependent on (object, or administrative) metadata throughout, with specific references under **R7 Data Integrity and Authenticity**, **R8 Appraisal**, **R9 documented storage procedures**, **R11 Data Quality**, **R13 Data Discovery and Identification**, and **R14 Data ReUse**.

The centralisation of all metadata in RAM supports a clear maturity score, but could hide some weaknesses at different points in the self-assessment.

The J criterion is explicit that metadata should “support [ ] use” and the examples have one reference to users at the ‘4. Optimized’ level: “*Metadata enables a richer rendering/reuse experience for the user*”. But the focus remains on delivery rather than engagement. Some of this is addressed under K, discovery and access, but K does not explicitly address ‘use’.

K - Discovery and access

“Processes to enable discovery of digital content and provide access for users.”

The strongest alignment with discovery is:

> **R13. Data Discovery and Identification**: “The repository enables users to discover the data and refer to them in a persistent way through proper citation.”

In CoreTrustSeal access forms part of **R1. Mission**, access rights are managed through **R2 Licences**, while **R3 Continuity of Access** addresses access where business continuity is threatened. Appropriate limitations on access are covered by **R4. Confidentiality & Ethics**.

RAM K. Discovery and Access caveats examples with “where access rights permit”. Without some understanding of the data (and the users seeking access) it is challenging to evaluate the maturity of access management systems in terms of data protection (cf. the RAM exclusion of security). Some insights should be provided by the responses to C. Legal Basis.

Maturity Levels

The CoreTrustSeal uses a self-assessed compliance level:
0 – Not applicable
1 – The repository has not considered this yet
2 – The repository has a theoretical concept
3 – The repository is in the implementation phase
4 – The guideline has been fully implemented in the repository

Noting: "*Compliance levels provide a useful part of the self-assessment process, but all applicants will be judged against statements supported by appropriate evidence and not against self-assessed compliance levels. In this regard, if the applicant believes a Requirement is not applicable, the reason for this must be documented in detail. Note also that compliance levels 1 and 2 can be valid for internal self-assessments, while certification may be granted if some guidelines are considered to be at level 3—in the implementation phase—since the Requirements include an assumption of a repository's continuous improvement*."

Compliance level zero here is arguably on a different scale from 1-4.

The origins of maturity approaches go back to the CMM Software[9] work

1: Initial	2: Repeatable	3: Defined	4: Managed (Capable)	5: Optimizing (Efficient)

ITIL[10], with a focus on IT service management, still uses these levels[11], but the successor to the CMM is the Capability Maturity Model Integration CMMI[12] (levels of capability and performance[13]) last updated in 2018.

0: Incomplete	1: Initial	2: Managed	3: Defined	4: Quantitatively Managed	5: Optimizing

In Adrian Browns Practical Digital Preservation (2013[14]) which forms the basis of the RAM the maturity levels are integrated into a vision which adds the notion of a 'roadmap' to support progress from the 'awareness' levels to the 'capability' levels.

[9] https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=11955
[10] https://www.axelos.com/best-practice-solutions/itil
[11] https://www.tsoshop.co.uk/gempdf/ITIL_Maturity_Model_v1_2W.pdf
[12] https://cmmiinstitute.com/
[13] https://cmmiinstitute.com/learning/appraisals/levels
[14] http://www.facetpublishing.co.uk/title.php?id=047555#.XYNp2yhKiUk

Table 4.9 Maturity levels

Stage	Maturity level	Description
Awareness	0 No awareness	The organization has no awareness of either the need for the process or basic principles for applying it.
	1 Awareness	The organization is aware of the need to develop the process, and has an understanding of basic principles.
	2 Roadmap	The organization has a defined roadmap for developing the process.
Capability	3 Basic process	The organization has implemented a basic process.
	4 Managed process	The organization has implemented a comprehensive, managed process, which reacts to changing circumstances.
	5 Optimized process	The organization undertakes continuous process improvement, with proactive management.

The DPC Rapid Assessment Model[15] removes the explicit awareness/capability distinction, noting that "the maturity levels are based on existing good practice and try to be agnostic to particular preservation strategies or approaches".

0: Minimal Awareness	1: Awareness	2: Basic	3: Managed	4: Optimized

It's tempting and logical to reduce the number of possible 'scoring' tiers in an assessment method. It makes the assignment process faster and simplifies later analysis. There may be valid reasons, supported by evidence, for not aligning with the CMMI but these are not discussed in the RAM model. The RAM scale measures two types of maturity: institutional awareness about the existence/need for a capability (minimal/aware) and the maturity of institutional capability (Basic, Managed and Optimized).

Within the DPC member ecosystem this may have limited impact, at least initially. But the topic of maturity assessment and improvement is very active. It has been investigated by CoreTrustSeal, forms part of the FAIR data work through projects like FAIRsFAIR and the RDA FAIR Maturity Working Group[16] and elsewhere (AIDA[17], NDSA Levels of Digital Preservation[18], DPCMM[19]). All these examples are closely associated with the data archiving and preservation community, there are other models across the wider data management and information technology sectors. This is not to imply that CMMI is the only possible maturity scale. These models all have varying levels of alignment with the CMMI approach which may be perfectly justified in their local context, but taken together may present a confusing picture.

[15] https://www.dpconline.org/our-work/dpc-ram
[16] https://www.rd-alliance.org/groups/fair-data-maturity-model-wg
[17] https://permalink.lanl.gov/object/tr?what=info:lanl-repo/lareport/LA-UR-11-11458
[18] https://ndsa.org//activities/levels-of-digital-preservation/
[19] https://coptr.digipres.org/Digital_Preservation_Capability_Maturity_Model_(DPCMM)

Applying an evaluation processes is not without cost (both for implementation and for addressing the outcomes) and a wide variety of scoring mechanisms will limit the number of models an organisation can adopt, and will limit the comparability of the potentially valuable assessment information they provide.

One possible benefit of using approaches which include the idea of “Quantitatively Managed” (CMMI level 4) is that such a (business) data-driven approach can be a useful precursor to defining the requirements for machine-actionability and automation of processes.

As noted above, continuous improvement often forms part of the top tier of maturity: optimized. Continuous improvement is implied by some examples of optimized on the RAM scale but the criteria also address the topic separately. This follows on from the DPC design decision to remove the ‘one-off’ roadmap stage of the Adrian Brown model and to prioritise the idea of measuring, benchmarking, setting goals and roadmaps as continuous activities.

The design intentions of an assessment method, and how they are communicated are important. In the case of the RAM capability maturity model there is no ‘minimum’ expectation of what equates to being ‘preservation-capable’. In something like the CMMI there is a consistent ideal state of 'Optimized' (above quantitatively managed), but sometimes this will not be attainable in every area of evaluation, or even desirable given local resources, priorities and risk scenarios.

Conclusions

The DPC RAM provides criteria designed to support incremental maturity assessment of archival preservation practice. The RAM criteria and examples provide a simple and effective reference point and tool for data archives, and for data preservation vendors. Further validation of the proposed maturity examples will form part of ongoing DPC RAM testing and change management.

Neither the DPC RAM, nor the CoreTrustSeal seek to evaluate particular disciplinary or domain expertise, but instead focus on evidence which supports assessment of capabilities within the local context. Both ask some contextual questions about local circumstances related to the organisation and collection, but there is arguably more work to do in clarifying the relationship between the collection under curation and the capabilities of the curator.

The trend towards centralisation of data storage and management environments is clear and positive. Technological solutions which automate and improve our ability to make data accessible and renderable 'now' are important, but we must maintain a focus on the changing needs of the data users as supported by curatorial experts. This could be the difference between delivering technically compliant digital objects and truly usable data assets.
The wider landscape of evaluation and maturity approaches does present a risk of increased operational cost, complexity and confusion. Developing consistent measurement approaches would support the generation of comparable outcomes that could help the data management community align evaluation approaches, identify key issues and agree common solutions.

The lack of context provided by digital object characteristics and the lack of input from the data user community means that it misses some key areas of assurance that data will remain usable and understandable the long term.

The deceptively simple acronym FAIR[20] hides a wealth of complexity that will be familiar to preservation practitioners. Both CoreTrustSeal and RAM manage to address Findable, and Accessible. CoreTrustSeal is arguably able to support more granular organisational assessment necessary to deliver Re-usable. The RAM provides an overview of governance and service capability from a business information perspective (policy, strategy procedure) and change perspective (continuous improvement). Arguably both approaches' are focussed on single bounded organisational entity, so have limited input into the Interoperability issue.

Self-assessment and evaluation are key components of maturing infrastructures. Maximising the comparability of results maximises the return on investment at individual archive/repository level and at community level. Ideally we'd find a way to align high level maturity with repository trust and object FAIRness.

[20] https://www.nature.com/articles/sdata201618