Assessing a Dark Archive: The Use of Standard Auditing Metrics as Design Tools for Digital Repositories

Alex Kinnaman[1], advised by Michael Popham[2], Rhiannon Bettivia[3], Allen Renear[4]

University of Illinois at Urbana-Champaign[1], Bodleian Digital Libraries Systems and Services[2], University of Illinois at Urbana-Champaign[3], University of Illinois at Urbana-Champaign[4]

Introduction: Developing Digital Repositories

As more digital collection projects develop, there is a noted lack of uniformity in how they are constructed. Standards do not yet exist for the development stages of such digital projects, which calls for an investigation of current digital assessment tools to determine if and how existing tools help guide and standardize digital project development.

Context: Digital Safe

Digital Safe is the Bodleian Digital Library Systems & Services' (BDLSS) solution at the University of Oxford for a collective infrastructure and technology for storing long-term, high security data. Thus far, Oxford lacks a universal storage space for the mass amount of student records, financial records, other personally identifiable information that need to be digitally preserved and stored.

Digital Safe is classified as a dark archive with limited access storage. In 2014 the project went on hiatus after completing 2 phases of its 3-phase project. In summer of 2016 the project began seeking funding for phase 3, requiring a review of the project. They opted to outsource technologies for storage and digital preservation, and manage the service via a local interface (Figure 1). This complicates what documentation exists and what is still in development.

This approach to auditing an incomplete digital project is challenging because of the lack of material and cohesion of the dark archive, which could be a useful tool for those thinking about or currently developing a digital collection. This research could also assist the development of digital preservation policy as it becomes more standardized.

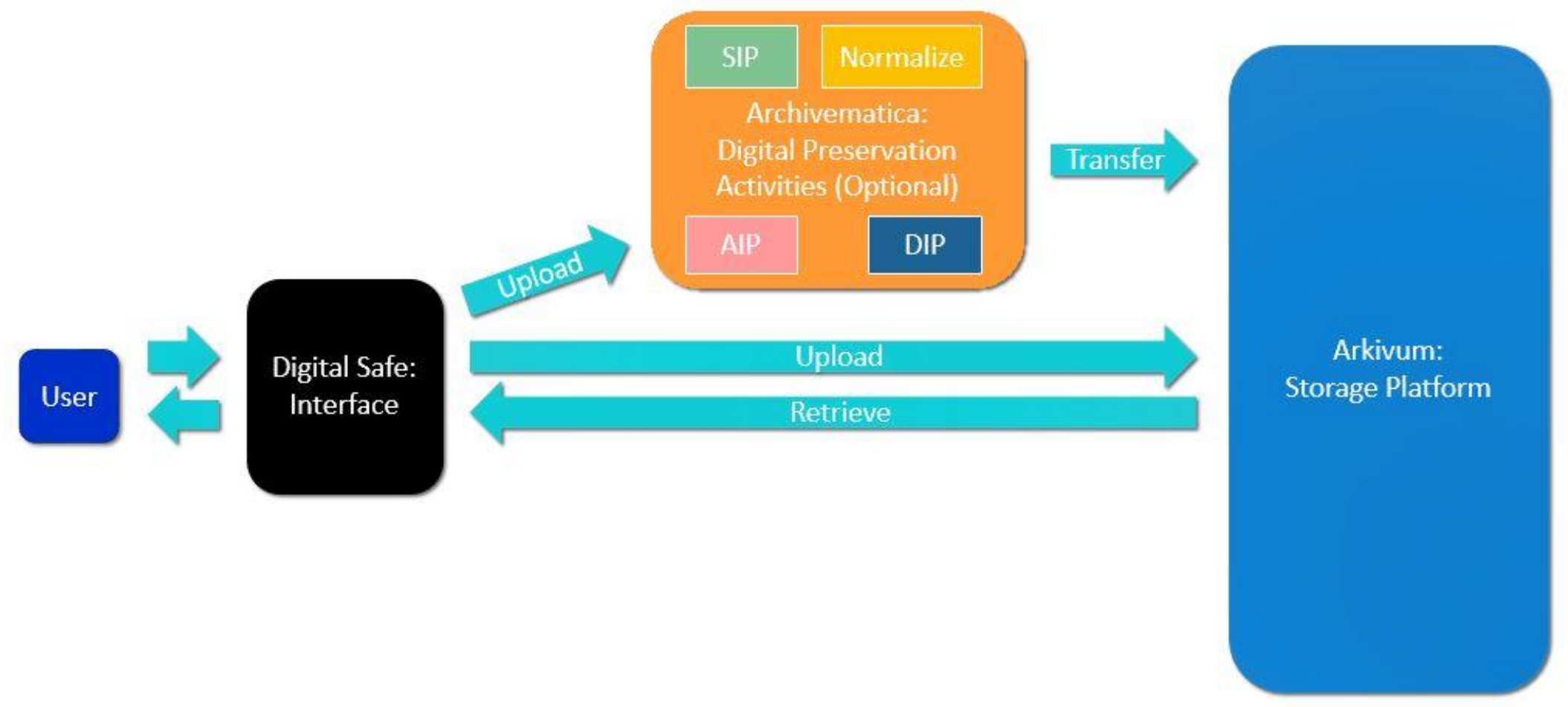

Figure 1. A visualization of the relationship between the three components of Digital Safe

Rationale

Digital Safe is a unique sample of non-traditional repository:

- Classified as a dark archive
- Development in-progress
- No infrastructure
- No official governance
- Combination of 2 technologies and 1 interface
- No test data

Limitations

- No case studies found of assessed dark archives or descriptions of planning processes
- Limited time
- Only tested with 2 metrics
- Arkivum altered their products in Jan. 2016
- DSA released newest version
- Lack of expertise

Literature Review

A literature review and environmental scan of current trends in digital preservation was conducted to understand how common concepts such as "transparency," "service," and "designated community," are defined by the users versus how they are defined by auditing metric creators like TRAC and ISO as leaders, and DSA and nestor as popular options is vital to understanding the effectiveness of auditing metrics for various types of archives and repositories. The environmental scan examined examples of formal audits, self-assessments, and peer assessments for comparison.

Research Question: Can standard auditing metrics be used as a scoping exercise for designing non-traditional repositories, and if so, how is each metric best utilized?

The Metrics

versus

TRAC

- Trustworthy Repositories Audit and Certification
- Developed by OCLC, 2007
- 84 questions, 3 sections
- Chosen for universal use and thoroughness, closeness to ISO 16363
- Formal certification
- Balance of complex criteria and manageable in the timeframe
- Original choice of BDLSS for assessing *Digital Safe*

DSA

- Data Seal of Approval
- Developed by DANS, 2008
- Transferred to international board, 2009
- 16 guidelines
- Chosen for popularity
- Basic certification

nestor Seal

- nestor Seal for Trustworthy Digital Archives
- Extended self-assessment
- Based on DIN31644

Methodology

1. Evidence Collection

Evidence for meeting audit criteria was collected from multiple sources. *Digital Safe* consists of a multitude of unorganized documents that lacked a single storage space. These documents included meeting minutes, formal project initiation documents, and various presentation and communication materials. Current documentation is not publicly available. Interviews with various stakeholders were conducted to gauge interest and to establish the stability of governance and infrastructure for *Digital Safe*. Arkivum and Archivematica both contain extensive documentation illustrating their services, available publicly online. Specific contract information with the University of Oxford was provided by Phase 3 project lead Neil Jefferies. Sources for TRAC, DSA, and nestor were consulted for examples of acceptable evidence for meeting their respective criteria, including the 2011 HathiTrust TRAC assessment, 3 DSA examples, and 2 nestor examples.

2. Assessments

a. TRAC

This assessment took place in July 2016 for the BDLSS. The results were presented as a formal report to the Oxford e-Research Center and offered a response for each criteria and recommendations for next steps based on identified gaps in documentation and other criteria evidence.

b. DSA + nestor Seal

The DSA assessment took place in March of 2017. DSA updated their guidelines in November of 2016, making comparisons to current examples challenging. The results were informal, unpublished, and based on the original TRAC report and reformatted for DSA. Similarly, the nestor assessment took place in April of 2017 and included expanded answers from the DSA assessment.

3. Comparison

The two certifications were compared on how they defined their vocabulary, what strengths and weaknesses in evidence were identified, and the general process of collecting evidence. Both were assessed for how they addressed the needs of their users as tools, and their benefits and drawbacks were identified.

Results

The informal audit results follow TRAC Criteria structure. Each response includes the criteria, the response, and the example evidence provided by TRAC. The responsibilities of *Digital Safe* as a service, Arkivum as a storage platform, and Archivematica as a digital preservation workflow tool are all considered for each criteria. If they do not have a responsibility for the criteria it is acknowledged. As an added measure for the BDLSS, the audit also includes a rating system that indicates the completeness of each criteria and section on a scale of 0-4.
The results were structured per the 16 Core Trustworthy Data Repositories Requirements described in the 2017-2019 version. The DSA Statement of Compliance scale of 0-4 and the nestor point scale of 0-10 were also included in the assessment. Both assessments were intended to be used as scoping methods and not as fully complete responses to the criteria that would meet certification or peer-assessment levels.

Findings

Though the results of these assessment are in the process of being analyzed, the experience of implementing the metrics and comparing them to the literature review and other formal and informal assessment have revealed several themes.

1. Definitions are complicated

Auditing metrics tend to define their vocabularies based on OAIS vocabulary or only within the context of their own guidelines, if they are included at all. The lack of universal definitions hinders institutions that are developing digital projects. Metrics tend to use "repository" as the catch-all term for a digital collection, but in the UK for example, a repository by definition is open access, removing dark archives from equally utilizing a metric for scoping without altering their own vocabularies. The result is that repositories tend to create their own vocabulary that may cause discrepancies with other definitions.

2. Documentation as Evidence

Evidence for meeting metric criteria is based on proof of successful implementation, such as showcasing the ingest process or demonstrating a search function. In the planning and development stages this is not necessarily possible. Documentation describing the ideal process in detail with explanation on how it will be implemented can substitute as evidence and be considered sufficient for partially completing a criteria.

3. TRAC is a pain

Even as a self-assessment, TRAC is extensive and highly repetitive. Section B, Digital Object Management, in particular asks for the same evidence in different contexts that could be consolidated. TRAC is the ultimate checklist, but not necessarily where a project would begin.

3. DSA leaves room for interpretation

First, DSA's statement of compliance requires an explanation for any requirement that is not applicable, that has not been determined yet, and that does not have public evidence. This allows for reflection on not just what but why a criteria is not yet meetable, and is a means to determine what the repository needs to define itself and its priorities.

4. DSA+nestor is self-guided

Where TRAC requires official auditors, DSA+nestor is a self-guided self-assessment that, when complete, is accepted largely based on peer-review. Aside from saving time, DSA+nestor is useful for better developing the theory and strategy of a repository that is also evaluated by peers.

5. Further Investigation

Ultimately, TRAC and other formal metrics are checklists for enhancing a repository, and DSA+nestor is popular because they offer peer-confirmation, self-assessment, and are self-paced. Further exploration into other metrics and with other examples is necessary to fully understand how to best utilize digital preservation standards.