

Central Depository II: Mapping the RLG/OCLC Attributes of a Trusted Repository to CDI key issues [draft report]

Nancy Y. McGovern, Digital Preservation Officer (DPO)

Last revised: March 2002

Related documents:

Establishing a Central Depository for Preserving Digital Image Collections - Part I: Responsibilities of Transferee by Anne R. Kenney, Oya Rieger, et al.

Attributes of a Trusted Digital Repository: Meeting the Needs of Research Resources, An RLG-OCLC Report, Draft for Public Comment, August 2001.

The CUL Central Depository Part I (CDI) Report¹ identified 16 key issues to be addressed in the CUL Central Depository Part II (CDII) report. We have mapped those 16 issues to the six components of the framework proposed in the RLG-OCLC report: *Attributes of a Trusted Digital Repository*.² The purpose of the mapping is to:

- Use the 6 higher level framework components that are proposed in the RLG/OCLC report to cluster the 16 issues to ensure all are addressed in the RLG/OCLC report and to make these two documents come into alignment
- Identify additional key issues to cover based upon areas in the RLG-OCLC framework that may not be addressed by CDI key issues
- Identify questions in those 6 areas for gathering information about existing Cornell projects and relevant initiatives

We had thought when we proposed the mapping that the RLG-OCLC framework components would provide clear-cut higher-level categories. We also thought that each key CUL CDI issue would fit neatly into one framework component. Neither assumption turned out to be true in practice, but working on the mapping produced several potentially interesting results:

- Most of the defining characteristics of the RLG-OCLC framework components implicitly or explicitly reference other framework components.
- The components of the RLG-OCLC framework are neither hierarchical (e.g., procedural accountability cuts across/underlies all of the components) nor equal in weight (e.g., system security is not less important than financial sustainability but it is easier to attain and more well-defined)
- The CUL CDI key issues may pertain primarily to one framework component, but each has a secondary relationship to one or more components.

¹ *Establishing a Central Depository for Preserving Digital Image Collections - Part I: Responsibilities of Transferee* by Anne R. Kenney, Oya Rieger, et al.

² *Attributes of a Trusted Digital Repository: Meeting the Needs of Research Resources*, An RLG-OCLC Report, Draft for Public Comment, August 2001.

Step 1. Summarize RLG-OCLC Framework Component Characteristics

We summarized these characteristics for each component of the RLG-OCLC framework narrative to make the mapping to CUL CDI key issues easier and more consistent. We numbered the components in the order in which they appear in the report. The numbers in parentheses are references to other framework components.

1. Administrative responsibility

- Provide evidence of fundamental commitment to implementing community-agreed standards, best practices
- Commit to understanding OAIS model and implementing
- Meet national/international standards on environment (6)
- Meet or exceed community standards and share measurements with depositors (6)
- Involve external community experts in regularly validating/certifying processes and procedures (6)
- Commit to transparency and accountability in all actions (6)

2. Organizational viability

- Demonstrate viability and trustworthiness (3)
- Reflect commitment to long-term retention/management in mission statements
- Have appropriate legal status, staff and professional development for responsibilities (1)(3)
- Establish transparent business practices, effective management policies (6)(3)
- Define comprehensive written agreements with depositors (6)
- Review and maintain policies and procedures (6)
- Undertake risk management, contingency and succession (trusted inheritors) planning (6)(3)

3. Financial sustainability

- Establish and maintain good business practices and an auditable business plan (1)(2)
- Demonstrate financial fitness and ongoing financial commitment (1)(2)
- Balance risk, benefit, investment, expenditure
- Maintain adequate budget and reserves and actively seek potential funding sources

4. Technological suitability

- Consider and adopt appropriate preservation strategies (6)
- Ensure appropriate infrastructure (hardware, software, facilities) for acquisition, storage, access (5)
- Establish technology management policy for repository (replacement, enhancement, funding) (2)(3)
- Comply with relevant standards and best practices (supported by adequate expertise) (6)
- Undergo regular external audits on system components and performance (6)

5. System security

- Assure security of systems for digital assets (3)
- Establish policies and procedures to meet requirements (copying, authentication, firewalls, backups, disaster preparedness, response, recovery, training) (4)(6)
- Stress processes that will detect, avoid and repair loss, document and notify about changes and resulting actions (4)(6)

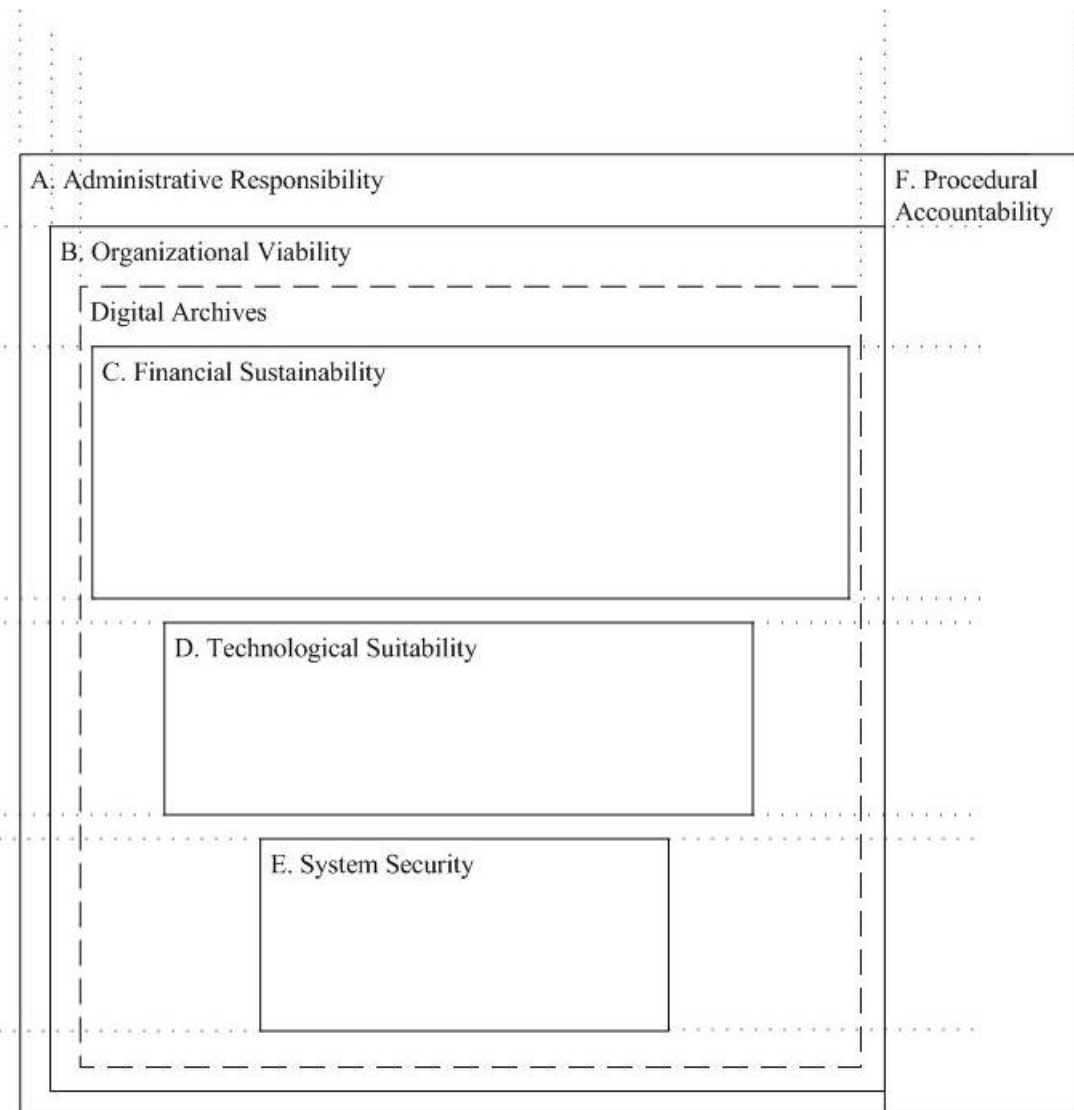
6. Procedural accountability

- Enact all relevant policies and procedures for specified tasks and functions, document all practices (1)(2)
- Establish monitoring mechanisms to ensure continued operation of systems and procedures (4)(5)
- Record and justify preservation strategies (1)(2)
- Set up feedback mechanisms to support problem resolution and negotiate evolving requirements between providers and consumers (1)(2)

Step 2. Identify relationships between the six components of the RLG-OCLC Framework

The diagram below suggests relationships between the RLG-OCLC framework components. All of the components are not equal (in significance, required resources, scope, etc.). There are dependencies and hierarchical relationships between components. The dotted lines indicate relationships that extend beyond an individual framework component. Relationships may extend:

- Beyond the digital archives but remain within the organization, e.g. the organization may maintain more than one digital archives, or the financial sustainability of the digital archives is impacted by other organizational obligations (represented by horizontal dotted lines)
- Beyond the organization, e.g. there will be ties between digital archives that are maintained by other organizations, or requirements that are imposed by external standards and other authoritative boards (represented by vertical dotted lines)



- A. *Administrative Responsibility*: encompasses all of the other components and lays the foundation for a trusted repository; is influenced by/based upon larger organizational and/or domain contexts
- B. *Organizational Viability*: encompasses the repository but relies upon some elements of Administrative Responsibility; is influenced by/based upon larger organizational and/or domain contexts
- *Digital Archives*: does not appear in the RLG-OCLC report but an organization may be responsible for one or more digital archives; has ties to other digital archives (part of larger preservation management matrix) and is influenced/adapted from external experiences and practice
- C. *Financial Sustainability*: is the most critical of the components within the repository, which cannot exist in its absence; relates to other financial commitments in the organization
- D. *Technological Suitability*: is the next most essential component within the repository and determines the success of the preservation program; should be influenced/adapted from external experiences and practice
- E. *System Security*: is critical to the success of the implementation, but there are known methodologies for establishing and maintaining system security; will be part of a larger context of system security practices, both within the organization and externally
- F. *Procedural Accountability*: cuts across and underpins the trusted nature of the repository; some percentage are dictated by/based upon external authorities