Foundation Documents:
Attributes of Trusted Digital Repository (TDR)

NOTE: The numbers in parentheses after refer to related (dependent) TDR attributes.

0. OAIS Compliance

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)

Overview of relationships between the framework components

0. ***OAIS Compliance:*** underlying principle that is an integral part of the other framework components
1. ***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
2. ***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 Border***: 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

3. ***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
4. ***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
5. ***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
6. ***Procedural Accountability***: cuts across and underpins the trusted nature of the repository; some percentage are dictated by/based upon external authorities