NORTHEAST DOCUMENT CONSERVATION CENTER

Planning for Digital Preservation:
20 Questions for Providers of Digital Storage Services

By Bernard Reilly, President, Center for Research Libraries

The following questions are based on *Trustworthy Repositories Audit & Certification (TRAC) : Criteria and Checklist*, version 1.0 (http://www.crl.edu/PDF/trac.pdf), and additional metrics developed by the Center for Research Libraries for trusted digital repositories.

1. What is the current museum, library, and/or archives client base of the provider? The provider should be able to supply references.

2. What types of content files does the provider accept and store? The provider should be able to present examples.

3. What protections does the repository have in place to prevent unauthorized access to, and/or use of, archived content?

4. What kinds of uses, if any, will the repository make or allow others to make of archived content? What rights must the content owner grant to the provider for such uses?

5. What services and/or features does the repository provide that increase the functionality or value of the content archived? Some repositories make tools, services, and other features available that can be useful to content owners.

6. What costs connected with the storage, management, migration, and preservation of content and metadata is the content owner expected to bear?

7. What documentation of the repository's systems, procedures, and policies is available for examination?

8. What metadata standards are observed and maintained for content files accepted and stored by the provider?

9. What characteristics or traits of the content that is accepted and stored are designated for preservation?

10. Does the provider modify content in any way to optimize the repository's processes? If "normalization" is part of the ingest process, what traits or functionalities of the content are lost?

11. How and how often does the provider check archived content (Archival Information Packages [AIPs]) against the content originally submitted (Submission Information Packages [SIPs])? Such comparisons are a way to detect corruption or loss of content.

12. What kinds of reports of such checks does the provider generate, and how frequently are those reports issued?

13. Does the provider offer content owners direct access to their archived content? Some repositories make online searching and verification of the presence of archived content available to content owners through a Web interface.

14. What provisions has the provider made for the migration of archived content to new software and hardware platforms when the current platform is obsolete? Has the repository completed a successful migration of content in the past?

15. Has the provider's repository undergone an IT audit against ISO standard 27001? Or against other industry standards? Has there been any independent party verification of the repository's services? Providers should be able to furnish certification or audit reports for these controls.

16. What level of systems redundancy does the repository have in place? The provider should be able to indicate the number and location(s) of sites where multiple copies of the archived content are hosted.

17. In the case of primary system failure or catastrophic natural or manmade disaster, how soon can the provider bring the backup system fully online? How will this recovery be funded? The provider should be able to reference a written disaster plan.

18. What additional backup provisions does the repository have against content loss or corruption?

19. What level and form of indemnification is provided to the content owner against loss or corruption of digital content?

20. How is the return of content to owners handled? The provider should be able to indicate in detail how, and in what form, files and metadata will be returned and how their removal from the repository system will be documented.