

Trustworthy Repositories Audit & Certification: Criteria Checklist

Organization:		Auditor:		Page	
Section:	A. Organizational Infrastructure	Interviewee(s):		Date	
Aspect:	A1. Governance & organizational viability				
Criterion	Evidence (Documents) Examined		Findings and Observations		Result
A1.1. Repository has a mission statement that reflects a commitment to the long-term retention of, management of, and access to digital information.					
A1.2. Repository has an appropriate, formal succession plan, contingency plans, and/or escrow arrangements in place in case the repository ceases to operate or the governing or funding institution substantially changes its scope.					

Trustworthy Repositories Audit & Certification: Criteria Checklist

Organization:		Auditor:		Page	
Section:	A. Organizational Infrastructure	Interviewee(s)::		Date	
Aspect:	A2. Organizational structure & staffing				
Criterion	Evidence (Documents) Examined		Findings and Observations		Result
A2.1. Repository has identified and established the duties that it needs to perform and has appointed staff with adequate skills and experience to fulfill these duties.					
A2.2. Repository has the appropriate number of staff to support all functions and services.					
A2.3. Repository has an active professional development program in place that provides staff with skills and expertise development opportunities.					

Trustworthy Repositories Audit & Certification: Criteria Checklist

Organization:		Auditor:		Page	
Section:	A. Organizational Infrastructure	Interviewee(s):		Date	
Aspect:	A3. Procedural accountability & policy framework				
Criterion	Evidence (Documents) Examined		Findings and Observations		Result
A3.1. Repository has defined its designated community(ies) and associated knowledge base(s) and has publicly accessible definitions and policies in place to dictate how its preservation service requirements will be met.					
A3.2. Repository has procedures and policies in place, and mechanisms for their review, update, and development as the repository grows and as technology and community practice evolve.					
A3.3. Repository maintains written policies that specify the nature of any legal permissions required to preserve digital content over time, and repository can demonstrate that these permissions have been acquired when needed.					
A3.4. Repository is committed to formal, periodic review and assessment to ensure responsiveness to technological developments and evolving requirements.					
A3.5. Repository has policies and procedures to ensure that feedback from producers and users is sought and addressed over time.					

Trustworthy Repositories Audit & Certification: Criteria Checklist

Organization:		Auditor:		Page	
Section:	A. Organizational Infrastructure	Interviewee(s):		Date	
Aspect:	A3. Procedural accountability & policy framework				
Criterion	Evidence (Documents) Examined		Findings and Observations		Result
A3.6. Repository has a documented history of the changes to its operations, procedures, software, and hardware that, where appropriate, is linked to relevant preservation strategies and describes potential effects on preserving digital content.					
A3.7. Repository commits to transparency and accountability in all actions supporting the operation and management of the repository, especially those that affect the preservation of digital content over time.					
A3.8 Repository commits to defining, collecting, tracking, and providing, on demand, its information integrity measurements.					
A3.9 Repository commits to a regular schedule of self-assessment and certification and, if certified, commits to notifying certifying bodies of operational changes that will change or nullify its certification status.					

Trustworthy Repositories Audit & Certification: Criteria Checklist

Organization:		Auditor:		Page	
Section:	A. Organizational Infrastructure	Interviewee(s):		Date	
Aspect:	A4. Financial sustainability				
Criterion	Evidence (Documents) Examined		Findings and Observations		Result
A4.1. Repository has short- and long-term business planning processes in place to sustain the repository over time.					
A4.2. Repository has in place processes to review and adjust business plans at least annually.					
A4.3. Repository's financial practices and procedures are transparent, compliant with relevant accounting standards and practices, and audited by third parties in accordance with territorial legal requirements.					
A4.4. Repository has ongoing commitment to analyze and report on risk, benefit, investment, and expenditure (including assets, licenses, and liabilities).					
A4.5. Repository commits to monitoring for and bridging gaps in funding.					

Trustworthy Repositories Audit & Certification: Criteria Checklist

Organization:		Auditor:		Page	
Section:	A. Organizational Infrastructure	Interviewee(s):		Date	
Aspect:	A5. Contracts, Licenses and Liabilities				
Criterion	Evidence (Documents) Examined		Findings and Observations		Result
A5.1 If repository manages, preserves, and/or provides access to digital materials on behalf of another organization, it has and maintains appropriate contracts or deposit agreements.					
A5.2 Repository contracts or deposit agreements must specify and transfer all necessary preservation rights, and those rights transferred must be documented.					
A5.3 Repository has specified all appropriate aspects of acquisition, maintenance, access, and withdrawal in written agreements with depositors and other relevant parties.					
A5.4 Repository tracks and manages intellectual property rights and restrictions on use of repository content as required by deposit agreement, contract, or license.					
A5.5 If repository ingests digital content with unclear ownership/rights, policies are in place to address liability and challenges to those rights.					

Trustworthy Repositories Audit & Certification: Criteria Checklist

Organization:		Auditor:		Page	
Section:	B. Digital Object Management	Interviewee(s):		Date	
Aspect:	B.1 Ingest: acquisition of content				
Criterion	Evidence (Documents) Examined		Findings and Observations		Result
B1.1. Repository identifies properties it will preserve for digital objects.					
B1.2. Repository clearly specifies the information that needs to be associated with digital material at the time of its deposit (i.e., SIP).					
B1.3. Repository has mechanisms to authenticate the source of all materials.					
B1.4. Repository's ingest process verifies each submitted object (i.e., SIP) for completeness and correctness as specified in B1.2.					
B1.5. Repository obtains sufficient physical control over the digital objects to preserve them (Ingest: content acquisition).					

Trustworthy Repositories Audit & Certification: Criteria Checklist

Organization:		Auditor:		Page	
Section:	B. Digital Object Management	Interviewee(s):		Date	
Aspect:	B.1 Ingest: acquisition of content				
Criterion	Evidence (Documents) Examined		Findings and Observations		Result
B1.6. Repository provides producer/depositor with appropriate responses at predefined points during the ingest processes.					
B1.7. Repository can demonstrate when preservation responsibility is formally accepted for the contents of the submitted data objects (i.e., SIPs).					
B1.8. Repository has contemporaneous records of actions and administration processes that are relevant to preservation.					

Trustworthy Repositories Audit & Certification: Criteria Checklist

Organization:		Auditor:		Page	
Section:	B. Digital Object Management	Interviewee(s):		Date	
Aspect:	B.2 Ingest: creation of the archivable package				
Criterion	Evidence (Documents) Examined		Findings and Observations		Result
B2.1. Repository has an identifiable, written definition for each AIP or class of information preserved by the repository.					
B2.2. Repository has a definition of each AIP (or class) that is adequate to fit long-term preservation needs.					
B2.3. Repository has a description of how AIPs are constructed from SIPs					
B2.4. Repository can demonstrate that all submitted objects (i.e., SIPs) are either accepted as whole or part of an eventual archival object (i.e., AIP), or otherwise disposed of in a recorded fashion.					
B2.5. Repository has and uses a naming convention that generates visible, persistent, unique identifiers for all archived objects (i.e., AIPs).					

Trustworthy Repositories Audit & Certification: Criteria Checklist

Organization:		Auditor:		Page	
Section:	B. Digital Object Management	Interviewee(s):		Date	
Aspect:	B.2 Ingest: creation of the archivable package				
Criterion	Evidence (Documents) Examined		Findings and Observations		Result
B2.6. If unique identifiers are associated with SIPs before ingest, the repository preserves the identifiers in a way that maintains a persistent association with the resultant archived object (e.g., AIP).					
B2.7. Repository demonstrates that it has access to necessary tools and resources to establish authoritative semantic or technical context of the digital objects it contains (i.e., access to appropriate international Representation Information and format registries).					
B2.8 Repository records/registers Representation Information (including formats) ingested.					
B2.9 Repository acquires preservation metadata (i.e., PDI) for its associated Content Information.					
B2.10 Repository has a documented process for testing understandability of the information content and bringing the information content up to the agreed level of understandability.					

Trustworthy Repositories Audit & Certification: Criteria Checklist

Organization:		Auditor:		Page	
Section:	B. Digital Object Management	Interviewee(s):		Date	
Aspect:	B.2 Ingest: creation of the archivable package				
Criterion	Evidence (Documents) Examined		Findings and Observations		Result
B2.11 Repository verifies each AIP for completeness and correctness at the point it is generated.					
B2.12 Repository provides an independent mechanism for audit of the integrity of the repository collection/content.					
B2.13 Repository has contemporaneous records of actions and administration processes that are relevant to preservation (AIP creation).					

Trustworthy Repositories Audit & Certification: Criteria Checklist

Organization:		Auditor:		Page	
Section:	B. Digital Object Management	Interviewee(s):		Date	
Aspect:	B.3 Preservation Planning				
Criterion	Evidence (Documents) Examined		Findings and Observations		Result
B3.1. Repository has documented preservation strategies.					
B3.2. Repository has mechanisms in place for monitoring and notification when Representation Information (including formats) approaches obsolescence or is no longer viable.					
B3.3 Repository has mechanisms to change its preservation plans as a result of its monitoring activities.					
B3.4. Repository can provide evidence of the effectiveness of its preservation planning.					

Trustworthy Repositories Audit & Certification: Criteria Checklist

Organization:		Auditor:		Page	
Section:	B. Digital Object Management	Interviewee(s):		Date	
Aspect:	B.4 Archival storage & preservation/ maintenance of AIPs				
Criterion	Evidence (Documents) Examined		Findings and Observations		Result
B4.1. Repository employs documented preservation strategies.					
B4.2. Repository implements/responds to strategies for archival object (i.e., AIP) storage and migration.					
B4.3 Repository preserves the Content Information of archival objects (i.e., AIPs).					
B4.4 Repository actively monitors integrity of archival objects (i.e., AIPs).					
B4.5 Repository has contemporaneous records of actions and administration processes that are relevant to preservation (Archival Storage).					

Trustworthy Repositories Audit & Certification: Criteria Checklist

Organization:		Auditor:		Page	
Section:	B. Digital Object Management	Interviewee(s):		Date	
Aspect:	B.5 Information Management				
Criterion		Evidence (Documents) Examined		Findings and Observations	
B5.1 Repository articulates minimum metadata requirements to enable the designated community to discover and identify material of interest.					
B5.2 Repository captures or creates minimum descriptive metadata and ensures that it is associated with the archived object (i.e., AIP).					
B5.3 Repository can demonstrate that referential integrity is created between all archived objects (i.e., AIPs) and associated descriptive information.					
B5.4 Repository can demonstrate that referential integrity is maintained between all archived objects (i.e., AIPs) and associated descriptive information.					

Trustworthy Repositories Audit & Certification: Criteria Checklist

Organization:		Auditor:		Page	
Section:	B. Digital Object Management	Interviewee(s):		Date	
Aspect:	B.6 Access Management				
Criterion		Evidence (Documents) Examined		Findings and Observations	
B6.1 Repository documents and communicates to its designated community what access and delivery options are available.					
B6.2 Repository has implemented a policy for recording all access actions (includes requests, orders etc.) that meet the requirements of the repository and information producers/depositors.					
B6.3 Repository ensures that agreements applicable to access conditions are adhered to.					
B6.4 Repository has documented and implemented access policies (authorization rules, authentication requirements) consistent with deposit agreements for stored objects.					
B6.5 Repository access management system fully implements access policy..					

Trustworthy Repositories Audit & Certification: Criteria Checklist

Organization:		Auditor:		Page	
Section:	B. Digital Object Management	Interviewee(s):		Date	
Aspect:	B.6 Access Management				
Criterion	Evidence (Documents) Examined		Findings and Observations		Result
B6.6 Repository logs all access management failures, and staff review inappropriate “access denial” incidents.					
B6.7 Repository can demonstrate that the process that generates the requested digital object(s) (i.e., DIP) is completed in relation to the request.					
B6.8 Repository can demonstrate that the process that generates the requested digital object(s) (i.e., DIP) is correct in relation to the request.					
B6.9 Repository demonstrates that all access requests result in a response of acceptance or rejection.					
B6.10 Repository enables the dissemination of authentic copies of the original or objects traceable to originals.					

Trustworthy Repositories Audit & Certification: Criteria Checklist

Organization:	C. Technologies, Technical Infrastructure & Security	Auditor:		Page	
Section:		C1. System Infrastructure	Interviewee(s):		Date
Aspect:					
Criterion	Evidence (Documents) Examined	Findings and Observations		Result	
C1.1 Repository functions on well-supported operating systems and other core infrastructural software.					
C1.2 Repository ensures that it has adequate hardware and software support for backup functionality sufficient for the repository's services and for the data held, e.g., metadata associated with access controls, repository main content.					
C1.3 Repository manages the number and location of copies of all digital objects.					
C1.4 Repository has mechanisms in place to ensure any/multiple copies of digital objects are synchronized.					
C1.5 Repository has effective mechanisms to detect bit corruption or loss.					

Trustworthy Repositories Audit & Certification: Criteria Checklist

Organization:		Auditor:		Page	
Section:	C. Technologies, Technical Infrastructure & Security	Interviewee(s):		Date	
Aspect:	C1. System Infrastructure				
Criterion	Evidence (Documents) Examined		Findings and Observations	Result	
C1.6 Repository reports to its administration all incidents of data corruption or loss, and steps taken to repair/replace corrupt or lost data.					
C1.7 Repository has defined processes for storage media and/or hardware change (e.g., refreshing, migration).					
C1.8 Repository has a documented change management process that identifies changes to critical processes that potentially affect the repository's ability to comply with its mandatory responsibilities..					
C1.9 Repository has a process for testing the effect of critical changes to the system.					
C1.10 Repository has a process to react to the availability of new software security updates based on a risk-benefit assessment.					

Trustworthy Repositories Audit & Certification: Criteria Checklist

Organization:	C. Technologies, Technical Infrastructure & Security	Auditor:		Page		
Section:		C.2 Appropriate technologies	Interviewee(s):		Date	
Aspect:						
Criterion		Evidence (Documents) Examined	Findings and Observations		Result	
C2.1 Repository has hardware technologies appropriate to the services it provides to its designated communities and has procedures in place to receive and monitor notifications, and evaluate when hardware technology changes are needed.						
C2.2 Repository has software technologies appropriate to the services it provides to its designated community(ies) and has procedures in place to receive and monitor notifications, and evaluate when software technology changes are needed.						

Trustworthy Repositories Audit & Certification: Criteria Checklist

		Auditor:	Page	
	C. Technologies, Technical Infrastructure & Security	Interviewee(s):	Date	
	C.3 Security			
	Evidence (Documents) Examined	Findings and Observations		Result
C3.1 Repository maintains a systematic analysis of such factors as data, systems, personnel, physical plant, and security needs.				
C3.2 Repository has implemented controls to adequately address each of the defined security needs.				
C3.3 Repository staff have delineated roles, responsibilities, and authorizations related to implementing changes within the system.				
C3.4 Repository has suitable written disaster preparedness and recovery plan(s), including at least one off-site backup of all preserved information together with an off-site copy of the recovery plan(s).				