



DCC Comments on RLG/NARA Audit and Certification Checklist

Authors: Seamus Ross [\[s.ross@hatii.arts.gla.ac.uk\]](mailto:s.ross@hatii.arts.gla.ac.uk)
Niklaus Bütikofer [\[niklaus.buetikofer@bluewin.ch\]](mailto:niklaus.buetikofer@bluewin.ch)
Andrew McHugh [\[a.mchugh@hatii.arts.gla.ac.uk\]](mailto:a.mchugh@hatii.arts.gla.ac.uk)

Table of Contents

Introduction	2
General Points Arising from the Draft Checklist	4
Omission of Evidential Requirements	4
Benchmarking	4
Efforts of Traditional Archiving Inspectors.....	4
Relationship with International Standards	4
Questions surrounding the Designated Community	5
Role of Access within the Checklist	5
Compliance Status	5
Semantic and Structural Consistency	6
Appendix A: Comments on Audit Checklist (26th March 2006).....	7
Appendix B: Examples Documents to Request in Advance of Audit.....	30
Appendix C: Individuals for Audit Interviews	33

Introduction

An audit and certification work group convening within the services team of the Digital Curation Centre met on the 6th of March 2006 in London. This meeting was supplemented by a series of conference calls over the next two weeks. Objectives identified for the work group at the first meeting were:

- (a) to validate the draft RLG-NARA Audit Checklist for the Certification of Digital Repositories;
- (b) to establish an alternative (ideally complementary) combination of self audit and third-party audit criteria, processes and guidelines;
- (c) to identify the classes of evidence that would be required if an auditor were to be able to answer the questions raised by the Checklist;
- (d) to identify the documents that we would wish to see in advance of an audit visit to enable the auditors to make maximum effective use of their time on site; and
- (e) to identify the repository staff that an auditor would wish to interview during a site visit.

While it is felt that a selection of competing schemes would benefit none, and instead simply undermine the collective efforts in this area, it is hoped that we can exploit existing internationally established standards and criteria, and avoid duplication of effort and the emergence of ambiguity. Initial work suggests that depositors, curators and end-users are not keen to have a selection of bodies offering disparate and potentially incompatible certification. Therefore we will seek as far as possible to ensure that our work fits within the existing context of both emerging work in this area (such as RLG-NARA, CRL, the Certification Task Force, DINI and Nestor) and more established international standards such as the ISO 9000 series (Quality Assurance), ISO 15489 (Records Management), ISO 17799 (Information Security) and ISO 14721 (OAIS).

The initial meeting concentrated on the RLG-NARA draft audit checklist. Each section, criterion and accompanying note was assessed and critically appraised; the result of this work is an amended checklist (*Appendix A*) that makes explicit the necessary amendments, evidence requirements and supplementary questions identified throughout the process. In addition, following two brainstorming sessions an example list of documentary evidence (*Appendix B*) and individuals (*Appendix C*) that we believe at this stage to be relevant to the audit process were identified and documented.

During our examination of the checklist several points were identified that had a more global relevance. Some of these were concerns that persisted through the document's overall structure instead of being simply associated with individual sections or criterion.. Essentially we concluded that the following shortcomings needed to be addressed:

1. Evidential requirements needed to complete the checklist need to be described;
2. The experience of the traditional archival audit community had not been tapped and should be;
3. the variability of the organisational context in which the audit and certification guidelines might be applied has not been sufficiently described;
4. the relationship of the checklist to international standards other than OAIS has not been adequately considered;
5. the Checklist's horizontal access (Planned thru Evaluated) needs to be reconsidered;

6. the relationship between designated community and trust is not adequately established; and,
7. semantic and structural consistency is apparent throughout the document.

In the next couple of paragraphs we have examined each of these issues in more detail. After that we comment on each of the criteria. Overall we were concerned that the document has a very theoretical tone, and does not really sit well at a implementation level—how will it be applied.

General Points Arising from the Draft Checklist

Omission of Evidential Requirements

A consistent concern within a number of the checklist sections is that requirements are frequently expressed in ambiguous terms with little insight into the ways in which the satisfaction of criteria could be measured. We agree that as well as presenting idealistic statements such as “*repository commits to professional development to keep staff expertise and skills current*” (section A2.3) the checklist, if it aspires to be a practical and easily applicable, it must offer some examples of the kinds of documents or testimonies that must exist as evidence for the responses to the checklist questions. We feel that without an indication of an acceptable evidence base that the checklist remains an unwieldy theoretical beast that is open to broad interpretation with sections too easily extrapolated to conceivably be used endorse even repositories with recognisable shortcomings. The checklist should be tightened up to eliminate redundancies, and ask: “are organisational procedures there”; “are all the main points present”; “if not, do other points compensate for those that are absent”?

A number of sections will only be assessable based on existing efforts; an “appropriate number of staff” (point A2.2) for instance can only be measured in terms of what has worked effectively for other institutions. Words like ‘appropriate’ ensure that although a third party certification authority may be equipped to determine the satisfaction of criteria, a self-assessment exercise becomes significantly less viable.

In summary, in reviewing the chec-list we have identified a significant shortfall in terms of the documentation requirements necessary to provide an evidence base of compliance. We have consequently annotated the checklist with our own observations and some suggestions of evidence that would be useful to auditors. We consider that this will increase the usability of the tool.

Benchmarking

In addition the current version of the checklist seems to overlook the importance of benchmarking. A number of the criteria can only be measured over time and require that benchmark positions be established to assess the development of the archive over time.

Efforts of Traditional Archiving Inspectors

Inspection in the archival context has a long tradition. In developing the checklist the kinds of efforts already undertaken by archival inspectors might have been usefully taken into account. Domain Dependent Sections

We were concerned about the the checklist’s applicability in different organisational context (such as government archives). To remedy this, we suggest introducing context specific modular sections that can be interchanged and presented alongside a core set of universally applicable criteria. This will ensure the increased scope of the checklist without compromising its ability to limit ambiguity and present a series of reasonably specific and where possible quantifiable characteristics of a trusted repository, supported by evidence requirements.

Relationship with International Standards

OAIS is so intrinsic to the checklist that we feel there is some danger that those subscribing to alternative (perhaps just as legitimate) models are necessarily excluded. Any repository audit and certification process must have a broad reach stretching beyond OAIS. The value of OAIS as a

shared vocabulary is without question; however, with ambiguity remaining throughout the community as to the meaning of certain of its terminology, and consequently to the lengths to which institutions must go in order to boast “OAIS compliance” (itself perhaps an intangible concept) some doubt continues to persist. This will detract from a document that ought to be usable by almost any institution to assert precisely to what extent it represents a “trusted digital repository”. To remedy this we would recommend that references to OAIS terminology (such as AIP, PDI, SIP) are presented as *examples* of more generic categories of information, and that efforts to explain the circumstances in which criteria are satisfied are made clearer and where possible more objectively quantifiable. In addition, the section on security within *section D* can be closely compared with the International Standard ISO 17799 on Information Security; it seems strange that while technical terminology from one standard (OAIS) is heavily relied upon throughout the checklist the document does not benefit from the same consideration of other relevant international standards when they are most appropriate (in this case ISO 17799). Similarly, existing financial audit standards are paid little heed, but will be essential in conducting the financial audit aspects of any audit. (This is perhaps more excusable given the likelihood that these are prone to vary within alternative legal systems.)

Questions surrounding the Designated Community

The checklist draws particular attention to the role of the designated community within *section C*. Our discussions raised some concerns with the very concept. It was suggested that the designated community bears little relation to the trusted status or otherwise of a digital repository in terms of long term preservation. While one might be capable of establishing an understanding of a community at a particular point in time the community itself will be so prone to change over time that monitoring and maintaining an understanding of its knowledge base will prove to be at best difficult, and more than likely impossible. Moreover, limiting stored representation information to that which is appropriate for a single perceived audience may prejudice a repository’s ability to provide content to users outwith these parameters at a later date. We acknowledge the accepted status enjoyed by the concept of designated communities, as well as the practicable and non-idealistic nature of the checklist, but we think it sensible at this stage to raise concerns over its long-term viability.

Role of Access within the Checklist

We are concerned at the prominent status that *access* enjoys within the checklist since in many cases this falls outwith the scope of characteristics that will contribute to the level of certifiable trust for a particular repository. Depending on the service level commitments of individual repositories the significance of access services and access controls will determine the importance of access. The issue is considered in A1.1 and in large sections of *section C*. However, from our discussions we conclude that while resource discovery and accessibility functionality is important in terms of a repository’s customer relations, it is of little relevance in terms of the level trust it is capable of offering.

Compliance Status

The checklist’s horizontal axis also raised some problems in our view. The various activity levels (*Planned, Documented, Implemented and Evaluated*) do not necessarily form a graceful trajectory of compliance. How would a third party use the checklist to conclude that a point was implemented without documentary evidence? Instead of making documentation a *stage* of

compliance we recommend that the documentation that must be provided as evidence of implementation is made more explicitly clear, and that the tiers of progress are simplified to *Planned*, and *Implemented*. The checklist needs also to have an evaluation outcome column in which the result of attempts to consider each criteria can be listed. It should have an evidence used column as well in which the evidence that was used to establish compliance with a criteria can be listed.

Semantic and Structural Consistency

At times within the checklist there are examples of inconsistencies. Acronyms from OAIS are generally not expanded, although in section B 3.6 the meaning of PDI (Preservation Description Information) is explicitly stated. Similarly, there are examples of inconsistencies in the framing of individual questions. Whereas the issues of creation and maintenance are covered in sections B 4.2 and B 4.3 as two separate questions, in other instances issues that should be examined in multiple questions are conflated into one (e.g. A 5.1, which ensures that repositories with responsibility over third party data both have and maintain appropriate contracts or deposit agreements). Each of the criteria needs to be reconsidered.

Appendix A: Comments on Audit Checklist (26th March 2006)

Below we have produced an abridged representation of the draft RLG-NARA Audit Checklist for the Certification of Digital Repositories. Suggested evidence requirements and additional observations from the *McHugh Ross Bütkefer Working Group* (henceforth MRB-WG) are provided alongside each checklist section.

The abridged checklist details the original wording from the RLG-NARA publication and where necessary the revised version suggested by the working group. These are generally accompanied by (non-exhaustive) examples of evidence that may be provided to support the satisfaction of each criterion. The final part of each section details any specific observations or further points of clarification that we had.

A. The Organisation

A1. Governance and Organisational Viability

A1.1. Repository has a mission statement that reflects a commitment to the long-term retention of, management of, and access to digital information on behalf of depositors.

MRB-WG Revised A1.1. Repository has a mission statement that reflects a commitment to the long-term retention and management of digital information on behalf of depositors.

MRB-WG Example Evidence Required:

Mission Statement;
Organisational Chart.

MRB-WG Observations:

Access to materials may be optional (e.g dark archives) and therefore should be omitted.

The context of the mission statement is crucial. Many repositories are subject to the overall goals of a parent institution and it is vital to determine whether the mission of the archive is represented in the mission statement of the institution the archive is a part of (e.g. an archive might be a subsidiary of commercial company, a department of government, or public service).

A1.2. Repository has a formal succession plan, contingency plans, and/or escrow arrangements in place in case repository ceases to operate or substantially changes its scope (i.e., return with adequate prior notification of digital objects to depositors and/or trusted inheritors identified).

MRB-WG Example Evidence Required:

Formal Documents describing exit strategies and contingency plans;
Depositor Agreements;
Testimonials from scenarios already encountered and viability of handling devised scenarios.

MRB-WG Observations:

Again, the 'spacing' of the repository within a larger institutional context will determine to a great extent the viability of these plans and arrangements.

Escrow arrangements themselves would need to be monitored especially where they involve third parties.

A2. Organisation Structure and Staffing

A2.1. Repository staff have skills and expertise appropriate to their duties.

MRB-WG Revised A2.1. Repository has identified and established the duties that it needs to perform and appointed staff equipped with adequate skills and expertise to fulfil these duties.

MRB-WG Example Evidence Required:

Organisational Chart;
Job Descriptions.

MRB-WG Observations:

Before the repository can ensure staff are able to perform the duties of the repository the repository has to ensure that it has identified and documented the duties that need to be performed.

A2.2. Repository has appropriate number of staff to support all functions and services designated in agreements with depositors.

MRB-WG Example Evidence Required:

Job Descriptions;
Depositor Agreements;
Evidence from other comparable institutions of staff numbers requirements (no. of staff per object?)

MRB-WG Observations:

Again, vital it is to identify the functions and services that are being offered, before determining the capabilities of the workforce to deliver them.

A2.3. Repository commits to professional development to keep staff expertise and skills current.

MRB-WG Revised A2.3. Repository has an active professional development programme in place which provides staff with skills and expertise development opportunities.

MRB-WG Example Evidence Required:

Expenditure (€ per staff-member);
Planning documents;
Awarded certificates.

MRB-WG Observations:

“Commitment” is not a firm enough concept. It is easy to be committed to doing something. We need to measure the actual training opportunities delivered.

A3. Procedural Accountability and Policy Framework

A3.1. Repository has a mechanism in place for reviewing, updating, and developing comprehensive policies and procedures as repositories grow and as the community practice evolves.

MRB-WG Revised A3.1. Repository has procedures and policies in place, and mechanisms for their review, update, and development as the repository grows and as the community practice evolves.

MRB-WG Example Evidence Required:

Procedure and policy documents;
Documentation detailing review, update and development mechanisms.

MRB-WG Observations:

Again, it's vital to establish the existence of appropriate procedures and policies as well as the associated mechanisms be validated.

A3.2. Repository has monitoring and feedback mechanisms in place to ensure continued operation, support problem resolution, and address evolving requirements of providers and consumers.

MRB-WG Example Evidence Required:

Evidence of workflow for feedback (i.e. how is feedback used and managed?);
Evidence of quality assurance - how is this related to feedback?

MRB-WG Observations:

There are multiple audiences requiring feedback and monitoring. This should be made more explicit.

A3.3. Repository is committed to formal, periodic review and assessment to ensure continued development.

MRB-WG Example Evidence Required:

Self-assessment documents;
Timetables for review and certification;
Evidence of implementation of outcomes of review;
Some repositories may be assessed by principal depositors - is there evidence of this?

MRB-WG Observations:

Again the word 'committed' is too weak.

A3.4. Repository has a documented history of the changes to its operations, procedures, software, hardware, traceable to its preservation strategies where appropriate.

MRB-WG Example Evidence Required:

Object level preservation metadata;
Repository's records retention strategy document.

MRB-WG Observations:

How long do we expect institutions to maintain the documentation?
To what standard should it be maintained?
Will this information not be incorporated within OAIS Preservation Description Information?

A3.5. Repository commits to transparency and accountability in all actions supporting the operation and management of the repository.

MRB-WG Revised A3.5. Repository guarantees *audit-level* transparency and accountability in all actions supporting the operation and management of the repository.

MRB-WG Example Evidence Required:

Unhindered access to content and associated information within repository.

MRB-WG Observations:

'Transparency' is ambiguous - one assumes this means transparency for audit, and does not necessarily exclude archives with confidential content from fulfilling their mandate to keep this secure.

A3.6. Repository commits to define, collect, track, and provide on demand, its information integrity measurements.

MRB-WG Example Evidence Required:

Policy and workflow documentation.

MRB-WG Observations:

What are information integrity measures?
What processes might an organisation put in place for collecting, tracking and providing these?
How is the application of these processes validated or instantiated?

A3.7. Repository commits to a regular schedule of certification and to notifying certifying bodies of operational changes that will change or nullify its certification status.

MRB-WG Example Evidence Required:

Certificates awarded following certification;
 For example, presence in a certification register;
 Future commitment as evidenced in timetable/budget allocation for certification.

MRB-WG Observations:

This perhaps confuses evidence with process – is this criterion really necessary?

A4. Financial sustainability**A4.1. Repository has a short- and long-term business planning process in place to support sustainability.**

MRB-WG Revised A4.1. Repository has short- and long-term business planning processes in place designed to promote sustainability.

MRB-WG Example Evidence Required:

Experience of comparable institutions;
 Financial audit reports;
 Annual financial report;
 Business plan;
 Exposure of business plan to scenarios.

MRB-WG Observations:

Does repository enjoy financial autonomy (see 'spacing' of mission statement in A1.1)? Does it exhibit sufficient control to determine its own financial sustainability?

A4.2. Repository has in place at least annual processes to review and adjust business plans as necessary.**MRB-WG Example Evidence Required:**

Recent audits and evidence of their impact on repository operating procedures.

MRB-WG Observations:**A4.3. Repository business planning and practices are transparent, compliant with relevant accounting standards and practices, and auditable.**

MRB-WG Revised A4.3. Financial practices and procedures are transparent, compliant with relevant accounting standards and practices, and audited by third parties in accordance with territorial legal requirements..

MRB-WG Example Evidence Required:

Evidence of financial audits already taking place;

MRB-WG Observations:

This criterion should be divided into two sections since financial auditing is a different, very specific thing that is quite distinct from business planning practices. The first part fits more comfortably in A4.2 (up to "transparent") while the latter part should concentrate more on accounting issue.
 Third party auditing will depend on the legal jurisdiction within which the repository operates.

A4.4. Repository has ongoing commitment to risk, benefit, investment, and expenditure analysis and reporting (including assets, licenses, and liabilities).

MRB-WG Example Evidence Required:

Risk register;
Evidence of revision based on risk.

MRB-WG Observations:

Risk/Benefit extends beyond simply financial areas.

A4.5. Repository recognizes the eventual strong possibility of a gap between repository-generated funding and the funding necessary to meet the repository's commitments to its depositors. It commits to bridging these gaps by securing funding and resource commitments specifically for that purpose; these commitments can come either from the repository itself or parent organizations, as applicable.

MRB-WG Example Evidence Required:

Financial documents;
Business plan.

MRB-WG Observations:

Is this not redundant - should these assurances not be found within the repository's business plan?

A5. Contracts, Licenses and Liabilities

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.

A5.1. If repository manages, preserves, and/or provides access to digital materials on behalf of another organization, it has and maintains contracts or deposit agreements.

MRB-WG Example Evidence Required:

Deposit agreements themselves;
Evidence of manageability/changeability in the event of changes effected by preservation process.

MRB-WG Observations:

Where are these stored for long term availability?
How are they negotiated and validated?

A5.2 Repository contracts or deposit agreements must specify and/or transfer appropriate preservation rights, as necessary.

A5.2. Repository contracts or deposit agreements must specify and transfer all necessary preservation rights.. If the agreements do not transfer all of them these documents must specify those that are transferred.

MRB-WG Example Evidence Required:

Contracts/deposit agreements.

MRB-WG Observations:

If this point is not superfluous it's certainly woolly - what are "appropriate" contracts and deposit agreements? Arguably satisfied by A5.1.
Please note original omission of trailing period after checklist section numbers from A5.1. to A5.4.

A5.3 Repository tracks and manages copyrights and restrictions on use as required by contract or license.

MRB-WG Revised A5.3. Repository tracks and manages intellectual property rights and restrictions on use as required by contract or license.

MRB-WG Example Evidence Required:

Depositor agreements;
Appropriate Workflow/policy documents.

MRB-WG Observations:

We concluded that IPR is much more appropriate and a more inclusive term than copyrights;
Any software stored may be subject to additional legal restrictions and these too must be recorded;

A5.4 If repository ingests digital content with unclear ownership/rights, it has policies addressing liability and challenges to those rights.

MRB-WG Revised A5.4. If repository ingests digital materials with unclear ownership/rights, it has policies in place for addressing liability and challenges that may arise as a result.

MRB-WG Example Evidence Required:

Appropriate policies.

MRB-WG Observations:

How is the suitability of a policy measured?
Different strategies might exist - can these be evaluated? (e.g an AV archive may commit resources to contingency fund to react to IPR challenges, instead of spending to track this information).

B. Repository Functions, Processes & Procedures**B1. Ingest/acquisition of content****B1.1. Repository identifies properties it will preserve for each class of digital object.****MRB-WG Example Evidence Required:**

Depositor agreement;

Workflow and policy documents.

Written definition of properties as agreed in the Producer/Depositor contract and which is appropriately respected in ingest procedure and AIP definition;

MRB-WG Observations:

What is a class of digital object? Formats? Semantic grouping? Those sharing properties?

There is no general classification of digital objects which has been widely adopted. Until one is widely adopted each repository will need to have its own appropriate classification. Each particular case must document the difference (deviance) between the class characteristics in the particular ingest procedure and the particular AIP definition.

B1.2. Repository has specified all appropriate aspects of acquisition, maintenance, access, and withdrawal issues in written agreements with depositors.**MRB-WG Example Evidence Required:**

Deposit agreements.

Minimal elements that should be covered in a deposit agreement include:

- property rights
- access rights
- conditions for withdrawal
- level of security
- level of finding aids
- SIP definitions
- time, volume and content of transfers

MRB-WG Observations:

This is redundant, representing no more than a more detailed coverage of A5.1.

B1.3. Repository has an identifiable, written definition for each SIP or class of information ingested by the repository.

MRB-WG Revised B1.3. Repository has a clear specification as to the information that needs to be associated with digital material at the time of its deposit (for example, SIP).

MRB-WG Example Evidence Required:

Details of information that is required to accompany deposited material.

MRB-WG Observations:

The proposed rewording disentangles the checklist from OAIS, although maintains value of terminology as an example.

B1.4. Repository has a process to ensure that the information is acquired from the expected source.

MRB-WG Revised B1.4. Repository has mechanisms to validate that material has come from the source that purports to be its origin.

MRB-WG Example Evidence Required:

Workflow documents;
Evidence of appropriate technological measures (e.g. checksums or MD5)
Logs from procedures and authentications

MRB-WG Observations:

The proposed rewording adds clarity to the point.

B1.5. Repository obtains sufficient physical control over the digital objects to preserve them.

MRB-WG Revised B1.5. Repository produces evidence that its ingest process supports the its verification that each ingested object (e.g. SIP) is as complete as promised by the originating institution within the relevant deposit agreement.

MRB-WG Example Evidence Required:

Workflow documents;
Deposit agreements;
System log files from system performing ingest procedures.

MRB-WG Observations:

We feel that the original questions B1.5. and B1.6. would benefit from a reversal, reflecting the chronological process of ingest.

B1.6. Repository's ingest process verifies each SIP for completeness and correctness.

MRB-WG Revised B1.6. Repository obtains sufficient physical control over the digital objects to preserve them; this may be achieved through analysis of the digital content; verification, analysis and creation of metadata; authentication and integrity checking; or by the creation of an archival object incorporating the data content and associated metadata within the repository (e.g. AIP).

MRB-WG Example Evidence Required:

Appropriate policy documents.
System log files from system performing ingest procedure.

MRB-WG Observations:

Partly redundant if neighbouring questions are satisfied;
The notes accompanying this are quite extensive, and this ought to be reflected within the checklist itself, which may be available only in isolation.
Once again, please note the reversal of questions B1.5. and B1.6.

B1.7. Repository provides producer/depositor with appropriate responses at predefined points during the ingest processes.

MRB-WG Example Evidence Required:

Depositor agreement;
Evidence of reporting back.

MRB-WG Observations:

This should be redundant, since it is predefined in the deposit agreement.
If repository cannot preserve material in the terms they have laid out within the deposit agreement they must renegotiate terms with depositor (or even recommend that the depositor place its material with another repository)

B1.8. Repository can demonstrate that all SIPs are either accepted as whole or part of an eventual AIP, or otherwise disposed of in a recorded fashion.

MRB-WG Revised B1.8. Repository can demonstrate that all submitted objects (e.g. SIPs) are either accepted as whole or part of an eventual archival object (e.g. AIP), or otherwise disposed of in a recorded fashion.

MRB-WG Example Evidence Required:

Disposal records;
System log files.

MRB-WG Observations:

B1.9. Repository can demonstrate when preservation responsibility is formally accepted for the contents of the AIP.

MRB-WG Revised B1.9. Repository can demonstrate if and when preservation responsibility is formally accepted for the contents of the archival object (e.g. AIP).

MRB-WG Example Evidence Required:

Deposit agreements;
Confirmation/receipt sent back to depositor.

MRB-WG Observations:

B2. Archival storage: management of archived information

B2.1. Repository has an identifiable, written definition for each AIP or class of information preserved by the repository.

MRB-WG Revised B2.1. Repository has an identifiable, written definition for each archival object (e.g. AIP) or class of information preserved by the repository.

MRB-WG Example Evidence Required:

Written definitions (within preservation metadata?)

MRB-WG Observations:

B2.2. Repository has a definition of each AIP (or class) that is adequate to fit long-term preservation needs.

MRB-WG Revised B2.2. Repository has a definition of each archival object (e.g. AIP) or class of object that is adequate to fit long-term preservation needs.

MRB-WG Example Evidence Required:

Existing benchmark evidence: what is necessary for "long term"?
Deposit agreements that determine what's meant by "long term"?
Community consensus

MRB-WG Observations:

Can this be truncated into point B2.1?

B2.3. Repository has a definition of how AIPs are derived from SIPs

MRB-WG Revised B2.3. Repository has a validated description of the process whereby archival objects (e.g. AIPs) are constructed from submitted objects (e.g. SIPs).

MRB-WG Example Evidence Required:

Process description documents.

MRB-WG Observations:

Partly redundant following criterion that deal with ingest process. We suggest that the word 'derived' is not precise because an AIP is not necessarily a subset of a SIP indeed it is likely to include the SIP and substantial quantities of additional information. We would therefore suggest that the word 'constructed' be used instead.

B2.4. Repository has and uses a naming convention that can be shown to generate visible, unique IDs for all AIPs.

MRB-WG B2.4. Repository has and uses a naming convention that can be shown to generate visible, persistent and unique IDs for all archival objects (e.g. AIPs).

MRB-WG Example Evidence Required:

Documentation describing naming convention and physical evidence of its application.

MRB-WG Observations:

Added a stress on the concept of persistent.

B2.5. If unique identifiers are associated with SIPs before ingest, they are preserved in a way that maintains a persistent association with the resultant AIP.

MRB-WG Revised B2.5. If unique identifiers are associated with submitted objects (e.g. SIPs) before ingest, they are preserved in a way that maintains a persistent association with the resultant archival object (e.g. AIP).

MRB-WG Example Evidence Required:

Workflow documents and evidence of traceability.

MRB-WG Observations:

.

B2.6. Repository verifies each AIP for completeness and correctness when generated.

MRB-WG Revised B2.6. Repository verifies each archival object (e.g. AIP) for completeness and correctness at the point it is generated.

MRB-WG Example Evidence Required:

Description of procedure that verifies completeness and correctness;
Logs of all instances where procedure is performed.

MRB-WG Observations:

Completeness and correctness ought to be determined with respect to the archival object and its intrinsic preservation description information. If this is the case then B2.6 is redundant.

B2.7. Repository provides an independent mechanism for audit of the integrity of the repository collection/content.

MRB-WG Revised B2.7. Repository provides evidence of access to suitable verification mechanisms and services, such as representation information registries and an independent mechanism for audit of the integrity of the repository collection/content.

MRB-WG Example Evidence Required:**MRB-WG Observations:****B3. Preservation planning, migration, & other strategies****B3.1. Repository has documented preservation strategies.****MRB-WG Revised B3.1. Repository employs documented preservation strategies.****MRB-WG Example Evidence Required:**

Documentation and evidence of application (e.g. in preservation metadata).

MRB-WG Observations:**B3.2. Repository implements/responds to strategies for AIP storage and migration.****MRB-WG Revised B3.2. Repository implements/responds to strategies for archival object (e.g. AIP) storage and migration.****MRB-WG Example Evidence Required:**

Technology/standards watch.

MRB-WG Observations:

Why is migration the only preservation strategy that the checklist focuses on?

B3.3 Repository uses appropriate international representation information [including format] registries**MRB-WG Revised B3.3. Repository demonstrates that it has access to necessary tools and resources to establish semantic or technical context of the digital objects it contains (e.g. access to appropriate representation information or format registries).****MRB-WG Example Evidence Required:**

Evidence of e.g. subscription to such repositories.

MRB-WG Observations:

Repositories should maintain all format information in house to maintain its independent ability to verify and check formats or other technical or semantic details associated with an archival object

B3.4. Repository records/registers representation information [including formats] ingested**MRB-WG Revised B3.4. Repository records/registers representation information [including formats] ingested.****MRB-WG Example Evidence Required:****MRB-WG Observations:**

B3.5. Repository preserves the content information of AIPs.

MRB-WG Revised B3.5. Repository preserves the content information of archival objects (e.g. AIPs).

MRB-WG Example Evidence Required:

MRB-WG Observations:

B3.6 Repository acquires Preservation Description Information for its associated content information.

MRB-WG Revised B3.6. Repository acquires preservation metadata (e.g. PDI) for its associated content information.

MRB-WG Example Evidence Required:

MRB-WG Observations:

Amended inconsistent terminology: acronyms should be expanded (or not) on a consistent basis

B3.7. Repository actively monitors AIP integrity.

MRB-WG Revised B3.7. Repository actively monitors the integrity of archival objects (e.g. AIPs)it holds.

MRB-WG Example Evidence Required:

MRB-WG Observations:

B3.8. Repository has contemporaneous records of actions taken associated with ingest and archival storage processes and those administration processes which are relevant to the preservation.

MRB-WG Revised B3.8. OMIT.

MRB-WG Example Evidence Required:

MRB-WG Observations:

This is redundant, since every time maintenance is undertaken a new archival object (AIP) is created, and the documentation is intrinsic.

B3.9. Repository has mechanisms in place for monitoring and notification when format (or other representation information) obsolescence is near/or are no longer viable.

MRB-WG Example Evidence Required:

MRB-WG Observations:

Difficult to provide evidence of ormeasure the mechanisms to change preservation plans - means to prove the maintenance of knowledge about emerging standards.

B3.10. Repository has mechanisms to change its preservation processes as a result of its monitoring activities.

MRB-WG Example Evidence Required:

MRB-WG Observations:

B3.11. Repository can provide evidence of the success of its preservation planning

MRB-WG Revised B3.11. Repository can provide evidence of the effectiveness of its preservation planning.

MRB-WG Example Evidence Required:

MRB-WG Observations:

Difficult to measure, other than in a negative sense.

B4. Data Management

B4.1. Repository captures or creates this minimum descriptive metadata and ensures it is associated with the AIP

MRB-WG Revised B4.1. Repository captures or creates an adequate set of descriptive metadata and validates its association with the archival object (e.g. AIP).

MRB-WG Example Evidence Required:

MRB-WG Observations:

B4.2. Repository can demonstrate that referential integrity is created between all AIPs and associated descriptive information.

MRB-WG Revised B4.2. Repository can demonstrate that cohesive bonds are created between all archival objects (e.g. AIPs) and associated descriptive information.

MRB-WG Example Evidence Required:

MRB-WG Observations:

Why are questions B4.2 and B4.3 separated into two separate points on the checklist, whereas elsewhere, for instance in question A5.1. a similar two part point is truncated into a single question?

B4.3. Repository can demonstrate that referential integrity is maintained between all AIPs and associated descriptive information.

MRB-WG Revised B4.3. Repository can demonstrate that cohesive bonds are maintained between all archival objects (e.g. AIPs) and associated descriptive information.

MRB-WG Example Evidence Required:

MRB-WG Observations:

See comments for B4.2.

B5. Access Management

B5.1. Repository access management system fully implements access policy

MRB-WG Revised B5.1. Repository access management system fully implements access management policies.

MRB-WG Example Evidence Required:
Measuring compliance here is extremely onerous -

MRB-WG Observations:

Which access policy is referred to here? Is it the depositor's, archive's or customers'?
Is the level of service offered by the repository really a certifiable characteristic in terms of trust?
Certification must distinguish (at least) three levels of access which will determine lengths to which repositories must go to qualify. Suggestions are **open access** (low responsibility), **conditional access**, whereby privacy and intellectual property laws are protected (medium responsibility) and **paid for access** (high responsibility).
Full stop omitted.

B5.2. Repository logs all access management failures, and staff review inappropriate "access denial" incidents.

MRB-WG Revised B5.2. Repository logs all access attempts, and reviews all 'access denial' incidents.

MRB-WG Example Evidence Required:

MRB-WG Observations:

It is felt that this consideration is unnecessary for open archives; see the distinction between access types raised in observations for section B5.1.

B5.3. Repository can demonstrate that the process that generates the DIP is complete in relation to the request.

MRB-WG Revised B5.3. Repository can demonstrate that the process that generates the dissemination object (e.g. DIP) is complete in relation to the request.

MRB-WG Example Evidence Required:

MRB-WG Observations:

It is difficult to valid compliance with this criterion as it is difficult to define all classes of requests future users are likely to submit.

B5.4. Repository can demonstrate that the process that generates the DIP is correct in relation to the request.

MRB-WG Revised B5.4. Repository can demonstrate that the process that generates the dissemination object (e.g. DIP) is correct in relation to the request.

MRB-WG Example Evidence Required:

MRB-WG Observations:

B5.5. Repository must demonstrate that all access requests result in a response of acceptance or rejection.

MRB-WG Example Evidence Required:**MRB-WG Observations:**

Is this really necessary to ensure the repository's *trusted* status?

B5.6. Repository enables the dissemination of authentic copies of the original or objects traceable to originals

MRB-WG Revised B5.6. Repository can demonstrate that copies can be traced back to their corresponding originals.

MRB-WG Example Evidence Required:**MRB-WG Observations:**

In its original form this requirement is irrefutably reasonable, but questions persist as to how it might be implemented or evidenced. Digital signing? Authenticity measures?

Although we did not address this in response to this criterion the use of the terms 'copies' and 'original' is a point of concern as there is widespread realisation that neither of these concepts are applicable in the digital realm.

C. Designated Community and the Usability of Information

C1. Documentation

C1.1. Repository has a documented definition of its designated community/ies--who it consists of, its knowledge base, what levels of service it expects, etc.

MRB-WG Revised C1.1. Repository has a documented definition of its designated community/ies--who it consists of, its knowledge base, and what levels of service the community expects.

MRB-WG Example Evidence Required:

MRB-WG Observations:

Is a designated community (designed seemingly as a shorthand means of preservation) an appropriate concept in this context? Can one reasonably expect to be able to monitor a designated community for the lifetime of a digital object's usefulness? Is limiting the maintained information likely to cause problems if alternative groups develop an interest in the stored resources?

Suggest removal of "etc" which serves only to increase this section's ambiguity.

Amid inconsistency in capitalisation with designated community we suggest a blanket use of the lower case version, in order to disentangle the checklist from exclusively OAIS applicability.

C1.2. Repository makes the definition of its Designated Communities available.

MRB-WG Revised C1.2. Repository makes the definition of its designated communities available.

MRB-WG Example Evidence Required:

Definition of designated communities.

MRB-WG Observations:

Why must this be published to engender trust? Perhaps as peace of mind to depositors and users, but this is more of an evidential means of demonstrating that the repository knows and understands the community or communities they serve. This is the vital point here.

C1.3. Repository defines, communicates, and commits to a definition of "understandability" with its Designated Community.

MRB-WG Revised C1.3. Repository defines, communicates, and commits to a definition of "understandability" with its designated community.

MRB-WG Example Evidence Required:

Definition of understandability (e.g. in depositor agreements)

MRB-WG Observations:

It might be argued that generic understandability to a reasonable lay-person is a more vital goal than to a specific community. Obviously the latter might be defined to encompass everyone, but there are dangers in catering only for a single perceived group whose ranks may be joined in the future by those with radically a different knowledge base or level of insight. How can future understandability be assured?

C2. Descriptive Metadata Appropriate to Designated Community

C2.1. Repository articulates minimum metadata requirements to enable the Designated Community to discover and identify material of interest.

MRB-WG Revised C2.1. Repository articulates minimum metadata requirements to enable the designated community to discover and identify material of interest.

MRB-WG Example Evidence Required:

Discovery metadata records.

MRB-WG Observations:

It is thought that the discovery methods offered by the repository are completely outwith the scope of a checklist that seeks to determine degrees of trust.

C3. Use and Usability

C3.1. Repository documents and communicates to its designated community what access and delivery options are available.

MRB-WG Example Evidence Required:

Again, the stated documents.

MRB-WG Observations:

Once more, is this a crucial consideration for the assessment of trust?

C3.2. 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.

MRB-WG Revised C3.2. Repository has implemented a policy for recording all access actions (includes requests and orders) that meet the requirements of the repository and information producers/depositors.

MRB-WG Example Evidence Required:

Appropriate policy documents.

MRB-WG Observations:

Use of "etc" is inappropriate.

Unnecessary indent.

C3.3. Repository ensures that agreements applicable to access conditions are adhered to.

MRB-WG Revised C3.3. Repository can demonstrate it adheres to agreements applicable to access conditions.

MRB-WG Example Evidence Required:

Deposit agreements;

Workflow and policy documents.

MRB-WG Observations:

C3.4. Repository has documented and implemented access policies (authorization rules, authentication requirements) consistent with deposit agreements for stored objects.

MRB-WG Revised C3.4. Repository has documented and implemented access policies (authorization rules, authentication requirements) capable of meeting terms established in deposit agreements.

MRB-WG Example Evidence Required:

Deposit agreements and workflow/policy documents.

MRB-WG Observations:

The repository's policies are established prior to the deposit agreements; the latter does not define policies, instead fits within their parameters. If the situation were reversed then an audit of policy today would be potentially irrelevant tomorrow.

C4. Verifying Understandability

C4.1. Repository has a documented process to test 'understandability to the Designated Community', as previously defined, of the information content associated with the Content Information and PDI and this includes defining the appropriate steps necessary should the agreed level of 'understandability' not be met.

MRB-WG Revised C4.1. Repository has a documented process to test 'understandability' of the information content associated with the content and preservation metadata (e.g. PDI), and this includes defining the appropriate steps necessary should the agreed level of 'understandability' not be met.

MRB-WG Example Evidence Required:**MRB-WG Observations:**

C4.2. Repository has verified that Content Information and PDI are understandable to Designated Community.

MRB-WG Revised C4.2. Repository has verified that content and preservation metadata (e.g. PDI) are understandable to designated community or communities.

MRB-WG Example Evidence Required:

Community testimony;
Preservation metadata;
Access workflow.

MRB-WG Observations:

Again, we have concerns over just ensuring understandability to a specific group that may not represent the full extent of a potential user base.

D. Technologies & Technical Infrastructure

D1. System infrastructure

D1.1. Repository functions on well-supported operating systems and other core infrastructural software.

MRB-WG Revised D1.1. Repository has appropriate operating systems and adequate core software infrastructure in place in order to satisfy its goals as outlined in its mission statement.

MRB-WG Example Evidence Required:

Benchmarking evidence;
Software inventory/system documentation.

MRB-WG Observations:

“Well supported” is an extremely vague term, and no insights are offered as to how this might be measured. Similarly, what is meant by “core infrastructural software”?
Unnecessary indent.

D1.2. Repository ensures that all platforms have a backup function, sufficient for the repository's services and for the data held (e.g., metadata associated with access controls, repository main content, etc.)

MRB-WG Revised D1.2. Repository ensures that all platforms have a backup function, sufficient for the repository's services and for the data held (e.g., metadata associated with access controls and repository main content).

MRB-WG Example Evidence Required:

This should be associated with a disaster recovery plan.

MRB-WG Observations:

Risk of backup (redundancy and security fears) must be measured in a disaster recovery plan or risk/benefit table. Therefore backup function must support disaster recovery and ensure as far as possible that institution is not exposed to risk, but at the same time it must not expose the organisation to risk. Once again, “etc” has no place within this kind of document.

D1.3. Repository stipulates the number and location of copies of all digital objects.

MRB-WG Revised D1.3. Repository manages the number and location of representations of all digital objects and their status.

MRB-WG Example Evidence Required:

Repository inventory;
Workflow/process documentation.

MRB-WG Observations:

We would recommend the use of “manages” rather than “stipulates” in this point.
Again we think the use of the word copy is inappropriate and we suggest that representations be used.

D1.4. Repository has mechanisms in place to insure any/multiple copies of digital objects are synchronized.

MRB-WG Revised D1.4. Repository has mechanisms in place to ensure any/multiple representations of digital objects are synchronized.

MRB-WG Example Evidence Required:

Workflow/process documentation.

MRB-WG Observations:

“Copies” is a loose term in this context, given the diverse means by which digital content is stored on disparate media types. The chosen media will determine some of the characteristics of its hosted digital objects. We would therefore prefer if the term “representations” is used.

Replaced “insure” with “ensure”.

D1.5. Repository has effective mechanisms to detect data corruption or loss.

MRB-WG Revised D1.5. Repository has effective and documented mechanisms to test for and detect data corruption or loss.

MRB-WG Example Evidence Required:

Appropriate documentation.

MRB-WG Observations:

We suggest promoting the importance of documenting these mechanisms and also that data corruption ought to be tested for by the institution, lessening the strain on a single detection process.

D1.6. Repository reports to its administration all incidents of data corruption or loss, and steps taken to repair/replace corrupt or lost data.

MRB-WG Revised D1.6. Repository reports to its administration and depositors all incidents of data corruption or loss, and steps taken to repair/replace corrupt or lost data.

MRB-WG Example Evidence Required:

Preservation metadata (e.g. PDI) records.

MRB-WG Observations:

Depositors should also be alerted to these circumstances;

We feel that the preservation metadata (e.g. PDI) ought to contain the details of repairs that have been undertaken.

D1.7. Repository has defined processes for storage media migration.

MRB-WG Revised D1.7. Repository has defined processes for storage media change (e.g., refreshing, migration).

MRB-WG Example Evidence Required:

Documented processes.

MRB-WG Observations:

Use of “migration” is unnecessarily limiting; refreshing is an alternative. Therefore, we prefer the use of the term “storage media change”.

D1.8. Repository has a documented change management process that identifies changes to critical processes.

MRB-WG Revised D1.8. Repository has a documented change management process that identifies changes to critical processes that effect the repository’s ability to comply with the the terms of depositor agreements.

MRB-WG Example Evidence Required:

Documentation of change management process.

MRB-WG Observations:

This should be given higher prominence within this section, and extended to encompass every aspect of system change;

Preservation metadata must log changes undertaken;

The impact of these changes must be considered, evaluated and documented;

Depositor agreements will influence these changes.

Unnecessary indent.

D1.9. Repository has a process for testing the effect of critical changes to the system.

MRB-WG Revised D1.9. Repository has a process for simulating critical changes to the system, testing their impact and validating the correctness of prior simulations.

MRB-WG Example Evidence Required:

Documented test procedures.

MRB-WG Observations:

Repository must be capable of not only testing the impact of changes but also methodically predicting their impact prior to deployment.

D1.10. Repository has a process to stay current with the latest operating system security fixes.

MRB-WG Revised D1.10. Repository has a process to react to the availability of new software security updates based on a risk-benefit assessment.

MRB-WG Example Evidence Required:

Risk register;

Evidence of update processes (e.g. server update manager daemon)

MRB-WG Observations:

This must be the outcome of a risk-benefit assessment; security patches are frequently responsible for upsetting alternative aspects of system functionality or performance. It may not be necessary for a repository to implement all software patches, and the application of any must be based on reflective decision making

Unnecessary indent.

D2. Appropriate technologies

D2.1. Repository has hardware technologies appropriate to the services it provides to its designated communities and has procedures in place to monitor and receive notifications when hardware technology changes are needed.

MRB-WG Revised D2.1. Repository has hardware technologies appropriate to the services it commits to in its mission statement and has procedures in place to monitor, receive notifications, and evaluate when hardware technology changes are needed.

MRB-WG Example Evidence Required:

Technology watch efforts;

Organisation chart;

Technical Questionnaire;

Hardware Register.

MRB-WG Observations:

D2.2. Repository has software technologies appropriate to the services it provides to its designated communities and has procedures in place to monitor and receive notifications when software technology changes are needed.

MRB-WG Revised D2.2. Repository has software technologies appropriate to the services it commits to in its mission statement and has procedures in place to monitor, receive notifications, and evaluate when software technology changes are needed.

MRB-WG Example Evidence Required:

Technology watch efforts;
Technical Questionnaire;
Software Register.

MRB-WG Observations:

It is felt that this stipulation overlaps sufficiently to render sections D1.1. and D1.10. redundant. This kind of overlap is in evidence in several sections of the checklist. We considered eliminating redundancy, but wondered whether it was intended to provide a means of cross-checking?

D2.3. Repository has procedures in place for monitoring or receiving notifications about changes in the needs of its Designated Communities (e.g., surveys, formal reviews, workshops and individual interactions).

MRB-WG Revised D2.3. Repository has procedures in place for monitoring or receiving notifications about changes in the needs of the designated communities served by the repository.

MRB-WG Example Evidence Required:

Records of designated community interactions;
Evidence of consequences of interactions.

MRB-WG Observations:

This criterion would fit better in section C, which deals explicitly with the designated community.

D3. Security

D3.1. Repository maintains a systematic analysis of its environment: data, systems, personnel, physical plant, security needs, etc.

MRB-WG Revised D3.1. Repository maintains a systematic analysis of such factors as data, systems, personnel, physical plant and security environment.

MRB-WG Example Evidence Required:

ISO 17799 compliance;
Analysis output.

MRB-WG Observations:

The section on security ought to be modularised as an expression of ISO 17799 conformance - Also, why use technical terminology from one ISO standard (OASIS) but omit that contained in ISO 17799? Again, the use of "etc" does not help the reader.

D3.2. Repository has implemented mechanisms (processes) to adequately address each of the defined security needs.

MRB-WG Example Evidence Required:

System workflow diagram;
ISO 17799 compliance;
Evidence of process from analysis to reactionary implementation.

MRB-WG Observations:

D3.3. Repository staff have delineated roles, responsibilities, and authorizations.

MRB-WG Example Evidence Required:

Organisational Chart;
Job Descriptions

MRB-WG Observations:

Is this not satisfied already in a general sense in section A? If this is the case then it is redundant and can be deleted.

D3.4. Repository has written disaster preparedness and recovery plan(s) (including at least one off-site copy of all deposited data).

MRB-WG Revised D3.4. Repository has suitable written disaster preparedness and recovery plan(s) (including at least one off-site representation of all deposited data).

MRB-WG Example Evidence Required:

Plans themselves;
Depositor agreements (to determine the suitability of these plans).

MRB-WG Observations:

Again, this will depend to some extent on the hierarchical spacing of the repository within its parent organisation, and the level of autonomy that it can realistically expect to command.

D3.5. Repository tests disaster plans regularly.

MRB-WG Revised D3.5. Repository tests and where necessary updates disaster plans on a regular basis.

MRB-WG Example Evidence Required:

Test log;
Evidence of refinement of disaster plans based on outcomes of testing.

MRB-WG Observations:

D3.6. Repository has defined processes for service continuity and disaster recovery.

MRB-WG Revised D3.6. Repository has defined suitable processes for service continuity and disaster recovery.

MRB-WG Example Evidence Required:

Defined processes themselves;
Depositor agreements to determine suitability within context of agreement.

MRB-WG Observations:

Again, having the processes is less important than their suitability in terms of depositor agreements; This would seem to be more appropriate in section A, in a section proposed by MRB-WG entitled **Risk**.

Appendix B: Examples Documents to Request in Advance of Audit

Document Name:	Repository Mission Statement
Definition:	The document detailing the overall mission of the repository, and if the repository is part of a larger organisation its spacing within the parent organisation.
Why?:	To provide evidence of a commitment to the long-term retention and management of digital information on behalf of depositors

Document Name:	Example Deposit Agreements
Definition:	Example documents describing the relationship between depositor and repository, the responsibilities undertaken, the level of service expected and the legal rights and responsibilities of the parties involved.
Why?:	To provide evidence of suitability of repository functions, and contractual controls.

Document Name:	Job Descriptions
Definition:	Documents detailing the roles and responsibilities of each member of the repository staff.
Why?:	To provide evidence of the existence of sufficient roles to satisfy goals outlined in the mission statement and depositor agreements.

Document Name:	Organisational Chart
Definition:	Document detailing the roles and responsibilities of staff and how they relate to each other.
Why?:	Further evidence of the existence of appropriate roles and interactions.

Document Name:	Annual Financial Report
Definition:	Document detailing expenditure and income from the preceding accounting period.
Why?:	Evidence of sound financial footing and planning.

Document Name:	Business Plan
Definition:	A document detailing the financial, organisational and methodological basis for the repository, providing a justification for its existence and a plan to ensure its persistence.
Why?:	Evidence of long-term organisational sustainability including issues such as plans for self-sustainability. This will also indicate the repository's spacing within a larger, parent organisation.

Document Name:	Job Descriptions
Definition:	Descriptions of the jobs within the organisation.
Why?:	Provides a mechanism for mapping between the organisational objectives and the mechanisms for delivering them.

Document Name:	Staff Profiles
Definition:	Overview of experience and expertise of key members of staff.
Why?:	Provide evidence of suitability of individuals performing key tasks within the repository.

Document Name:	Policy Documents
Definition:	Documents detailing repository's policy in key areas. Example policies will cover acquisitions, preservation strategies, means of identifying objects, access and disaster recovery.
Why?:	Provide a range of insights illustrating the means by which the repository performs particular functions, provides particular services, and reacts to a range of circumstances.

Document Name:	Procedure Manuals
Definition:	Detailed documents describing procedures carried out by the repository. Example procedures include backup, data checking, storage media change, and system maintenance.
Why?:	Provides evidence of policy in more practical terms.

Document Name:	Workflow Models
Definition:	Detailed documents describing interrelation of activities central to the repository's operation.
Why?:	These ought to provide insights into the path of a deposited object through the repository and indicate the ways in which external influences such as emerging preservation approaches, shortcomings identified during testing procedures, and customer expectations can impact on digital materials within the repository.

Document Name:	Technical Architecture
Definition:	Document describing the hardware and software infrastructure that provides a technical foundation for the repository's functionality.
Why?:	Provides evidence of suitability of hardware and software infrastructures to support effectively the functions and services aspired to in both the mission statement and individual depositor agreements.

Document Name:	System Handbooks
Definition:	Detailed documentation describing the operation of repository systems.
Why?:	Provides evidence that technology is sufficiently extensive to meet repository's functional requirements.

Document Name:	Maintenance Reports
Definition:	Documentation describing maintenance that has been undertaken within the system. This should include the application of security and functionality upgrades and the repair or replacement of corrupt or lost data objects.
Why?:	Enables the auditors to determine the effectiveness of the team and the quality of service that the repository can provide.

Document Name:	Certification Documents
Definition:	Documents awarded by an accredited certification body or self-conferred following a formal self-assessment process.

Why?:	Evidence of existing success in audits, and of a greater commitment to the audit and certification process.
-------	---

Appendix C: Individuals for Audit Interviews

The following tables indicated the individuals that we will seek input from during the process of audit. Needless to say, depending on the size of the institution, in many cases two or more of these individuals may well be the same person.

Representative Name:	Head of Repository
Description:	The person in charge of the repository's operation.
Rationale/Process:	On-site interview (detailed in pre-written semi-structured questionnaire)

Representative Name:	Individual Responsible for Hardware
Description:	Technical Team Leader responsible for design, implementation and maintenance of repository hardware.
Rationale/Process:	On-site interview (detailed in pre-written semi-structured questionnaire)

Representative Name:	Individual Responsible for Software
Description:	Technical Team Leader responsible for design, implementation and maintenance of repository software.
Rationale/Process:	On-site interview (detailed in pre-written semi-structured questionnaire)

Representative Name:	Individual Responsible for Ingest Procedure
Description:	The individual that accepts submitted objects (e.g. SIPs), validates them, and prepares them for archival storage.
Rationale/Process:	On-site interview (detailed in pre-written semi-structured questionnaire)

Representative Name:	Individual Responsible for Archive and Preservation Procedures
Description:	The individual that is responsible for maintenance of archival objects (e.g. AIPs) and monitoring and applying appropriate preservation processes.
Rationale/Process:	On-site interview (detailed in pre-written semi-structured questionnaire)

Representative Name:	Individual Responsible for Access Provision
Description:	The individual responsible for the delivery of information objects (e.g. DIPs).
Rationale/Process:	On-site interview (detailed in pre-written semi-structured questionnaire)

Representative Name:	Depositors of digital materials
Description:	Representative of projects or organisations responsible for supplying stored content.
Rationale/Process:	Telephone interview (detailed in pre-written semi-structured questionnaire)

Representative Name:	Information Seekers
Description:	Individuals or representatives of projects or organisations interested in retrieving digital information from the repository.
Rationale/Process:	Telephone interview (detailed in pre-written semi-structured questionnaire)