The International Journal of Digital Curation
Issue 2, Volume 3 | 2008

Bringing Self-assessment Home: Repository Profiling and Key Lines of Enquiry within DRAMBORA

Andrew McHugh, Seamus Ross, Perla Innocenti,
HATII, University of Glasgow

Raivo Ruusalepp, Hans Hofman,
National Archive of the Netherlands

October 2008

Summary

As repositories of various shapes and sizes continue to appear across the digital preservation landscape, means are urgently required to facilitate their evaluation. In what remains an immature discipline there are seldom any assurances of the viability of individual preservation infrastructures, and a pragmatic, risk-averse approach is critically important. The Digital Repository Audit Method Based on Risk Assessment (DRAMBORA) provides repository administrators with a flexible self-audit methodology and online tool, facilitating the validation of their objectives and methods and the management of intrinsic and extrinsic threats. This article introduces DRAMBORA, outlining its respective strengths and describing where it fits into a wider evaluation context.

The *International Journal of Digital Curation* is an international journal committed to scholarly excellence and dedicated to the advancement of digital curation across a wide range of sectors. ISSN: 1746-8256 The IJDC is published by UKOLN at the University of Bath and is a publication of the Digital Curation Centre.

Introduction

Digital repositories are a manifestation of complex organizational, financial, legal, technological, procedural, and political interrelationships. Accompanying each of these are innate uncertainties, exacerbated by the relative immaturity of understanding prevalent within the digital preservation domain. Recent efforts have sought to identify core characteristics that must be demonstrable by successful digital repositories, expressed in the form of check-list documents, intended to support the processes of repository accreditation and certification. In isolation though, the available guidelines lack practical applicability; confusion over evidential requirements and difficulties associated with the diversity that exists among repositories (in terms of mandate, available resources, supported content and legal context) are particularly problematic. A gap exists between the available criteria and the ways and extent to which conformity can be demonstrated.

The Digital Repository Audit Method Based on Risk Assessment (DRAMBORA) is a methodology for undertaking repository self- assessment, developed jointly by the Digital Curation Centre (DCC) and DigitalPreservationEurope (DPE). DRAMBORA requires repositories to expose their organization, policies and infrastructures to rigorous scrutiny through a series of highly structured exercises, enabling them to build a comprehensive registry of their most pertinent risks, arranged into a structure that facilitates effective management. It draws on experiences accumulated throughout 18 evaluative pilot assessments undertaken in an internationally diverse selection of repositories, digital libraries and data centres (including institutions and services such as the UK National Digital Archive of Datasets, the National Archives of Scotland, Gallica at the National Library of France and the CERN Document Server). Other organizations, such as the British Library, have been using sections of DRAMBORA within their own risk assessment procedures.

Despite the attractive benefits of a bottom-up approach, there are implicit challenges posed by neglecting a more objective perspective. Following a sustained period of pilot audits undertaken by DPE, DCC and the DELOS Digital Preservation Cluster aimed at evaluating DRAMBORA, it was stated that had respective project members not been present to facilitate each assessment, and contribute their objective, external perspectives, the results may have been less useful. Consequently, DRAMBORA has developed in a number of ways, to enable knowledge transfer from the responses of comparable repositories, and incorporate more opportunities for structured question sets, or key lines of enquiry, that provoke more comprehensive awareness of the applicability of particular threats and opportunities.

In Search of Means to Engender Trust

Those within the Digital Curation profession charged with information stewardship responsibilities have long sought to establish trustworthy means to manage, preserve and ensure the accessibility of digital materials. The contemporary domain landscape suggests that information repositories are likely to play a role of considerable importance in the pursuit of assurances of trustworthiness. Recent events suggest that decentralization will be part of a natural progression. Within the UK, the decision taken by the Arts and Humanities Research Council (AHRC) in 2007 to discontinue the funding of its Arts and Humanities Data Service (AHDS) appeared to

be based on an assertion that local repository infrastructures could together provide similarly adequate preservation services. In order to legitimize such decisions, it is essential that the community has appropriate mechanisms available to support repository assessment. Trustworthiness as a concept has wide-reaching implications, and influences relationships both internal and external to the repository. Management, staff, financiers and partners must all be satisfied that their efforts are capable of meeting formal expectations. Similarly, information creators, depositors and consumers are naturally interested in obtaining similar assurances of the competencies of the organisations providing maintenance, preservation and dissemination services. On what grounds the AHRC decided that institutional repositories were equipped to continue to do the work previously undertaken by the AHDS remains unclear. Nevertheless, having acknowledged through years of prior investment the importance of information preservation, it is inconceivable that the decision can have been taken without due consideration of the respective capabilities and suitability of both the AHDS as it did exist, and the alternative environments which now appear to have inherited preservation responsibilities.

A number of mainstream reference materials are now available to support the assessment of digital repository environments. Considerable work has been undertaken to develop audit check-lists that will eventually provide an intellectual basis for awarding certification to sufficiently capable repository service providers. There are two principal examples currently available.

Released in 2007, the Trustworthy Repositories Audit and Certification (TRAC) Criteria and Check-list (Center for Research Libraries & RLG OCLC Programs, 2007) was developed by a consortium jointly overseen by the US National Archives and Records Administration (NARA) and the Research Libraries Group (RLG) (prior to its absorption within OCLC), and is now maintained by the Center for Research Libraries. TRAC describes approximately 90 characteristics that must be demonstrable by repositories that aspire to a certifiable, trustworthy status.

The second example, also released last year, adopts a more regionally specific focus. The nestor Catalogue of Criteria for Trusted Digital Repositories (nestor Working Group,.2006) was developed in Germany by the Network of expertise in Digital long-term preservation (nestor). Structured similarly to the TRAC document, this provides examples and perspectives that are more representative of a German operational, legal and economic context. Both TRAC and nestor are examples of a top-down assessment philosophy. Both seek to define an objective consensus of the priorities and responsibilities that should exist within any repository environment (albeit, in nestor's case, mainly limited to Germany). To adopt only this perspective is to some extent counter-productive, since it implicitly disregards the great variety that is visible across contemporary digital repository platforms. Diversity in terms of funding, scale, legislative responsibilities and restrictions, content types, technology, and policy are identifiable in even a localized sample. Given this landscape, generically defined criteria are difficult to conceive; if expressed too vaguely they tend to lack meaning, but if too specific will be rendered irrelevant for a significant proportion of potential users.

Feedback from the repository community has demonstrated that such concerns do exist. Although each of these check-lists was developed by diversely assembled

individuals committed to *reflecting* existing good practice (and not to mandate novel or theoretical approaches to preservation), the calls of "this bit doesn't apply to me" from repository practitioners have been consistently audible. In several cases this reflects short-sightedness on the part of those working within the repositories; criteria have been painstakingly phrased to ensure their flexibility, and facilitate optimal general applicability. But nevertheless, it is evident that within the community there is the need for a more tailored assessment solution that takes into account atypical repository qualities, as either a companion piece, or alternative, to the existing guidelines.

The Digital Repository Audit Method Based on Risk Assessment (DRAMBORA) (Digital Curation Centre & DigitalPreservationEurope, 2007) developed by the Digital Curation Centre and DigitalPreservationEurope is designed to meet this gap. It adopts a bottom-up approach, enabling repositories to relate their benchmarks for success more explicitly to their own aims and contextual environment. Capable of being used both independently and in association with more objective guidelines, *DRAMBORA* describes a formalized process that encourages repositories to consider and document their mission, objectives, constraints and activities, before deriving, expressing and planning to address the fundamental challenges that threaten overall success.

General Repository Characteristics

The developers of DRAMBORA met with the creators and administrators of the TRAC and nestor criteria check-lists in early 2007 with a view to formalizing the repository problem space, in order to ensure that each of the three efforts remained compatible, and capable of generating comparable results. Despite the difficulties associated with determining an objective and universally reflective perspective of "digital repositories", the benefits in undertaking this exercise were clear. An accepted understanding of what digital repositories actually are is a necessary precursor to any work that seeks to determine their effectiveness.

Adopting a broad view that echoes the work undertaken by RLG/OCLC in their seminal 2002 "Trusted Digital Repositories – Attributes and Responsibilities" (RLG/OCLC Working Group, 2002), ten general principles of repositories (CRL/OCLC/NESTOR/DCC/DPE, 2007) have been conceived, capable of encapsulating all the organizations and organizational components that could be subject to assessment using the assembled groups' respective tools. In isolation, the list of principles is insufficient to support assessment but nevertheless provides a structure that informs the processes and outcomes of TRAC, nestor and DRAMBORA, and contributes to their compatibility.

The ten principles, which should be demonstrable by organizations claiming digital repository status, and therefore suited to assessment using these tools, are:

1. Mandate & Commitment to Digital Object Maintenance;
2. Organizational Fitness;
3. Legal & Regulatory Legitimacy;
4. Efficient & Effective Policies;
5. Adequate Technical Infrastructure;
6. Acquisition & Ingest;
7. Preservation of Digital Object Integrity, Authenticity & Usability;
8. Metadata Management & Audit Trails;
9. Dissemination;
10. Preservation Planning & Action.

Clearly the coverage of these principles extends more broadly than to simply technology, and issues of organizational competence, legal legitimacy and adequacy of policies are all similarly prioritized. From an object management perspective, mappings can be identified between the principles' explicit requirements with the functional model described in the Reference Model for an Open Archival Information System (Consultative Committee on Space Data Systems [CCSDS], 2002). The DRAMBORA process presupposes no additional characteristics of any audited digital repository, other than these ten principles.

The Perils of Objectivism

As alluded to previously, there are considerable difficulties associated with the generalization of optimal repository characteristics. The most fundamental problem is that to do so equates to an assumption that all repositories share a singularity of purpose, and that their priorities are uniform, irrespective of where or why they exist. But the diversity evident within repositories, manifested in terms of (among other things) mandate, available resources, supported content and legal context, is also identifiable in the ways that success can be demonstrably realized. Listing blue-sky criteria for digital repositories is a valuable process; TRAC and nestor are both compelling reference materials, selection boxes for organizations seeking to develop new repository features, or to subject their existing infrastructures to gap analyses.

However, both of these criteria check-lists are expressed in necessarily vague terms, and it is therefore quite challenging from the perspective of repository practitioners to understand how conformity might be adequately measured. Both documents are intended to address an apparently growing demand from the repository community, and repository users, for a formalized system of repository audit and certification. In fact, the two terms, 'audit' and 'certification' have been synonymised far too frequently in discussions within the preservation environment, and rarely has either one been given appropriate dedicated consideration, in isolation from the other. Considerable value can be found in taking each in turn and considering its respective dependencies and the infrastructures necessary to adequately support it. The latter, the process of certification is well served by documents such as TRAC and nestor. The conferment of a universally acknowledged recognition of success presupposes the availability of an objective benchmarking mechanism. One cannot compare apples to oranges, and similarly a certification process that is based variably upon the specific issues associated with individual repositories would immediately sacrifice its weight of legitimacy. The discussion of whether or not certification is indeed a high priority within the preservation community is separate, and will no doubt continue for some time. But the most compelling benefits of certification, and the most obvious stakeholders within such a process, will almost all demand comparability of results to enable an objective view of individual repositories' successes in a wider context.

In contrast, the audit process, although an essential precursor to the award of certification, is quite distinct in terms of its requirements. Best practice guidelines and check-lists provide an undoubtedly useful intellectual foundation upon which to construct an audit, but in their current form, neither TRAC nor nestor's documents provide, in explicit or implicit terms, a sufficiently tangible structure for determining where conformity and success actually exist. Neither offers sufficiently detailed insights into the mechanics of the audit. Which individuals should be involved? What

questions should be posed? How should experimental evaluation of systems be conducted? What are the quantitative or qualitative evidence expectations that will adequately demonstrate sufficient check-list compliance? Acknowledging these questions, the Digital Curation Centre undertook a series of pilot audits in a diverse range of preservation environments in 2006 and early 2007. The selection of participants was suitably diverse, including several repositories, exhibiting a range of varied characteristics. The British Atmospheric Data Centre (BADC); the National Digital Archive of Datasets (NDAD); the National Library of New Zealand's National Digital Heritage Archive (NDHA); the Florida Digital Archive (FDA) at the Florida Centre for Library Automation; and the Beazley Archive (BA) at the University of Oxford were among those that kindly agreed to take part. As well as providing the participating organizations with an objective and expert insight into the effectiveness of their operations, and determining the robustness and global applicability of those metrics and criteria already conceived, the audits were aimed at exploring the optimal means for *conducting* assessment. The research set out to develop an increased understanding of how evidence is practically accumulated, assessed, used and discarded throughout the audit process. Researchers investigated the ways in which practical, objective sense could be made of the potentially limitless kinds of evidence that might be submitted in support of certification, and to classify evidence examples according to their origins, form and weight of legitimacy. Regularizing disparate evidence equips the auditor to effectively cross-compare, corroborate and prioritize the full range of proof and testimony that is provided throughout a repository's bid for certification.

DRAMBORA: A Methodology for Audit

During these assessments a methodology for performing repository audit was quickly established and subject to considerable subsequent refinement. In March 2007 the process was formalized as DRAMBORA. The methodology itself is flexible, and responsive to the structural and contextual peculiarities of individual repositories, its metric for success directly linked with repositories' own aims. More objective guidance materials such as TRAC and nestor can be used in combination, informing the process, and prompting analysis of particular issues, but no criteria are mandatorily applicable.

Consisting of two discrete primary phases, the DRAMBORA process places considerable emphasis on demonstrable, and not just inferred, success. The initial phase is a process of information accumulation, aggregation and documentation. Numerous responses must be provided to describe in detailed terms the repository's strategic purpose, its action planning, and any contextual factors that influence or limit its ability to meet its objectives. This is a detailed and highly structured scene-setting exercise. A hierarchical analysis is undertaken, beginning with consideration of the repository's mandate. This is its essential mission, expressed in a document, legislative instrument or policy that describes and justifies its existence and legitimizes its purpose. Subsequently, the organization is subject to increasingly focused scrutiny, requiring detailed descriptions of fundamental repository objectives as well as the activities aimed at their completion and any asset dependencies. Finally, each of the repository's contextual influences must be made explicit. These may include legislative requirements, technological limitations, or policies resulting from strategic planning - anything that significantly constrains the repository's business should be documented. The ten principles described above provide a structure that facilitates

these efforts to describe, document and relate the various responses. For example, objectives must be identified to correspond with maintaining organizational fitness, legal legitimacy, and technological adequacy as well as every aspect of digital object management workflow. The outcome of this phase is a comprehensive organizational overview, which immediately leads into the latter phase, concerned with the identification of risk.

The risk identification, assessment and management part of the DRAMBORA process is where conclusions are derived from the organizational picture detailed within the previous phase. Risk is utilized as a convenient means for visualizing repository success – those repositories most capable of demonstrating the adequacy of their risk management (as opposed to those facing the least number of risks) are those that can more reasonably claim a trustworthy status. Preservation is fundamentally a risk management process. Numerous uncertainties or threats relating to any number of social, semantic and technological factors are capable of inhibiting long-term access to digital materials. Successful repositories are those that plan for these uncertainties, and convert them to risks that can be managed to mitigate the likelihood of problems occurring and limit their potential impact. Risks are implicit in every aspect of an organization's goals and activities, and can be borne or influenced by any number of internal or contextual factors. Perhaps most importantly, repository risk is assessed as an all-encompassing issue. In common with the ten principles, consideration must be made of not just the service-oriented procedures and policies, but also of organizational, legal, resource-related and technological risks.

Of course, one might assume that the results of such assessment will be of little value in a global sense, and will limit opportunities for repository comparison. Following the DRAMBORA assessment process, how, for example, can one compare two repositories with dramatically different preservation goals? In fact, to pose such a question is to misunderstand the complex realities of the digital repository landscape. "Digital repository" is a convenient, broadly applicable term, that unfortunately, when subject to even gentle analysis, means very little, as evidenced by the necessarily broad ten principles. Repositories are now so widespread within such diverse disciplines that increasingly granular classification has become necessary. Websites, databases, CRM systems, banking software, eLearning or eResearch environments, digital libraries, blogs, wikis and even personal desktops can be feasibly described as repository environments, with identifiable mappings to the ten principles, OAIS functional model or any other defining instrument that one elects to reference. Even notwithstanding the smaller subset of repositories that exist within the "preservation community", there is sufficient diversity to make questions of comparability between disparate or unrelated repositories virtually moot.

Information creators, depositors or consumers will not select repositories based on the results of certification alone. Their first consideration will be to determine which of the available repositories appear committed to providing a service that meets their requirements and expectations. As individual classes of repository are increasingly identified and described, their common services and characteristics can be understood and ultimately subjected to comparison. DRAMBORA enables such classification to take place prior to and during an organizational assessment. In order for its legitimacy to be accepted, any such classification must be representative of practice, and not

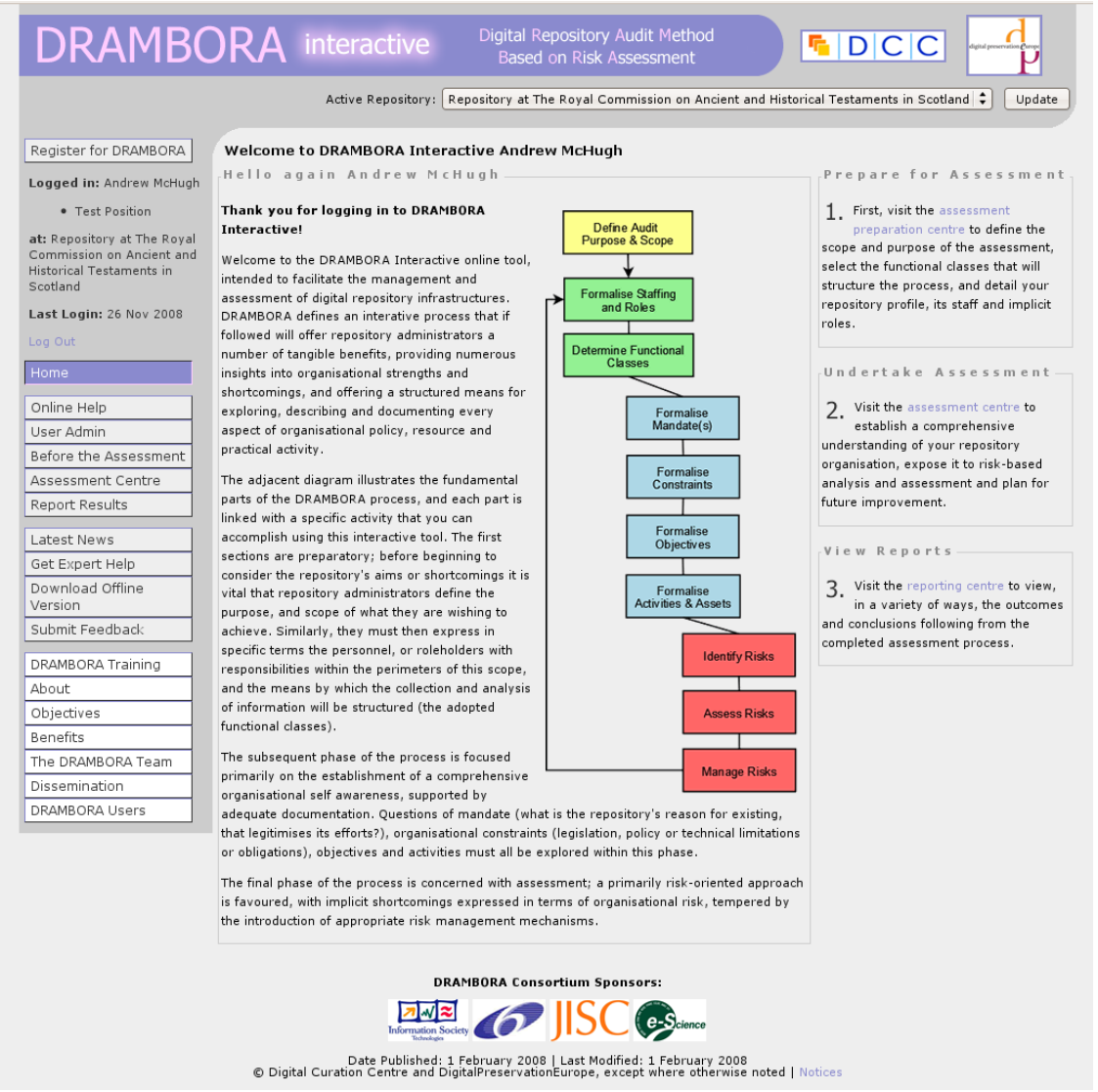

Figure 1. DRAMBORA Overview Screen.

prescriptive, evolving *from* the repositories themselves. DRAMBORA empowers repositories to define their own position within a repository landscape of potentially limitless diversity, spacing themselves in a context of comparable repositories that are, in terms of organisation, function or policy, similar. By doing so, they can influence, inform and benefit from the tailored, evolved perspective of "best practice" that exists within their particular sector of the "repo-sphere". No two repositories are likely to be identical, but if a repository shares insights from one repository with a comparable funding model, another preserving similar file formats, and a further example that operates within the same legislative context, the potential benefits are obvious.

A further compelling argument against the importance of establishing a single-tier ranking system is that, given the current state of repositories, the primary value of evaluation is probably not to *sell* the repository. Conversely, the results are best suited to internal use, a means to facilitate the planning efforts of repository administrators and practitioners, and support sustained, structured and responsive improvement. For this reason, DRAMBORA is mainly deployed as a self-assessment tool. In many respects, its implicit processes are indistinguishable from good repository management procedures. Repositories should be maintaining an organizational self-awareness, and

continuously monitoring their status, and exposure to potentially disruptive forces. Maturity modelling is at DRAMBORA's very heart - its cyclical nature facilitates structured evolution and ongoing improvement. Each iteration through the DRAMBORA process references that which has gone before. Over time, a diminishing level of risk severity illustrates repository improvement, without doubt the most fundamental prerequisite to the establishment of trustworthiness.

The completion of the DRAMBORA audit does not result in the generation or conferment of a certificate. Repositories seeking an endorsement to place proudly on their website or a flag to wave in order to woo potential customers or funders will not find these as *explicit* outcomes of the DRAMBORA process. It undoubtedly equips repositories extremely well to subsequently obtain such expressions of success, if and when they become available, but the most important reward is in the streamlining and optimization of repository infrastructures.

The Perils of Subjectivism

Fundamental to DRAMBORA's effectiveness is its bottom-up approach; within its defined self-audit process, the parameters for success are associated directly with the objectives and activities of the audited repository. Similarly, specific contextual factors and constraints are considered only where they are relevant. This ensures that the results of the process are, from the participating repository's perspective, wholly applicable and immediately useful.

However, this approach is not immune to criticism; as discussed above, without objective consensus on the definition of success, the comparability and reproducibility of results is lessened. This is of course tolerable; DRAMBORA's primary purpose is to provoke better repository management through the results of its process. Of more immediate concern with respect to a wholly subjective approach is that the potential for repositories to improve may be limited by their own horizons. Self-assessment alone can only indicate problems within the bounds of what repositories believe that they should be doing. Problems arise when organizations are oblivious to their shortcomings, or unaware of the potential benefits available to them and which they might usefully seize. How indeed can repositories comment on the likelihood or potential impact of unanticipated risks of which they are yet to fall foul? These issues have all been identified within a series of facilitated repository assessments conducted since DRAMBORA's launch by DCC and DPE, and by the DELOS Digital Preservation Cluster.

Feedback from these activities has indicated that the process of self-assessment has been universally valuable for participating organizations. However, a consistent concern that has been mooted by participating repositories is that if required to conduct the process without the assistance of experienced audit facilitators, the results would have been less comprehensive. This was a problem identified prior to the first release of the DRAMBORA methodology, in its initial document form, and some efforts were made to alleviate its effects by incorporating a list of around 80 example risks that might be modified by repositories for inclusion in their own risk responses. This is perhaps insufficient however – the list of risks is a top-down concession within an otherwise bottom-up focused approach, and suffers from the same criticisms leveled at objective metrics in a diverse realm that are described above. Recent developments within DRAMBORA are expected to largely overcome this issue however.

In early April 2008 a second version of the methodology was released as *DRAMBORA Interactive*, an online tool that offers an intuitive form-based interface, peer-comparison features, sophisticated and extensible reporting mechanisms and maturity tracking. By requiring users to describe the characteristics of their own repositories the tool presents "comparable organizations" with insights into the priorities and challenges of their peers, in order to help ensure a more comprehensive coverage. This information will form the basis for a series of repository profiles capable of encapsulating core roles, responsibilities, functions and risks for a variety of repository types. The availability of these profiles is expected to facilitate and further legitimize both repository assessment and development. Currently, repository profiling measures correspond with a number of descriptive fields already utilized within the DigitalPreservationEurope project's Registry of Repositories. These include:

- Institution Type;
- Country;
- Description;
- Domains and Disciplines Covered;
- Scope;
- Material Types;
- Languages;
- Technical Properties (including software);
- OAI-PMH Properties;
- Legal Properties;
- Ingest and Preservation Strategy.

By requiring repositories to define their own characteristics, the DRAMBORA software is able to make appropriate recommendations, based on the responses of their peers. If web archiving repositories in France, Germany and Belgium have each described similar European legislative requirements, and another UK-based web archiving project has not done so, then the system will be capable of drawing this to their attention, in case they have omitted a significant detail from their own self-assessment. The list of characteristics suggested above is unlikely to be exhaustive, and it is hoped that it can be extended in the future to enable increasingly granular and optimally meaningful repository classification. The ultimate outcome will be the evolution of an ontology of repository attributes. Some theoretical work has already indicated the feasibility of these efforts.

Within the context of the DELOS Digital Preservation Cluster four audits of Digital Library environments were undertaken, using DRAMBORA, with a view to determining common characteristics of Digital Library repositories, in order to facilitate both knowledge transfer and comparison. The report (DELOS Digital Preservation Cluster, in press), due to be published imminently at the time of writing describes a range of common objectives, constraints, roles, responsibilities, activities and risks within the University of Michigan Library's MBooks, CERN's Document Server, Gallica at the Bibliothèque Nationale de France and the Swedish National Library's Digital Library. The overall approach is philosophically an amalgam of top-down and bottom-up; to some extent suggestions that can follow based on intrinsic conclusions are prescriptive, but there is a careful acknowledgement of the specificity of individual types of repositories. The intention is always to reflect the current state of repositories, and not to mandate a classification scheme with its genesis in research theory.

Further diminishing the threat posed to the completeness of audit coverage, and reflecting other audit contexts, DRAMBORA's authors are focusing on the conception and formalization of a number of "key lines of enquiry", detailed question sets intended to inform and regularize the assessment process. Associated with individual repository profiles these will empower the individuals working within repositories to pursue, as an external auditor would, the most important issues within their own environment, and instill greater confidence in the value and comprehensiveness of results.

Throughout the various phases of pilot assessments that preceded the development of DRAMBORA and enabled its validation, it became increasingly possible to identify key lines of enquiry to correspond with particular objective check-list criteria, and generic or domain-specific risks. Structured frameworks have evolved, means for relating criteria or risks to the realities of the information infrastructure under scrutiny. Taking an example risk as a starting point, one might conceive of example practical responses; questions that determine whether both the will and capacity exist to facilitate risk management; and example risk vulnerabilities or consequences. The intention is to make it more straightforward for both auditors and repositories to identify where risks are evidently applicable, and to build an increased sense of the obstacles and problems that might be implicit, although difficult to perceive within both common and atypical responses. Aligning challenges with fundamental objective criteria adds further value, particularly when the process is perceived as a preparatory step prior to welcoming external auditors into the organization, who will no doubt rely on a more objective benchmarking approach. DRAMBORA can be usefully combined with other objective metrics such as TRAC or nestor. Both are pervasive influences, presenting structured insights into the kinds of issues that may correspond to risks, shortcomings and perceived points of failure. An example of the kinds of information that would be referenced for an individual risk is included in Table 1 below.

In Conclusion

It has been acknowledged that the DRAMBORA Interactive system must offer more than simply increased usability to the self-assessment process. It must perform the role of audit facilitator, and be injected with sufficient scope and functionality to guide an individual through the audit process and as far as possible ensure the comprehensiveness of their responses. That it can do so by referring users to the responses provided by peer organizations is of potentially considerable value, which will only increase as the number of respondents documenting their own repository experiences continues to grow. Either in association with objective guidelines or in isolation, DRAMBORA offers benefits to repositories both individually and collectively. As a means of opening lines of communication between discrete, but related repositories, DRAMBORA is capable of determining and disseminating expressions of both general and more specialist best practice. Categories of repositories can be constructed to reflect and inform practical realities. In what remains an immature discipline, where the naïvety and uncertainty of core practitioners remain considerable barriers to progress, the circulation of emerging insight tailored to specific circumstances has the potential to be of tremendous benefit.

Key Lines of Enquiry Example

Risk:	Identifier to information referential integrity is compromised -it becomes impossible to associate identifiers and information.
TRAC Criterion:	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).
Risk Responses:	- Objects are renamed to correspond with identifiers - Objects are stored in a directory named to correspond to identifier - Objects are packaged using alternative mechanism with identifier information (e.g., in a zip file with associated text file) - Database table maintains identifier with corresponding field describing full path where object resides, or a sub-path from the root of the archive that remains consistent even if the archive information is transplanted elsewhere, paired with a current path prefix. For example, record the archival path as /2006/london/record.pdf, with a current prefix of /usr/archive which can be subsequently moved to C:\Documents and Settings\Archive\ with minimal effort)
Key Lines of Enquiry:	- Does repository apply its own identifiers or maintain existing ones for information packages? - Under what circumstances could identifier collision occur? - Is a bespoke or off-the-shelf (e.g. Handle, DOI, PURL) identifier scheme employed? - Are third-party resolver services required? - What overt costs are associated with applying or resolving identifiers? - In what circumstances could the identifier become divorced from the related object? - What redundancy is employed to maintain referential integrity?
Vulnerabilities or Consequences:	- Repository maintains the use of the file path from the digital object's original environment as the identifier for the archived object, meaning that two distinct objects originating from different locations share a duplicate identifier /usr/archive/2006/report.pdf. - Identifier consists of the time stamp at the point of ingest, but two ingest systems operate simultaneously and duplicate identifiers are consequently applied. - Archive is migrated to an alternative file system and paths listed within the database are no longer current, resulting in loss of referential integrity. For example, a database records that an object with the unique ID #123 corresponds to location /home/archive/report.pdf on UNIX but it is subsequently moved to c:\archive\report.pdf on a Microsoft Windows server, invalidating the stored reference.

Table 1. Example of Key Lines of Enquiry.

References

Center for Research Libraries, & RLG OCLC Programs. (2007). *Trustworthy repositories audit & certification (TRAC): Criteria and checklist*, Version 1.0. Retrieved February 11, 2007, from http://www.crl.edu/content.asp?l1=13&l2=58&l3=162&l4=91

Consultative Committee on Space Data Systems. (2002). Reference Model for an Open Archival Information System (OAIS) – ISO 14721. Retrieved March 11, 2007, from http://public.ccsds.org/publications/archive/650x0b1.pdf

CRL/OCLC/NESTOR/DCC/DPE. (2007). *Core requirements for digital archives*. Retrieved January 31, 2007, from http://www.crl.edu/content.asp?l1=13&l2=58&l3=162&l4=92

DELOS Digital Preservation Cluster. (in press). Investigation of the potential application of the DRAMBORA Toolkit in the context of digital libraries to support the assessment of the repository aspects of digital libraries.

Digital Curation Centre, & DigitalPreservationEurope. (2007). Digital Repository Audit Method Based on Risk Assessment (DRAMBORA), Version 1.0. Retrieved March 11, 2007, from http://www.repositoryaudit.eu/

nestor Working Group. (2006). *Catalogue of criteria for trusted digital repositories*, Version 1 (draft for public comment). Retrieved December 11, 2006, from http://www.nbn-resolving.de/?urn:nbn:de:0008-2006060703

RLG/OCLC Working Group on Digital Archive Attributes. (2002). *Trusted digital repositories: Attributes and responsibilities*. An RLG-OCLC Report. Retrieved May 11, 2002, from http://www.oclc.org/programs/ourwork/past/trustedrep/repositories.pdf