Risk management foundations for digital libraries: DRAMBORA (Digital Repository Audit Method Based on Risk Assessment)

Andrew McHugh[1], Perla Innocenti[1], Seamus Ross[1], and Raivo Ruusalepp[2]

[1] [1] HATII at the University of Glasgow, 11 University Gardens, Glasgow G12 8QJ, UK
{a.mchugh, p.innocenti, s.ross}@hatii.arts.gla.ac.uk
[2] [2] Nationaal Archief , 2595 LK, Den Haag, Netherlands
raivo@eba.ee

Abstract. This paper proposes the use of the DRAMBORA (Digital Repository Audit Method Based on Risk Assessment), the Digital Curation Centre (DCC) and DigitalPreservationEurope (DPE) audit toolkit for digital repositories, as a tool to ensure the preservation capabilities of digital libraries. Digital repositories lie at the heart of digital libraries: ensuring long-term sustainability of their content is a fundamental responsibility of a digital library system and environment. DRAMBORA is designed to facilitate the assessment of digital repositories' risk exposure: it facilitates internal audit by providing repository administrators with a means to assess their capabilities, identify their weaknesses, and recognize their strengths. The toolkit represents the latest complementary development in an ongoing international effort to conceive criteria, means and methodologies for audit and certification of trustworthy digital repositories. DRAMBORA already includes the ten CRL principles for digital preservation repositories. As part of the ongoing developments of the toolkit we are investigating its applicability within the digital library domain, and the identification of core principles of digital preservation that can be incorporated into the DELOS Digital Library Reference Model, to ensure that digital libraries conforming to the reference model have preservation functionality.

1 Introduction

A digital repository lies at the heart of a digital library. As outlined in the DELOS Digital Library Manifesto [1], the digital library universe is a complex framework in which at least three types of conceptually different "systems" can be identified, namely, digital libraries (DLs), digital library systems (DLSs) and digital library management systems (DLMSs). Architecture, personalization, quality, policy and usability are essential to the design and deployment of digital libraries. But if we cannot ensure the long-term sustainability of the content, ensuring the presence of these capabilities would be pointless. Therefore, we require mechanisms that will enable us to measure the success of digital libraries and their underlying repositories in content preservation, as this is a fundamental building block of a digital library system and environment.

Ten principles surround the definition of a trusted digital repository. Those principles were agreed in January 2007 at a meeting hosted by Center for Research Libraries

(CRL), which assembled four projects (Digital Curation Centre, DigitalPreservationEurope, nestor and Center for Research Libraries) responsible for the development of mechanisms and standards to support the audit, certification and accreditation of repositories [2]. According to these principles, regardless of their mission, business model and source of funding, all trustworthy digital repositories should:

1. Commit to continuing maintenance of digital objects for its identified community(ies).
2. Demonstrate organizational fitness (including financial, staffing, structure, processes) to fulfill its commitment.
3. Acquire and maintain requisite contractual and legal rights and fulfill responsibilities.
4. Have effective and efficient policy framework.
5. Acquire and ingest digital objects based upon stated criteria that correspond to its commitments and capabilities.
6. Maintain/ensure the integrity, authenticity and usability of digital objects it holds over time.
7. Create and maintains requisite metadata about actions taken on digital objects during preservation as well as about the relevant production, access support, and usage process contexts before preservation.
8. Fulfill requisite dissemination requirements.
9. Have strategic programme for preservation planning and action.
10. Have technical infrastructure adequate for continuing maintenance and security of digital objects.

One of the things that must be established is how to ensure that the repositories underlying the digital libraries are designed, maintained and managed in ways that reduce the risk of loss of content and context of the digital library holdings.

In order to achieve this, the Digital Curation Centre (DCC) and DigitalPreservationEurope (DPE) have created an audit toolkit for digital repositories: DRAMBORA (Digital Repository Audit Method Based on Risk Assessment), available online at `http://www.repositoryaudit.eu`. Fundamentally, this toolkit can be used to assess the performance of digital libraries and also to provide guidance with respect to digital library design and minimize the risk in terms of the preservation capabilities. Digital repositories are still in their infancy and this model is designed to be responsive to the rapidly changing landscape. The toolkit aims to encompass a broader range of digital repositories of all sizes and purposes. DRAMBORA already includes the ten CRL principles for digital preservation repositories. Ongoing developments of the toolkit will investigate its applicability within the digital library domain, and the identification of core principles of digital preservation that can be fed into the DELOS Digital Library Reference Model [3]. This introduces a reference model (a set of concepts and relationships that represent the significant aspects of each of them) for each of the indicated systems in the Digital Library Manifesto (DLs, DLSs and DLMSs). But for all its strengths, the DELOS Digital Library Reference Model has not yet incorporated preservation as a integral feature. There have been some attempts, such as the DELOS Digital Preservation Cluster, to identify which core preservation aspects must be present in a digital library reference model. But as yet we have not been able to find these characteristics. As one

of the last pieces of work that DELOS Digital Preservation Cluster is conducting as part of its final programme of research, there are three audits of digital libraries using DRAMBORA. We hope that as result of this process not only we will understand the applicability of DRAMBORA, but also we will arrive at some core principles of dig preservation that we can integrate into the reference model.

2 DCC, DPE and a risk-based approach to audit and digital preservation

The DRAMBORA toolkit was developed as collaboration between the Joint Information Systems Committee and Core eScience funded Digital Curation Centre (DCC) in the United Kingdom and the European Commission co-funded initiative DigitalPreservationEurope (DPE).

The JISC-funded DCC [4] provides a focus on research into digital curation expertise and best practice for the storage, management and preservation of digital information to enable its use and re-use over time. DPE [5] is a three-year project (2006-2009), co-funded by the European Commission (IST-2006-034762), and comprising nine partner organizations from eight European countries. DPE addresses the need to improve coordination, cooperation and consistency in current activities to secure effective preservation of digital materials. Developing mechanisms to support collaboration between repositories and audit to enable repositories to ensure that they are performing to the highest possible standards are two of the core areas in which DPE operates. These two initiatives will continue to work together to test and refine the toolkit, to manage the development and deployment of an online tool, and to foster its widest possible take-up within the United Kingdom, Europe and broader international contexts.

DRAMBORA has been shaped by the awareness that repositories face a multitude of technological, organizational and methodological challenges within their activities. If considered as treatable or avoidable, risks can be more feasibly addressed and subsequently overcome. Therefore the first step for a repository to be successful is to identify the risks it is facing (risks analysis) and then learn how to manage them (risk management).

Digital preservation lies at the heart of digital libraries, as mentioned in the first paragraph. However, there is yet no single universal or unified standard to inform digital libraries preservation: therefore, ensuring the long-term sustainability of the content must lie in a combination of technology and effective risk management practice. That is why, in the digital libraries environment, we must look beyond traditional practice to policies of risk management, to guarantee that the digital library has in place adequate mechanisms to ensure long-term viability of content within its repository.

The ability to adequately deal with risk is an integral part of any successful business: risk management is an integral component of good management and decision-making at all levels. Such is the intrinsic uncertainty that characterizes the digital domain, that principles of risk management assume an even more profound level of importance when dealing with digital information. Risk management systems have emerged as a tool to complement existing management information tools and systems and can assist an organization to achieve predefined objectives and strategies related to core business func-

tions, asset management and projects [6]. Risk means being exposed to the possibility of a bad outcome, and risk management is about being proactive. It means taking deliberate action to shift the odds in your favor: the resources available for managing risks are finite and the aim is therefore to achieve an optimum response to risks, prioritized in accordance with an evaluation of the risks. Risk is unavoidable, and every organization needs to take action to manage risk in a way that it can justify to a tolerable level. The amount of risk that is judged to be tolerable and justifiable is the organization's 'risk appetite'.

The concept of risk is often interpreted in terms of threats, hazards, loss and other negative impacts. In the general organizational context, it is more fruitful to consider the risk as exposure to the consequences of uncertainty, or potential deviations from what is planned or expected [7]. Risk management is usually presented as a cycle that consists of individual stages:

- Identifying the context where risks have to be managed.
- Identifying risks.
- Assessing and evaluating risks.
- Defining measures to address and manage risks.

Digital preservation is nowadays often defined as a risk management exercise where the aim is to convert the uncertainty about maintaining usability of authentic digital objects into quantifiable risks. The purpose of a digital repository is to do everything it can to mitigate the risks that impede its ability to provide access to authentic digital information. The measure of success of a repository's work is the 'quality' of information it releases to its users.

The issue of risk has been considered from a number of perspectives within the context of digital curation and preservation. For instance, a variety of work has sought to analyze the risks associated with particular file formats, perceiving the risk as something intrinsic to what a digital repository does, based upon the technical challenges associated with maintaining the usability of digital files and storage media [8]. More recently some authors, such as Ross [9] and Ross and McHugh [10], have described the inherent uncertainty associated with digital preservation.

3 DRAMBORA

3.1 The origin of the toolkit

The development of the DRAMBORA toolkit follows a concentrated period of repository pilot audits undertaken by the DCC, conducted between April 2006 and January 2007 at a diverse range of organizations including national libraries, scientific data centres and cultural and heritage data archives. The goal was to determine an optimal methodology for the assessment of preservation repositories, and to evaluate the applicability and robustness of the RLG-NARA [11] and nestor audit check-lists [12]. The primary objective was to conceive an understanding of the evidential basis for demonstrating a repository's successful compliance with check-list criteria. In total five repositories agreed to participate in the activity, providing diversity in scale and location: the British Atmospheric Data Centre at the Council for the Central Laboratory of

the Research Councils, Beazley Archive at the University of Oxford, the National Digital Archive of Datasets, the National Digital Heritage Archive of the National Library of New Zealand, Florida Digital Archive at the Florida Center for Library Automation. The results of the audits have been and are in the course of being documented within a series of audit reports [13]. Further conclusions have been documented in work undertaken by Ross and McHugh [14] and Ross and McHugh [15].

These test audits have been enormously beneficial, informing the understanding of issues of organizational compliance, evidence and what it means in practical terms for a repository to be trusted and trustworthy. At the same time, the use of existing tools to underpin the DCC audits exposed difficulties with the practical applicability of these instruments. In their current form these instruments do not have associated metrics for determining the extent and effectiveness of organizational compliance; as a result, it remains difficult to conceive reliable means for comparing and assessing repositories that are heterogeneous in terms of their scale, scope or mission. International consensus on methodology and criteria for auditing digital repositories remains an essential outcome. The Digital Curation Centre developed its approach to audit activities initially in conjunction with CRL. Rather than representing a straightforward alternative (and therefore competitive) means for repository assessment, the DCC/DPE DRAMBORA toolkit aims to provide a complementary approach that can be used in association with the efforts of both TRAC and nestor.

3.2 What DRAMBORA enables

Building on risk management work that has been undertaken within the digital preservation domain and beyond, DRAMBORA toolkit [16] guides auditors through a series of tasks, categorized according to core institutional characteristics and activities (Fig.1). The toolkit provides a metric, with which the auditor establishes the organizational context and goals of a repository and then expresses how it is achieving these in terms of risk. Risk is used as a metric, because it can be expressed quantitatively, supporting comparisons across several repositories.

Within the toolkit, the authentic and understandable digital object is positioned at the centre of a risk-based approach to audit; digital curation is ‘characterized as a process of transforming controllable and uncontrollable uncertainties into a framework of manageable risks’, classified according to a repositorys activities, assets and regulatory context. To this end, this methodology seeks to determine whether the repository has made every effort to avoid and contain the risks that might impede its ability to receive, curate and provide access to authentic, and contextually, syntactically and semantically understandable digital information.

DRAMBORA encourages repository administrators and staff to identify and classify the risks (Table 1) that carry the most profound implications with respect to their own organizations business continuity and at every stage of their activities, to assess the probability of their occurring, to appreciate their potential impact if they should arise, to avoid, mitigate and treat risks, and to maintain appropriate evidential documentation to ensure that any conclusions of this assessment are verifiable. In this framework evidence is afforded considerable significance; repositories are expected not only to

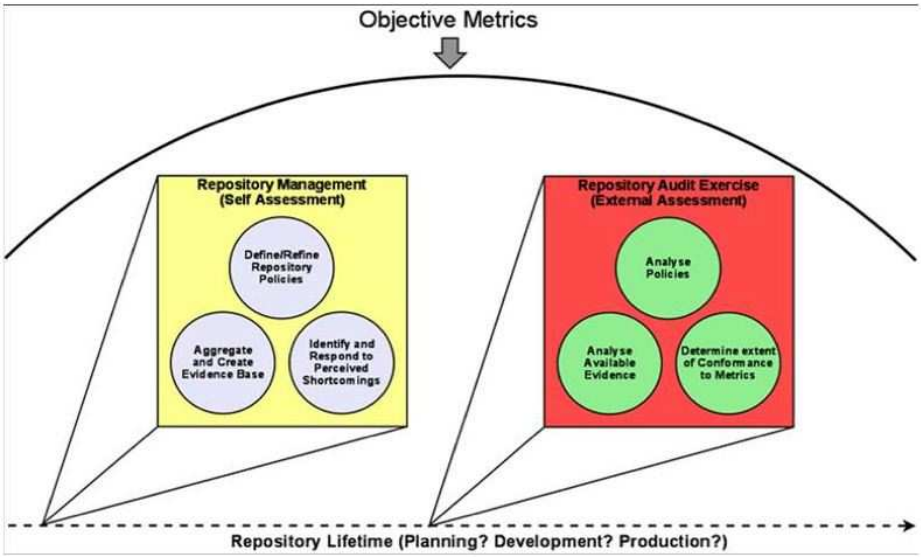

Fig. 1. Repository management and audit exercise fit together within the objective metrics of the repository planning, development and production.

identify risks and manage them appropriately, but also to demonstrate their ability to do so, even if only internally.

The self-audit process progresses through six stages:

- **Stage 1: Identify organizational context.** The purpose of this stage is to identify the repositorys role, and to chart its goals and objectives. The scope of the audit will be largely determined by the repositorys own scope and mandate.
- **Stage 2: Document regulatory framework.** This stage gives auditors the opportunity to provide or refer to evidence capable of supporting an assertion that the repository operates appropriately with respect to relevant regulatory frameworks; has an efficient and effective policy framework; is aware of the societal, ethical, juridical, and governance frameworks; is aware of the legal, contractual and regulatory requirements to which the repository is subject.
- **Stage 3: Identify activities, assets and their owners.** The goal of this stage is to develop a conceptual model of what the repository does and how it does it, by examining its activities and work processes, key assets and technology, and the staff involved. In order to support different situations in auditing practice, the self-audit toolkit has defined a total of eight broad functional classes of activities of a digital repository. These are further grouped into operational and support functional classes to represent the core functions of a digital repository: acquisition and ingest, preservation and storage, description and metadata management, access and dissemination; and functions that can be found in any organization: organization and management, staffing, finance management, technology support and security.

Each of these activities is usually carried out by a number of staff members, and an individual should be assigned with responsibility for each activity, which is linked to one or more key assets of the repository.

- **Stage 4: Identify risks.** The aim of this stage is to derive from organizational activities and assets a comprehensive selection of pertinent risks faced by the repository. Some risks can be derived from examining the mandate and objectives, regulatory environment and the model of the repositorys work (activities, assets, staffing and technology solutions). This principal outcome is the definition of an organizational worry radius, detailing the parameters within which risk management must be undertaken.
- **Stage 5: Assess and calculate risks.** The aim of this stage is to characterize the risks and risk relationships derived within the previous stage, and to assess the severity of each. Each risk must be enriched with a number of additional attributes; among the most significant are values describing the probability and potential impact of each, which cumulatively offer a quantitative insight into the overall riskiness of the repositorys business activities.
- **Stage 6: Manage risks.** The purpose of this stage of the audit is to provide the auditor with tools for effectively and efficiently managing the identified and assessed risks. Once a risk has been assessed, a business decision must be made to determine how the risk is to be approached. This should consider the risks potential impact, its frequency, its owners and its stakeholders. Risk mitigation strategies and tasks should be assigned, with accompanying deadlines for achieving predefined targets.

DRAMBORA is not a certifying tool or an OAIS-compliance toolkit, but rather a self-assessment and repository management tool, intended to measure how well the organization is doing in preserving its digital materials. Even if success within the self-audit process remains difficult to quantify completely [17], by defining risks with an associated impact and probability index it is possible to describe the severity of individual risks, and consequently the overall riskiness of a particular organizational environment.

Following the successful completion of the self-audit exercise, organizations can expect to have:

- established a comprehensive and documented self-awareness of their mission, aims and objectives, and of activities and assets intrinsic to these;
- constructed a detailed catalogue of pertinent risks, categorized according to type and inter-risk relationships, and fully described in terms of ownership, probability and potential impact of each risk;
- created an internal understanding of the successes and shortcomings of the organization, enabling it to effectively allocate or redirect resources to meet the most pressing issues of concern;
- prepared the organization for subsequent external audit whether that audit will be based upon the TRAC, nestor or forthcoming digital repository audit assessment criteria.

In summer 2007, the following repositories have been assessed using DRAMBORA 1.0: International Institute for Social History, Amsterdam, The Netherlands; National

Table 1. Complete risk description used in the self-audit toolkit is shown above. However, auditors are by no means restricted to this and may choose to use a more extensive set of attributes to characterize risks in their risk register.

Risk Description	
Risk Identifier:	A text string provided by the repository to uniquely identify this risk and facilitate references to it within risk relationship expressions
Risk Name:	A short text string describing the risk
Risk Description:	A longer text string offering a fuller description of this risk
Example Risk Manifestation(s):	Example circumstances within which risk will or may execute
Date of Risk Identification:	Date that risk was first identified
Activity the risk is linked to	Reference to an activity and/or asset the risk is linked with
Nature of Risk:	Physical environment
	Personnel, management and administration procedures
	Operations and service delivery
	Hardware, software or communications equipment and facilities
Owner:	Name of risk owner - usually the same as owner of corresponding activity
Escalation Owner:	The name of the individual who assumes ultimate responsibility for the risk in the event of the stated risk owner relinquishing control
Stakeholders:	Parties with an investment or assets threatened by the risk's execution, or with responsibility for its management
Risk Relationships:	A description of each of the risks with which this risk has relationships
Risk Probability:	This indicates the perceived likelihood of the execution of this particular risk
Risk Potential Impact:	This indicates the perceived impact of the execution of this risk in terms of loss of digital objects' understandability and authenticity
Risk Severity:	A derived value, representing the product of probability and potential impact scores
Risk Management Strategy(ies):	Description of policies and procedures to be pursued in order to manage (avoid and/or treat) risk
Risk Management Activity(ies):	Practical activities deriving from defined policies and procedures
Risk Management Activity Owner:	Individual(s) responsible for performance of risk management activities
Risk Management Activity Target:	A targeted risk-severity rating plus risk reassessment date

Archives of Scotland, Edinburgh, UK; National Library of the Czech Republic; National Central Library of Florence, Italy; Netarkivet (Danish Internet Archive), Denmark; Ludwig Boltzmann Institute in Linz, Austria, in cooperation with the Ars Electronica Center; E-LIS repository managed by CILEA, Rome, Italy; Lithuanian Museum of Ethnocosmology, Lithuania.

With the release of DRAMBORA 2.0 and a online interactive tool, as more and more organizations undertake the self-audit process, an increasingly rich understanding can be formed about the specific risks faced by particular kinds of organizations. Self-auditing repositories will be classified according to their mandate, funding, size and type of collections and geographical location. This information will be used to facilitate the more refined focusing of assessment processes for similar or comparable organizations. DRAMBORA not only supports the production of audit reports but also allows users to collaboratively contribute to an international effort to better understand the risks associated with digital curation. Users of the online tool will be able to opt to have their reports and risk tables rendered anonymously and included in the DCC/DPE repository risk database to support further refinement of the audit tool.

3.3 DRAMBORA in the context of digital libraries

An underlying, and key constituent of a digital library, a repositorys task is to identify and assess surrounding uncertainties, transform them into measurable risks and to define and implement means by which they can be effectively combated and mitigated. It is easy to see that the risks are not only technological but also organizational, staff and systems related, and connected with the external factors arising from the environment where the digital repository operates. It is our aim to investigate how DRAMBORA can work at all the layers of the DELOS Digital Library Reference Model.

DRAMBORA can be usefully employed in defining and managing a typical risk profile for digital libraries. The toolkit already presents a generic list of risks derived from an analysis of the TRAC check-list and the *nestor* criteria catalogue, and ISO 27001:2005 *Information technology – Security techniques – Information security management systems – Requirements*.

Digital libraries face not only technological infrastructure challenges, such as IT security, but also risks typically related to rights clearance, insufficient funding in the long term period and community involvement. With this regard, some example risks highlighted by DRAMBORAinclude:

– *Legal liability for IPR infringement*, when a repository is legally accountable for a breach of copyright, patent infringement or other IPR-related misdemeanor as a direct result of its business activities. The nature of this risk is related to personnel, management and administration procedures and it is contagious (that is, the execution of this risk will increase the likelihood of anothers). Example manifestations of this risk might include the reverse engineering of a software application in contravention of its end user license agreement, and the copyright breach of a institutional repository in disseminating e-journal content. The risk might be relevant to the repository if it deals with content with specific associated intellectual property rights, if it does not consult with legal experts when determining the legality

of their activities with respect to IPR restricted content, and if there is evidence of a high degree of litigiousness within the domain or jurisdiction within which the repository operates. Mitigation strategies include avoidance, such as assessing preserved materials to determine those to which intellectual property restrictions may apply, and seeking legal advice to determine legality of activities with respect to IPR restricted. The repository should establish policies and procedures to follow in the event of IPR challenge. This risk is strictly related to other contagious risks: *Management failure, Loss of trust, Business objectives not met, Business policies and procedures are inconsistent or contradictory*.

- *Finances insufficient to meet repository commitments*, when finances are insufficient to adequately resource each of the businesss integral activities. This is a relevant risk if the repository doesnt undertake appropriate budgetary management, a financial investment is necessary to achieve repository objectives, and within its current business model, the repository is not capable of self-sustainable income generation. Again, the nature of this risk is related to personnel, management and administration procedures and it is contagious. Example of risk manifestations includes the repository operating on an annual loss, and insufficient resource to facilitate every intrinsic activity. Avoidance strategies include developing self-sustainability with charged-for services, and obtaining assurances of budgetary availability. In the event of this risks execution, the repository should solicit additional funding to enable the achievement of organizational objectives, revise objectives if the funding stream is insufficiently flexible and maintain a residual fund where possible to meet shortfalls. This risk is strictly related to other contagious risks: *Management failure, Loss of trust* and in a contagious way to all the other risks listed.
- *Community feedback not acted upon*, when feedback, although received, has no influence over the repositorys business activities and modus operandi. This risk shows whether an appropriate proportion of staff time is allocated to responding to community feedback, or to reflecting it in changes to operational objectives; whether policies and procedures are in place to enable the repository to react within an appropriately timely fashion to the receipt of community feedback; and whether the operational objectives are adaptable to react to community feedback. An example manifestation may include the repository's failure to react to the fact that its user communities are increasingly incapable of using data encoded within the repositorys chosen formats with the software that they principally employ. The risk might be avoided by establishing policies to acknowledge and react to community feedback, and to formally acknowledge failure to act with community and retrospectively react to received feedback.
- *Exploitation of IT security vulnerability*. This risk describes a situation where shortcomings in the repositorys security provisions can be identified and used to gain unauthorized access to its systems. Situations where unpatched software security loopholes are hacked, or intruders gain physical access to the repository through a security door that is wedged open for example, are not uncommon. This may be relevant where vulnerabilities are evident within repository's physical and system security; where it is possible that individuals internal or external to the repository might be motivated to compromise system security to acquire or vandalize materials; and more generally wherever archived materials are stored on network ac-

cessible computers. Such technological and physical access risks can be treated in several ways:

- Establish and regularly evaluate policies and procedures for physical and software security in accordance with relevant standards.
- Limit execution of non-essential services.
- Update software with latest security patches.
- Allocate staff time to analyze attempted security compromises and monitor security sources for details of known vulnerabilities.
- Compel users to change passwords frequently.
- In the event of risks execution, rebuild the system to ensure there are no residual effects of system compromise.

Completion of the DRAMBORA process will yield a number of valuable results, facilitating both retrospective reflection and proactive planning for digital libraries. Firstly, organizations managing digital libraries will have established a documented self-awareness of their fundamental objectives, and of associated activities and assets. By defining their operational contexts, organizations are well positioned to determine their own assessment parameters as well as verify that their resources are optimally invested and positioned to ensure success. Secondly, organizations will have developed a documented understanding of the risks they face expressed in terms of their likelihood and potential impact. Mapped to organizational aspirations and efforts, this will facilitate subsequent organizational development and resource allocation, and offer a quantifiable insight into the contemporary severity of risks faced. Finally, organizations will have defined their chosen means for risk management, determining the appropriate strategies for avoidance, treatment, transfer and tolerance as well as the mechanics of their implementation. This process, which should be repeated on a regular basis, will provide opportunities to establish and achieve quantifiable targets, facilitating the improvement and ongoing development of every aspect of organizational activity of digital libraries, digital library systems and digital library management systems.

4 Conclusion and next steps

This paper has proposed to investigate the applicability of DRAMBORA (Digital Repository Audit Method Based on Risk Assessment), the Digital Curation Centre (DCC) and DigitalPreservationEurope (DPE) audit toolkit for digital repositories, as a tool to ensure the preservation capabilities of digital libraries. In many aspects, digital libraries include repositories as a component of their systems; the DRAMBORA toolkit should be useful to those needing to identify what kinds of risk they face with their digital library, and manage them. This toolkit is designed to facilitate the assessment of risk exposure faced by digital repositories; it facilitates internal audit by providing repository administrators with a means to assess their capabilities, identify their weaknesses, and recognize their strengths. It complements other emerging work on attributes and criteria for Trustworthy Digital Repositories. While work on the development of the toolkit was driven by DPE and DCC, its construction owed much to the developments undertaken by the Digital Preservation Cluster of DELOS. DRAMBORA self-audit

should be considered in the design of digital libraries, digital library systems and digital libraries management system, and should be integrated in the overall framework of a Digital Libraries Reference Model.

As part of the next DRAMBORA iterations and the release of an interactive web-based tool, in connection with the Digital Preservation Cluster of DELOS (JPA4), DDC and DPE are going to test this hypothesis in some international digital libraries, to assess whether or not the toolkit can be easily applied to the digital libraries context, and if not what modifications would be needed to it to make it applicable. This will allow both the investigation of the potential application of DRAMBORA in the context of digital libraries, and the assessment of the repository aspects of digital libraries.

The transfer of the results of this task to the Digital Curation Centre and DigitalPreservationEurope will ensure that the results achieved will survive past DELOS. Finally, results of the audits (although in anonymous form) will be published as a way of raising awareness of the DRAMBORA toolkit in the digital library community.

References

1. A digital library is “a (potentially virtual) organization that comprehensively collects, manages, and preserves for the long term rich digital content and offers to its user communities specialized functionality on that content, of measurable quality, and according to prescribed policies”. In: DELOS Digital Library Manifesto), http://www.delos.info/index.php?option=com_content&task=view&id=345 (2006) 8
2. Core Requirements for Digital Archives. Center for Research Libraries (CRL), http://www.crl.edu/content.asp?l1=13&l2=58&l3=162&l4=92 (2007)
3. A Reference Model for Digital Library Management Systems, http://www.delos.info/index.php?option=com_content&task=view&id=345
4. Digital Curation Centre (DCC), http://www.dcc.ac.uk
5. DigitalPreservationEurope (DPE), http://www.digitalpreservationeurope.eu
6. Lemieux, V.: Managing Risks for Records and Information. ARMA International, (2004) 2
7. UK Treasury Orange Book. Management of Risk Principles and Concepts. Crown (2004) 7
8. Risk Communication Tool, ERPANET, ERPAguidence tools, http://www.erpanet.org/guidance/docs/ERPANETRiskTool.pdf, (2003). Cornell University Library Virtual Remote Control (VRC) tool, Risk Management for Web Resources, http://irisresearch.library.cornell.edu/VRC/methods.html (2004). JISC, Managing Risk: a Model Business Preservation Strategy for Corporate Digital Assets , http://www.jisc.ac.uk/whatwedo/programmes/programme_preservation/programme_404/project_managingrisk.aspx (2005). Lawrence, G., Kehoe, W., Rieger, O., Walters, W., Kenney, A.: Risk Management of Digital Information: A File Format Investigation. CLIR Report no. 93, http://www.clir.org/pubs/reports/pub93/pub93.pdf (2000). Lemieux, V.: Managing Risks for Records and Information. ARMA International (2004). McGovern, N., Kenney, A., Entlich, R., Kehoe, W., Buckley, E.: Virtual Remote Control. Building a Preservation Risk Management Toolbox for Web Resources. D-Lib Magazine, vol. 10, no. 4, http://www.dlib.org/dlib/april04/mcgovern/04mcgovern.html (2004)
9. Ross, S. Uncertainty, Risk, Trust and Digital Persistency. NHPRC Electronic Records Research Felloships Symposium Lecture, University of North Carolina at Chapel Hill (2006)

10. Ross, S., McHugh, A. The Role of Evidence in Establishing Trust in Repositories. D-Lib Magazine, vol. 12, no. 7/8 http://www.dlib.org/dlib/july06/ross/07ross.html (2006) (Also published in Archivi e Computer, 2006)
11. The Research Libraries Group (RLG), National Archives and Records Administration (NARA) Audit Checklist for Certifying Digital Repositories. http://www.rlg.org/en/page.php?Page_ID=20769 (2006)
12. nestor Working Group nestor: Catalogue of Criteria for Trusted Digital Repositories, v1. Trusted Repositiories Certification (2006) http://edoc.hu-berlin.de/series/nestor-materialien/8/PDF/8.pdf
13. Ross, S., McHugh, A. The Digital Curation Centre Repository Pilot Audits: Results and Lessons. forthcoming
14. Ross, S., McHugh, A. The Role of Evidence in Establishing Trust in Repositories. D-Lib Magazine, vol. 12, no. 7/8 http://www.dlib.org/dlib/july06/ross/07ross.html (2006)
15. Ross, S., McHugh, A. Preservation Pressure Points: Evaluating Diverse Evidence for Risk Management. Forthcoming
16. McHugh, A., Ruusalepp, R., Ross, S., Hofman H. Digital Repository Audit Method Based on Risk Assessment. Digital Curation Centre (DCC) and DigitalPreservationEurope (DPE), (2007)
17. McHugh, A., Ruusalepp, R., Ross, S., Hofman H. Digital Repository Audit Method Based on Risk Assessment. Digital Curation Centre (DCC) and DigitalPreservationEurope (DPE), (2007) 43