An introduction to Repository Assessment and DRAMBORA

Perla Innocenti, Andrew McHugh, Seamus Ross
Raivo Ruusalepp, Hans Hofman
Digital Curation Centre (DCC), DigitalPreservationEurope (DPE),
HATII at the University of Glasgow & National Archives of the Netherlands

Data Audit Framework and DRAMBORA Interactive Launch
British Academy, London, 1st October 2008
Objectives of digital longevity

- Digital preservation aims to ensure that future users will be able to discover, retrieve, render, manipulate, interpret, and use digital information in the face of constantly changing technology.

- It involves conservation, renewal, restoration, selection, destruction, enhancing, updating, and annotating.

- It is a risk management activity at all stages of the longevity pathway -- translating uncertainties into manageable risks.

- Digital Preservation is an ongoing activity to ensure recurring value of digital objects.
Preservation risk is actual

- It is technological
- It is physical
- It is organisational
- It is socio-cultural
- It is legal
- It is financial
- It is political
- It is contractual

Actual risks can be assessed and managed
What is a “risk”? 

- many definitions of risk that vary by specific application and situational context 

- risk is described both qualitatively and quantitatively 

- frequently risk is considered as an indicator of both: 
  - threat, vulnerability, impact, uncertainty 
  - the chance that specific individuals are willing to undertake for some desired goal
Risk aversion vs. risk appetite
RBA in the digital world

- Risk-Benefit Analysis is one of the criteria to document appraisal - along with:
  - relevancy to organizational mission
  - adherence to organizational policy
  - authenticity
  - integrity and usability
  - provenance
  - physical descriptions
  - media format and compression
  - condition
  - metadata availability
  - accuracy & completeness
  - ……

- Quantifies in monetary terms risks and benefits (with associated costs) of the appraisal process, including items for which the market does not provide a satisfactory measure of economic value
RBA: risk modelling

Flight insurance company – statistical risk

Passenger – perceived risk

European Aviation Safety Agency – projected risk
Chronology of certification and audit criteria and toolkits

- **2002**: Trusted Repositories Attributes & Responsibilities
- **2002**: Reference Model for an Open Archival Information System (standardised as ISO 14721 in 2003)
- **2005**: RLG/NARA Draft Audit Check-list for Repository Certification released for public comment
- **2006-2007**: CRL and DCC Pilot Repository Audits
- **Dec 2006**: Catalogue of Criteria for Trusted Digital Repositories published (en) by nestor
- **Mar 2007**: Digital Repository Audit Method Based on Risk Assessment (DRAMBORA toolkit), text version 1.0 published by DCC/DPE
- **Apr 2007**: Trustworthy Repositories Audit & Certification (TRAC) Criteria and Check-list published by CRL
- **Spring 2008**: DRAMBORA Interactive, online version 2.0
Trustworthy Repositories Audit & Certification (TRAC) Criteria and Check-list

• RLG/NARA assembled an International Task Force to address the issue of repository certification
  – TRAC is a set of criteria applicable to a range of digital repositories and archives, from academic institutional preservation repositories to large data archives and from national libraries to third-party digital archiving services

• Provides tools for the audit, assessment, and potential certification of digital repositories

• Establishes audit documentation requirements required

• Delineates a process for certification

• Establishes appropriate methodologies for determining soundness and sustainability of digital repositories

http://www.crl.edu/content.asp?l1=13&l2=58&l3=162&l4=91
A3.4 Repository is committed to formal, periodic review and assessment to ensure responsiveness to technological developments and evolving requirements.

Long-term preservation is a shared and complex responsibility. A trusted digital repository contributes to and benefits from the breadth and depth of community-based standards and practice. Regular review is a requisite for ongoing and healthy development of the repository. The organizational context of the repository should determine the frequency of, extent of, and process for self-assessment. The repository must also be able to provide a specific set of requirements it has defined, is maintaining, and is striving to meet. (See also A3.9.)

Evidence: A self-assessment schedule, timetables for review and certification; results of self-assessment; evidence of implementation of review outcomes.
DCC Pilot Audits

The UK Digital Curation Centre engaged in a series of pilot audits of a TRAC draft in diverse environments

- Six UK, European and International organisations: national libraries, scientific data centres, cultural heritage archives

  British Atmospheric Data Centre at the Council for the Central Laboratory of the Research Councils, UK
  Beazley Archive at the University of Oxford, UK
  National Digital Archive of Datasets, UK
  National Digital Heritage Archive of the National Library of New Zealand
  Florida Digital Archive at the Florida Center for Library Automation, US
DRAMBORA (Digital Repository Audit Method Based on Risk Assessment)

www.repositoryaudit.eu

Developed by DCC & DPE, evidence-based, recognizes current approaches
Version 1.0 released in March 2007
Version 2.0 released as an electronic tool in Spring 2008

DRAMBORA invites repositories to:
- **develop an organisational profile**, describing and documenting mandate, objectives, activities and assets
- **identify** and **assess** the risks that impede their activities and threaten their assets
- **manage** the risks to mitigate the likelihood of their occurrence
- **establish effective contingencies** to alleviate the effects of the risks that cannot be avoided

It supports:
- **Validation** [“Are my efforts successful?”]
- **Preparation** [“What must I do to satisfy external auditors?”]
- **Anticipation** [“Are my proposals likely to succeed?”]
10 Characteristics of Digital Repositories

• Commitment to digital object maintenance
• Organisational fitness
• Legal & regulatory legitimacy
• Effective & efficient policies
• Acquisition & ingest criteria
• Integrity, authenticity & usability
• Audit trail and metadata
• Dissemination
• Preservation planning & action
• Adequate technical infrastructure

(CRL/OCLC/nestor/DCC/DPE meeting, January 2007)
DRAMBORA Workflow

Preliminary collecting and analysis of repository documentation

Organize appointments and onsite visits with repository staff (managers, curators, IT, legal experts…)

Risk registry finalization

Audit report finalization

Impact on individuals and organisations

Define Audit Purpose & Scope

Formalise Staffing and Roles

Determine Functional Classes

Formalise Mandate(s)

Formalise Constraints

Formalise Objectives

Formalise Activities & Assets

Identify Risks

Assess Risks

Manage Risks

Repository assessment and DRAMBORA
## Anatomy of a risk (I)

<table>
<thead>
<tr>
<th><strong>Risk Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Risk Identifier:</strong></td>
</tr>
<tr>
<td><strong>Risk Name:</strong></td>
</tr>
<tr>
<td><strong>Risk Description:</strong></td>
</tr>
<tr>
<td><strong>Example Risk Manifestation(s):</strong></td>
</tr>
<tr>
<td><strong>Date of Risk Identification:</strong></td>
</tr>
<tr>
<td><strong>Activity the risk is linked to:</strong></td>
</tr>
<tr>
<td><strong>Nature of Risk:</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
# Anatomy of a risk (II)

<table>
<thead>
<tr>
<th><strong>Owner:</strong></th>
<th>Name of risk owner - usually the same as owner of corresponding activity</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Escalation Owner:</strong></td>
<td>The name of the individual who assumes ultimate responsibility for the risk in the event of the stated risk owner relinquishing control</td>
</tr>
<tr>
<td><strong>Stakeholders:</strong></td>
<td>Parties with an investment or assets threatened by the risk’s execution, or with responsibility for its management</td>
</tr>
<tr>
<td><strong>Risk Relationships:</strong></td>
<td>A description of each of the risks with which this risk has relationships</td>
</tr>
<tr>
<td><strong>Risk Probability:</strong></td>
<td>This indicates the perceived likelihood of the execution of this particular risk</td>
</tr>
<tr>
<td><strong>Risk Potential Impact:</strong></td>
<td>This indicates the perceived impact of the execution of this risk in terms of loss of digital objects’ understandability and authenticity</td>
</tr>
<tr>
<td><strong>Risk Severity:</strong></td>
<td>A derived value, representing the product of probability and potential impact scores</td>
</tr>
<tr>
<td><strong>Risk Management Strategy(ies):</strong></td>
<td>Description of policies and procedures to be pursued in order to manage (avoid and/or treat) risk</td>
</tr>
<tr>
<td><strong>Risk Management Activity(ies):</strong></td>
<td>Practical activities deriving from defined policies and procedures</td>
</tr>
<tr>
<td><strong>Risk Management Activity Owner:</strong></td>
<td>Individual(s) responsible for performance of risk management activities</td>
</tr>
<tr>
<td><strong>Risk Management Activity Target:</strong></td>
<td>A targeted risk-severity rating plus risk reassessment date</td>
</tr>
</tbody>
</table>

Repository assessment and DRAMBORA
Risk Impact in the repository context

- Impact can be considered in terms of:
  - impact on repository staff or public well-being
  - impact of damage to or loss of assets
  - impact of statutory or regulatory breach
  - damage to reputation
  - damage to financial viability
  - deterioration of product or service quality
  - environmental damage
  - loss of ability to ensure digital object authenticity and understandability is ultimate expression of impact
Benefits of DRAMBORA

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

1. Established a comprehensive and documented self-awareness of their mission, aims and objectives, and of intrinsic activities and assets

2. Constructed a detailed catalogue of pertinent risks, categorised according to type and inter-risk relationships

3. Created an internal understanding of the successes and shortcomings of the organisation

4. Prepared the organisation for subsequent external audit
• DRAMBORA = risk-based approach enabling repositories to monitor how they are handling the risks associated with preservation through repository level management

• It recognizes the benefits of preservation and value whether evidential, reuse, or some other purpose have been determined at object or collection level

• It is a manual tool + a number of mechanisms (e.g. interactive interface, automation)
DRAMBORA collaborates with...

- Trustworthy Repository Audit and Certification (TRAC) Criteria and Checklist Working Group
- Center for Research Libraries (CRL) Certification of Digital Archives Project
- Network of Expertise in Long-term storage of Digital Resources (nestor)
- DELOS Digital Preservation Cluster (WP6)
- International Audit and Certification Birds of a Feather Group
- SHAMAN (Sustaining Heritage Access through Multivalent ArchiviNg)
- ISO TC46 /SC 11 Working Group
DRAMBORA 1.0

- Textual version
- Released in early March 2007
- [http://www.repositoryaudit.eu/](http://www.repositoryaudit.eu/)
- Over 1000 individuals registered and downloaded the toolkit
- Positive feedback
- A test period within the DPE project
Testing DRAMBORA 1.0

- National Archives of Scotland, Edinburgh, UK
- National Library of the Czech Republic
- National Central Library of Florence, Italy
- International Institute for Social History, Amsterdam, The Netherlands
- 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

The NATIONAL ARCHIVES of SCOTLAND

Repository assessment and DRAMBORA
Testing DRAMBORA 1.0

DELOS Digital Preservation Cluster
- MBooks Michigan-Google Digitization Project, US
- CERN Document Server, Switzerland
- Kungliga Biblioteket, Stockholm
- Gallica, National Library of France

Among other users
- British Library, London, UK
- US Geological Survey
- European repositories and archives
- American universities
What DRAMBORA users learned...

• “Good, visible and persuading documentation of risks might help to improve conditions for their successful management. And, of course, as soon as you have the truly trusted repository, you need the good documentation and certification to prove it”

• “We discovered some points of weakness in the repository and also learned to stop fretting about the stuff we actually do very well”

• “Assessment will be continued and the risk register will be an integral part of the repository once it becomes operational”

• “We originally planned to use TRAC for both our internal and later external audit. We also looked at NESTOR. [...] we believe that regular self audits using DRAMBORA will make the external audit easier and cheaper”
DRAMBORA 2.0 Interactive


- Online free tool offering:
  - intuitive form based interface
  - peer-comparison features
  - extensible reporting mechanisms and maturity tracking

- It allows registering and editing a repository auditing profile

- DRAMBORA's uses PHP/MySQL and AJAX to output CSS styled XHTML, Linux and Apache web server
DRAMBORA Interactive

DRAMBORA Online Tool :: Assessment Centre :: Manage Risks

The risk management measures defined in this stage describe the responses that will be implemented following the assessment process. Responsibility for each management measure should be allocated to one or more roles, and details of timescales and projected outcomes defined.

Risk: Loss of key member(s) of staff...

Risk Name: Loss of key member(s) of staff
Description: Individuals with roles, responsibilities or aptitudes vital to the achievement of business objectives parts company with the repository, rendering the achievement of those objectives less straightforward
Risk Owner: Administration
Probability: High
Impact: Low (Organisational Viability)
Severity: 8 (out of 25)

Add a Risk Mitigation Strategy
Save Risk Management
Further developments

- DPE Training Programme, WePreserve Joint Training Event, Prague, 13-17 October 2008
  - For general public
  - For auditors
- Accreditation of self-auditors
- Repository profiling
- DRAMBORA in Japan
- Dissemination in international conferences and journals
- DELOS report
- Version 3.0 (downloadable)
Why assessing with DRAMBORA

- Align with international efforts
- Evidence-based approach using risk as a metric
- Repository level management
- Self-assessment
- Identify, prioritise and manage risks, verifying compliance, checking effectiveness and identifying opportunities for improvements
- DRAMBORA interactive interface to facilitate the collection of information necessary to conduct a risk-analysis assessment, its analysis and reporting
- We are working towards automating the process that DRAMBORA encapsulates
Think metric!

DRAMBORA:
converting uncertainties into manageable risks

www.repositoryaudit.eu

THANK YOU