

An introduction to Repository Assesement 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 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

		袋
KANGAROO		
	36.80	中
Kangaroo Meat Chinese Style	36.80	宮
Kangaroo Meat with Chilli Sauce	36.80	沙
Satay Kangaroo Meat	36.80	鐵板
Sizzling Kangaroo Meat ShangHai Style	36.80	川
Kangaroo Meat Szechuan Style	36.80	三
Kangaroo Meat with Chinese Wine and Black Vinegar Soya Sauce		
CROCODILE		鱷
	46.80	薑蔥
Crocodile in Ginger and Shallor Sauce	46.80	川式
Crocodile with Szechuan Sauce	46.80	鐵板
Sizzling Crocodile with ShangHai Sauce		

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

- 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>

TRAC example

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

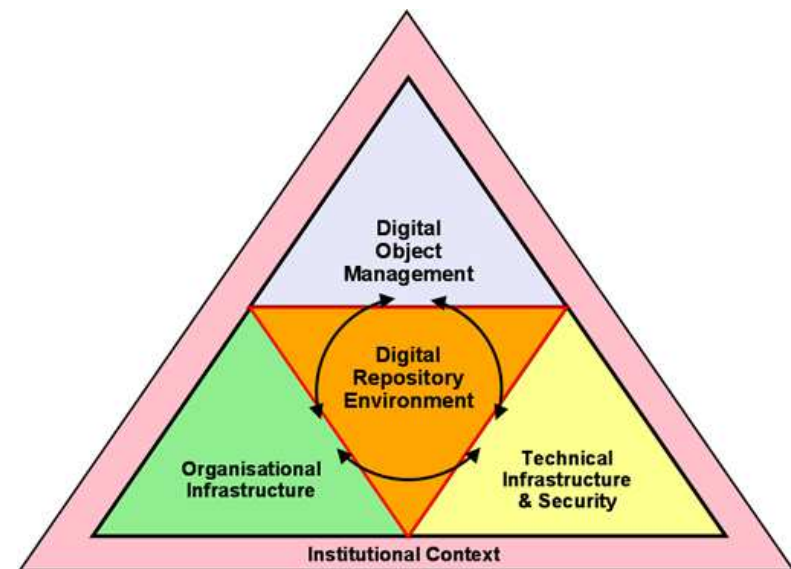
It supports:

- **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

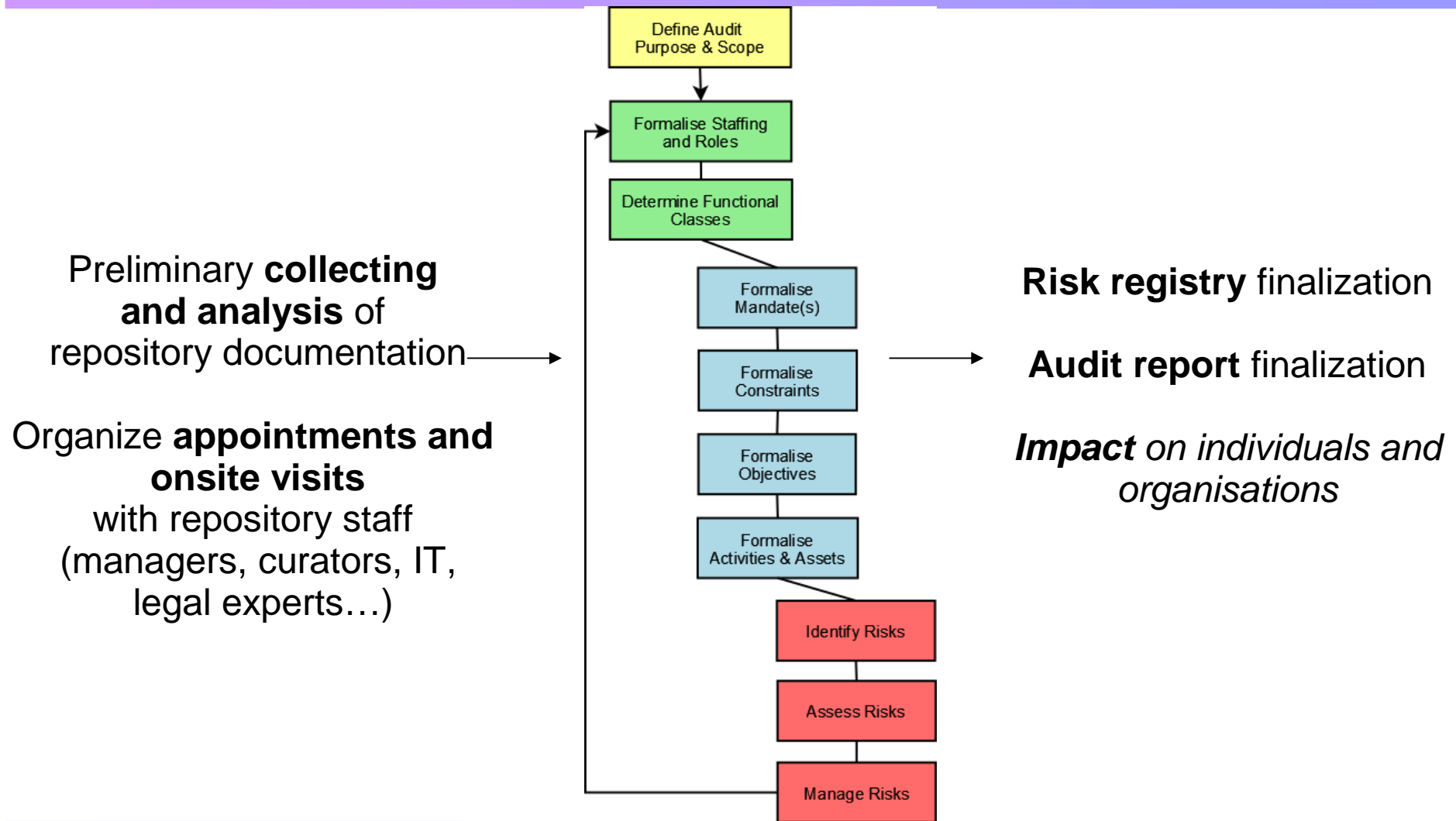
- Commitment to digital object maintenance ● ○
- Organisational fitness ●
- Legal & regulatory legitimacy ●
- Effective & efficient policies ●
- Acquisition & ingest criteria ○
- Integrity, authenticity & usability ○
- Audit trail and metadata ○
- Dissemination ○
- Preservation planning & action ○
-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



© HATII UofGlasgow, 2007

(CRL/OCLC/neslor/DCC/DPE meeting, January 2007)

DRAMBORA Workflow



Anatomy of a risk (I)

Risk Description	
Risk Identifier:	<i>A text string provided by the repository to uniquely identify this risk and facilitate references to it within risk relationship expressions</i>
Risk Name:	<i>A short text string describing the risk</i>
Risk Description:	<i>A longer text string offering a fuller description of this risk</i>
Example Risk Manifestation(s):	<i>Example circumstances within which risk will or may execute</i>
Date of Risk Identification:	<i>Date that risk was first identified</i>
Activity the risk is linked to	<i>Reference to an activity and/or asset the risk is linked with</i>
Nature of Risk:	<i>Physical environment</i>
	<i>Personnel, management and administration procedures</i>
	<i>Operations and service delivery</i>
	<i>Hardware, software or communications equipment and facilities</i>

Anatomy of a risk (II)

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

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, RBA & Appraisal

- 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

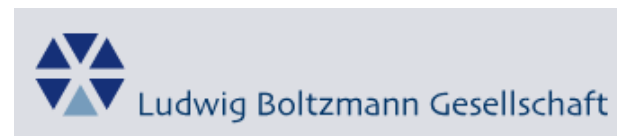
- Textual version
- Released in early March 2007
- <http://www.repositoryaudit.eu/>
- Over 1000 individuals registered and downloaded the toolkit
- Six public tutorials (London, The Hague, Arlington, Manchester, München, Stockholm)
- Positive feedback
- A test period within the DPE project

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



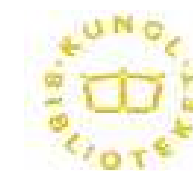
The NATIONAL ARCHIVES of SCOTLAND



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



- Released 2008, <http://www.repositoryaudit.eu/>
- 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 interactive

Digital Repository Audit Method
Based on Risk Assessment

Active Repository: Test Repository

Logged in: Test User
• Administrator
at: Test Repository
Last Login: 05 Aug 2008
[Log Out](#)

DRAMBORA Online Tool :: Assessment Centre :: Manage Risks

[Assessment Home](#) | [Add Mandate](#) | [Add Constraints](#) | [Add Objectives](#) | [Add Activities and Assets](#) | [Add Risks](#) | [Access Risks](#) | [Manage Risks](#)

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](#)

- identified risks
- defined activities
- defined objectives
- defined constraints
- defined mandate
- assessment progress
- saved snapshots

DRAMBORA Consortium Sponsors:



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