Risk Management Foundations for DLs: DRAMBORA (Digital Repository Audit Method Based on Risk Assessment)

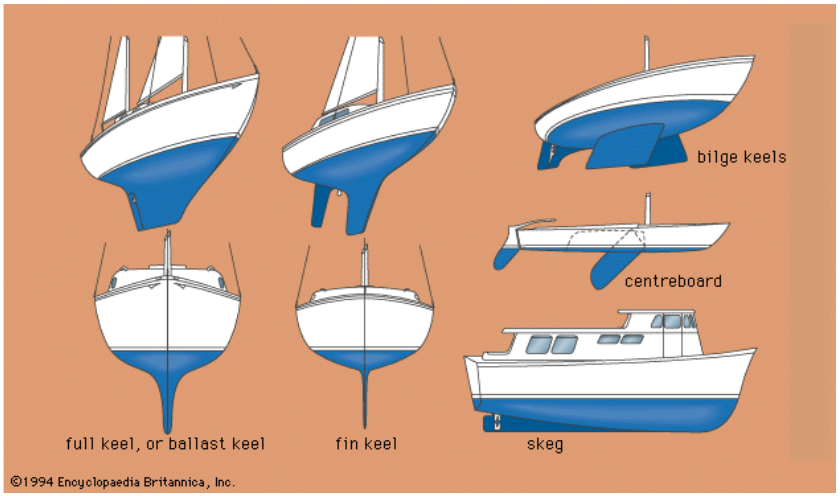
Perla Innocenti, Andrew McHugh, Seamus Ross, Raivo Ruusalepp

Digital Curation Centre (DCC), DigitalPreservationEurope (DPE),
HATII at the University of Glasgow & National Archives of the Netherlands

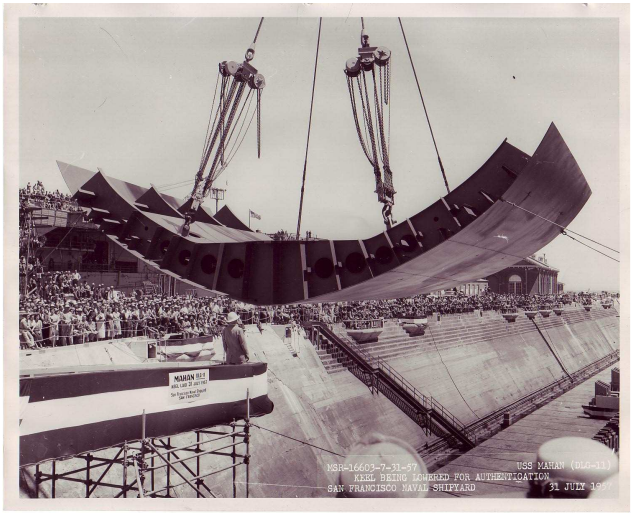
DELOS 2nd Workshop on Foundations of Digital Libraries
ECDL 2007, Budapest 20/09/07

About

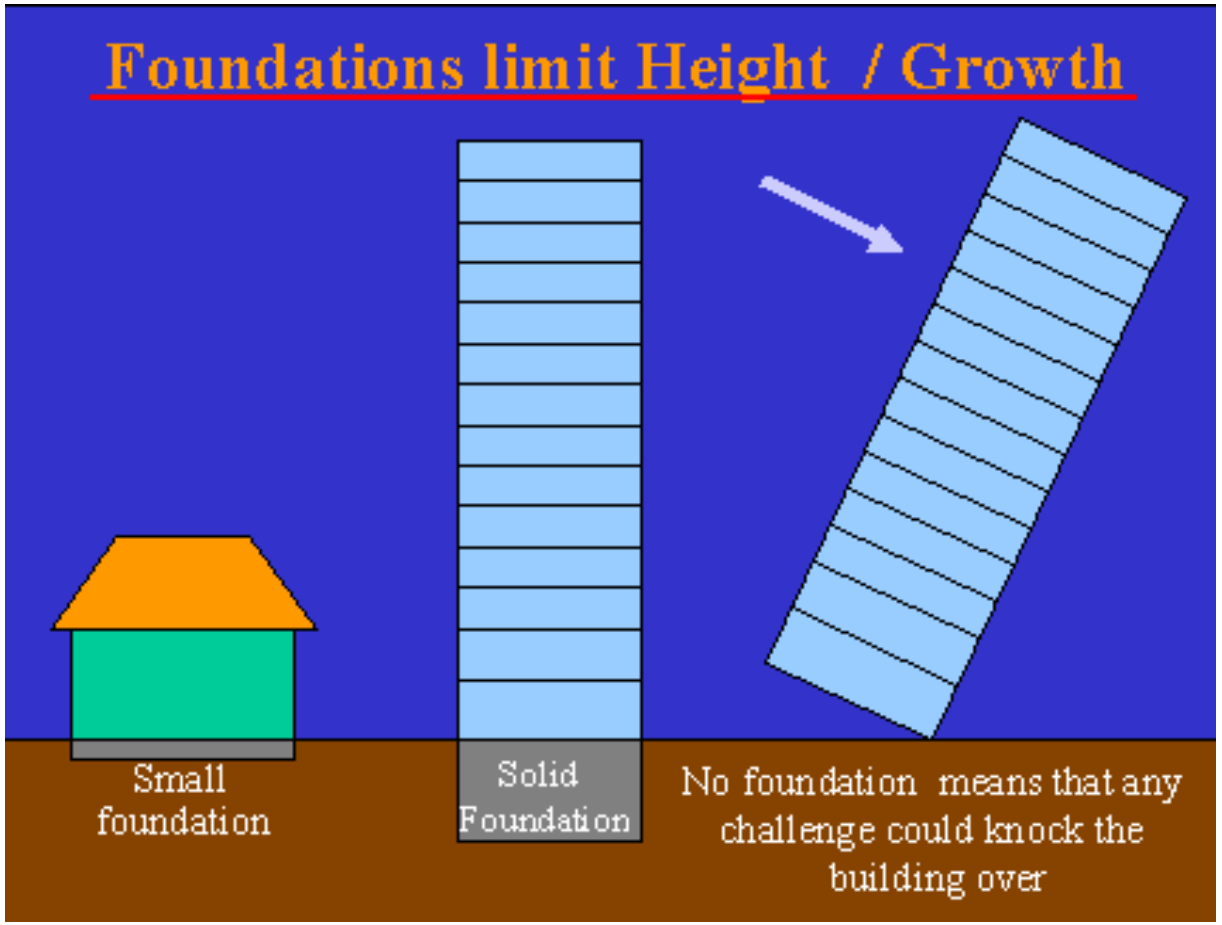
- Digital Libraries and Preservation
- How can we measure performance
- Introduction to the DRAMBORA Toolkit
- Progress on applying it to DLs



Keels and Laying the Keel



Risk Management Foundations for Digital Libraries



DRAMBORA and DLs: A Scientific Approach

Hypothesis	- A digital repository lies at the heart of a digital library. - Content preservation is a fundamental building block of a digital library system and environment.
Thesis	DRAMBORA can identify core principles of digital preservation that can be fed into the DELOS Digital Library Reference Model.
Demonstration	- Autumn 2007: DELOS JPA4, DDC and DPE will test DRAMBORA in international digital libraries, to assess whether or not the toolkit can be applied to the digital libraries context, and if not what modifications would be needed to it to make it applicable. - December 2007: presentation of results at DELOS conference in Pisa.

Digital Preservation Today

- Growth in creation of digital information with **scholarly**, **scientific** and **cultural** value continues to accelerate
- Practical approaches aimed at ensuring long-term **authenticity**, **integrity** and **understandability** of digital materials are emerging at a similar pace
- The discipline remains immature though:
  - Are adopted approaches **successful**?
  - What is the **metric** for defining success?
  - Which approaches are **appropriate** for particular digital preservation challenges?
  - Which preservation services and/or service providers can be **trusted**?

Trust, Trustworthiness and Safe Stewardship

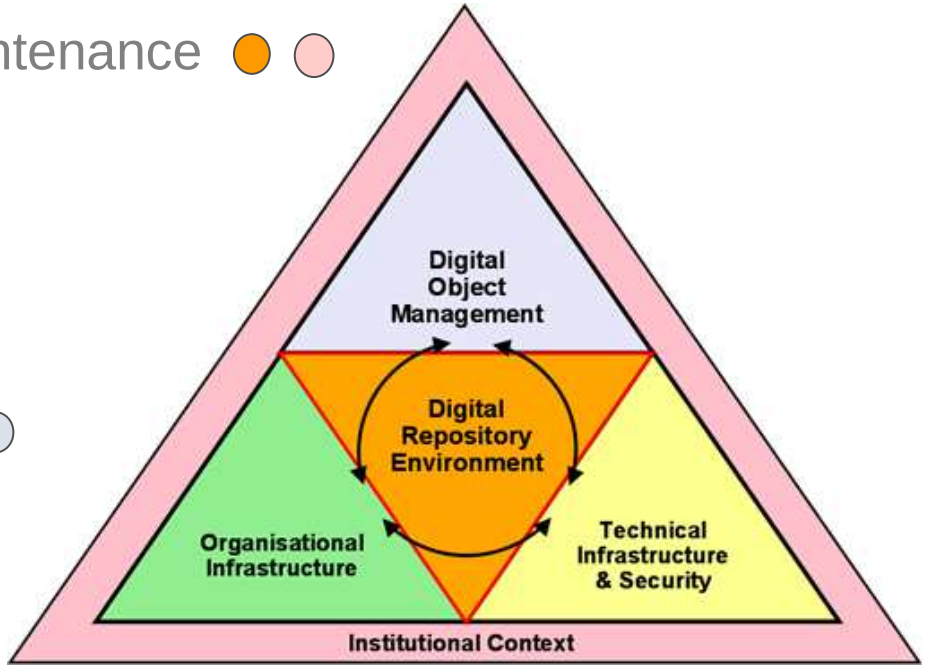
- Evolution of the Digital Preservation (specifically Repository) Landscape:
  - **Defining** the problem
    - *Preserving Digital Information*
    - *Trusted Digital Repositories: Attributes & Responsibilities*
  - **Practical Responses** to the problem
    - repository software [DSPACE, ePrints, Fedora];
    - metadata schema [PREMIS];
    - reference models [OAIS];

- This work focuses on **determining the success of the solutions we propose or have already deployed**

- *"Stewardship is easy and inexpensive to claim; it is expensive and difficult to honor, and perhaps it will prove to be all too easy to later abdicate"* Lynch (2003)

10 Characteristics of Digital Repositories

- An intellectual context for the work:
  - Commitment to digital object maintenance
  - Organisational fitness
  - Legal & regulatory legitimacy
  - Effective & efficient policies
  - Acquisition & ingest criteria
  - Integrity, authenticity & usability
  - Provenance
  - Dissemination
  - Preservation planning & action
  - Adequate technical infrastructure



Trust in repositories

- Trustworthiness – a key characteristic that a repository needs to demonstrate
- How can a repository demonstrate this
- Digital curation is all about taking organisational, procedural, technological and other uncertainties and transforming them into manageable risks

Existing memory institutions

- Are trusted in traditional paper environment
- Why assume their competence in the digital realm?
- New environment requires *all* players to establish trusted status
  - Taxonomy of goods/services (do they belong to same class) do they have similar qualities;
  - we need theory of underlying competence of trustworthy agent for a given task;
  - are the characteristics of that task relevant for a different task

Risk

- Are repositories capable of:
  - identifying and prioritising the risks that impede their activities?
  - managing the risks to mitigate the likelihood of their occurrence?
  - establishing effective contingencies to alleviate the effects of the risks that occur?
- If so, then they are likely to engender a trustworthy status – if they can demonstrate these capabilities

Meeting the shortfall

- Independent measuring of repositories is seen as an essential aim
- It's taken as axiomatic that audit is an appropriate mechanism for establishing repository trustworthiness
- Central to this discussion are issues of:
  - criteria for assessment
  - evidence
  - risk management

} particularly relevant for DRAMBORA

DRAMBORA

- *"A trusted digital repository will understand threats to and risks within its systems."* – from the introduction to the TRAC Criteria & Checklist

- Developed by DCC & DPE, DRAMBORA encourages 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.

- Methodology, tools and associated examples support:
  - **Validation** [*"Are my efforts successful?"*]
  - **Preparation** [*"What must I do to satisfy external auditors?"*]
  - **Anticipation** [*"Are my proposals likely to succeed?"*]

The origin of DRAMBORA: DCC Pilot Audits

- Digital Curation Centre (DCC) engaged in a series of pilot audits in diverse environments
- 6 UK, European and International organisations
- National Libraries, Scientific Data Centers, Cultural and Heritage Archives
- Rationale
  - establish evidence base
  - establish list of key participants
  - refine metrics for assessment
  - contribute to global effort to conceive audit processes
  - establish a methodology and workflow for audit

DRAMBORA Objectives

- The purpose of the DRAMBORA toolkit is to assist an auditor to:
  - define the mandate and scope of functions of the repository
  - identify the activities and assets of the repository
  - identify the risks and vulnerabilities associated with the mandate, activities and assets
  - assess and calculating the risks
  - define risk management measures
  - report on the self-audit

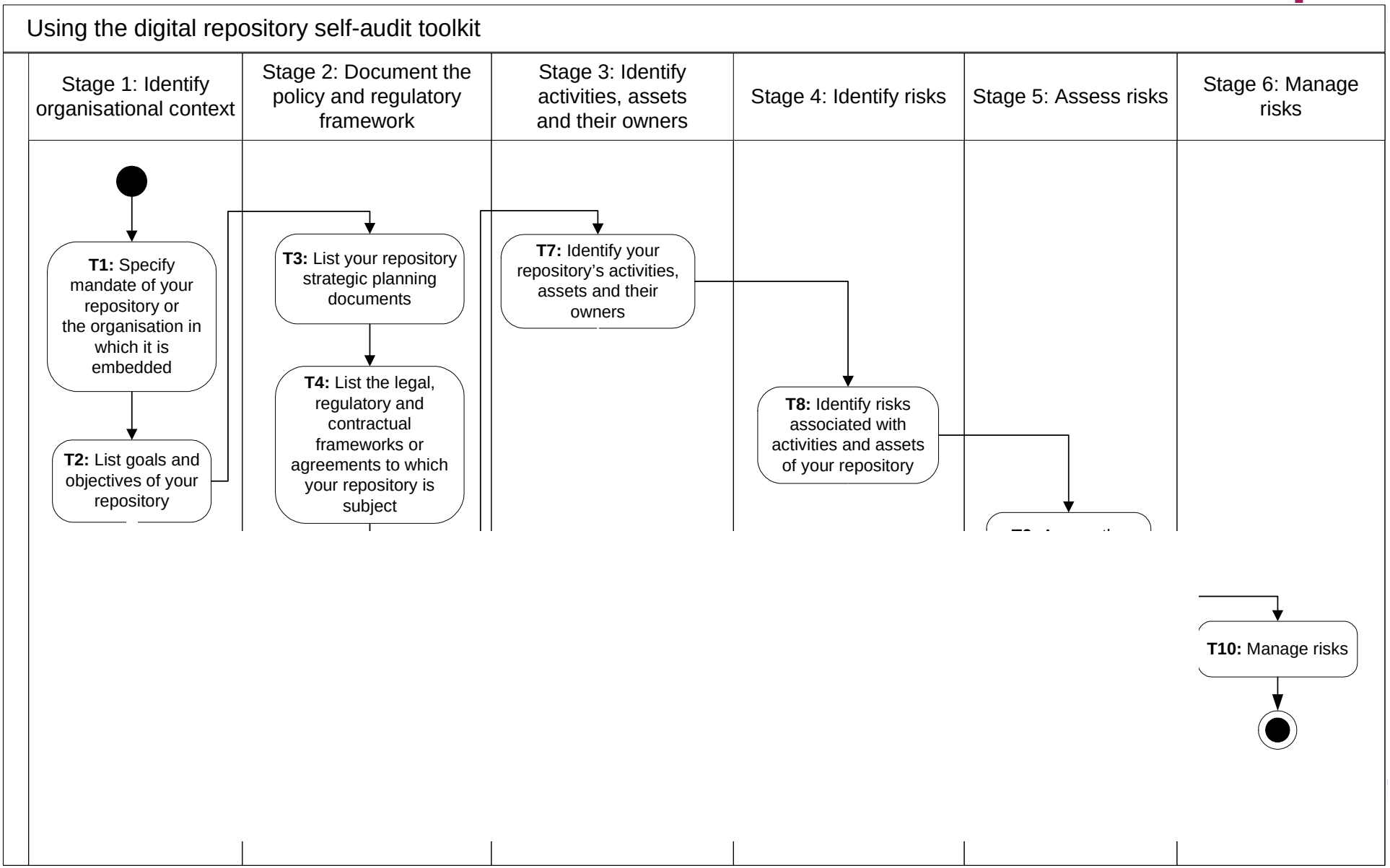
Benefits of DRAMBORA

- Following the successful completion of the self-audit, organisations can expect to have:
  - Established a **comprehensive and documented self-awareness** of their mission, aims and objectives, and of intrinsic activities and assets
  - Constructed a **detailed catalogue of pertinent risks**, related to digital repositories categorised according to type and inter-risk relationships
  - Created an **internal understanding** of the successes and shortcomings of the organisation
  - **Prepared the organisation** for subsequent external audit

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

DRAMBORA Workflow



Stage 4: Identifying Risks

- Assets & Activities associated with **vulnerabilities** – characterised as risks
- Auditors must build **structured list of risks**, according to associated activities and assets
- **No single methodology** – brainstorming structured according to activities/assets is effective

Kinds of risk

- **Assets or activities fail** to achieve or adequately contribute to relevant goals or objectives
- **Internal threats** pose obstacles to success of one or more activities
- **External threats** pose obstacles to success of one or more activities
- **Threats to organisational assets**

Example Risk: Budget cut/withdrawal of funding

- **Description**
  - Repository operational budget is cut or withdrawn
- **Example manifestation**
  - Local recession provokes budgetary reduction of government financed repository
  - Digital Library fails to demonstrate its centrality to its funding and user community.

Example Risk: Legal liability for IPR infringement

- **Description**
  - 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

- **Example manifestation**
  - 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

Example risk: Exploitation of IT security vulnerability

- **Description**
  - shortcomings in the repository's security provisions can be identified and used to gain unauthorized access to its systems

- **Example manifestation**
  - unpatched software security loopholes are hacked, or intruders gain physical access to the repository through a security door that is wedged open

Stage 5: Assess Risks

- Fundamental issues are:
  - Likelihood of risks
  - Potential impact of risks
  - Relationships between / groupings of risks

- A risk assessment must be undertaken for each identified risk

Stage 6: Manage Risks

- Combination of avoidance, tolerance and transfer
  - avoid circumstances in which risk arises
  - limit likelihood of risk
  - reduce potential impact of risk
  - share the risk
  - retain the risk

DRAMBORA Future

- Version 2.0 to be released at the start of October 2007, as an interactive online tool
- Autumn 2007: Digital Libraries audits within Digital Preservation Cluster of DELOS (JPA4)
- Dissemination of results and activities in scientific journals
- Version 3.0 in Spring 2008
- Accreditation of self-auditors in 2008

Thank you!

- If you have any further questions about the use of DRAMBORA in the context of digital libraries email us at:

  feedback@repositoryaudit.eu