DRAMBORA interactive

Self-audit and self-certification principles using DRAMBORA toolkit

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

---

About

- Concept of risk and risk management in digital preservation

- DRAMBORA methodology and activities

- DRAMBORA Interactive walkthrough

- Group exercise

- Discussion on exercise and Wrap-up

Digital objects break!

- **Inaccessibility of digital object**
  - Object becomes lost
  - Degradation of storage medium means content can not be read
  - Technological obsolescence

- **Syntactical interpretation or representation failures**

- **Semantic opaqueness**
  - Lack of contextual information (e.g. suitable metadata)
  - Loss of process & dynamic nature

- **Legal impediments**

- **The organisation and its staff**
    - Lack of organisational will
    - Decentralised and node-based organisation

© HATII UofGlasgow, 2005

Historic Media on Display at the Launch of the UK Digital Curation Centre (DCC), November 04 www.dcc.ac.uk

---

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.

Risk management

- **Risk management** is the process of measuring, or assessing risk and developing strategies to manage it

  1. **Risk assessment** is the determination of quantitative and/or qualitative value of risk related to a concrete situation and a recognized threat
  2. …….
  3. …….

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

Risks in daily life

Risk Management Model

IDENTIFY INTERNAL AND EXTERNAL CONTEXT

IDENTIFY RISKS

COMMU-NICATE

MONITOR AND REVIEW

ANALYSE AND ASSESS RISKS

MANAGE AND TREAT RISKS

Risk-Benefit Analysis (RBA)

- **Risk =** probability of the occurrence of an event multiplied (though it may not be mathematically multiplicative) by the severity of the event

- **Benefit** = a valued or desired outcome; an advantage

- **Risk-benefit analysis** = economic method of evaluation, based on comparison of the risk of a situation to its related benefits

- What constitutes a risk?
- Is a particular risk worth reducing?
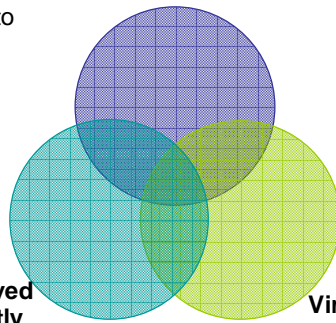- How much would it cost to reduce it?

Výstup na vlastní nebezpečí.
K Meridianové síni 22 schodů.
Na ochoz věže 87 schodů.

The ascent is made at one´s own risk.
There are 22 stairs to reach the meridian Room.
There are 87 stairs to reach the gallery
of the Tower.

RBA: evaluation of risks

e.g. cholera: need a microscope to see it and scientific training to understand

Perceived through science

e.g. global warming, low-level radiations, mobile phones, passive smoking (what scientists don't know or cannot agree)

Perceived directly

Virtual risk

e.g. climbing a tree, riding a bike, driving a car

J. Adams, Risk-Benefit Analysis, 1999

RBA: risk modelling

Flight insurance company – statistical risk

Passenger – perceived risk

European Aviation Safety Agency – projected risk

Risk management & digital preservation

- Lack of literature for risk-assessment in LIS vs. computer science

- Differences in definitions used by different disciplines

- The measurement of risk is problematic

- The greatest challenge is the interpretation of the risk, i.e., to determine when a risk is acceptable

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

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

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.

---

nestor *Catalogue of Criteria for Trusted Digital Repositories V1*

nestor - Working Group Trusted Repositories – Certification developed a **Catalogue of Criteria**

- aimed at German memory organisations and institutions, service providers devising, planning and implementing digital repositories
- provides guidance, tools for self-checking, and potentially certification
- **Abstract** *criteria*
  - applicable for a range of digital repositories, and valid over a longer period,
- Explanations, examples, references:
  - internationally discussed and standardised
  - render the state-of-the-art
  - reflect specific, national conditions (legal framework, organisational structure)
- Basic principle**: Adequacy**
  - evaluation is always based on the objectives and tasks individual digital repository concerned

www.digitalpreservation.de

nestor Catalogue example

` **1 The digital repository has defined its goals.**
The DR should have a clear conception of its objectives. It has determined which tasks it fulfils, and which principles it observes in doing so. This is crucial, as trustworthiness is not an absolute term, rather it depends on the goals of the particular DR. Following the principle of adequacy, evaluation of the individual criteria is always based on the specific goals. The DR ensures that its objectives are transparent so that others - most notably users and producers - can themselves gauge the repository's trustworthiness. (The goals are often published in the form of a "policy".)

[PANDORA: The purpose of the PANDORA Archive, 2006]
[Oxford Digital Library: Background, Services, Principles and Guidelines, 2006]
[Dokumenten- und Publikationsserver der Humboldt-Universität zu Berlin: Ziele und
*   inhaltliche Kriterien, 2006]*
[National Archives: Custodial policy for digital records, 2006]
[Erpanet: Erpanet-Tagung "Policies for Digital Preservation", 2003]

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   DCC

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?"*]

So what is the difference?

A pizza recipe
- 500 gr of flour
- 1 cup warm water
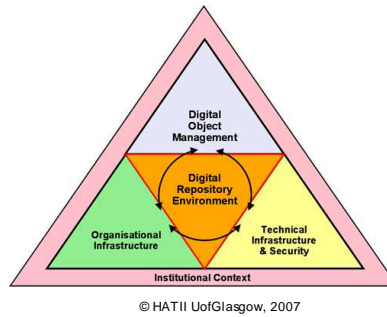- 1 tablespoon of yeast
- 1/4 cup olive oil
- a pinch of salt
+ topping
+ process

What do I want my pizza to be like and why? Do I have the means to make it? Did I make it the way I wanted it? How can I improve?
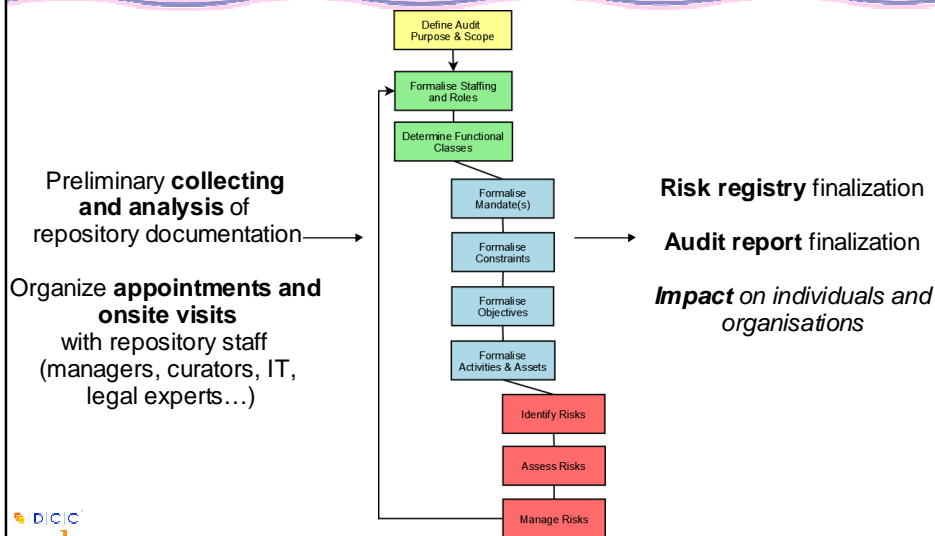
10 Characteristics of Digital Repositories

- 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/nestor/DCC/DPE meeting, January 2007)

DRAMBORA Workflow

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

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

Documentary Evidence

- Sometimes mere presence will be encouraging, other times content will require scrutiny
- Several example documents
    - Risk Register
    - Repository Mission Statement
    - Example Deposit Agreements (including legal arrangements)
    - Job Descriptions
    - Organisational Chart
    - Staff Profiles/CVs/Resumes
    - Annual Financial Reports
    - Business Plan
    - Policy Documents

Documentation (continued)

- System Procedure Manuals
- Technical Architecture
- Maintenance Reports
- Results of Other Audits
- Other Documentation Records
- Document and records management processes provide insights
- Privacy concerns must be addressed
- Evaluation methods must be refined

Testimonial Evidence

- Useful means to:
  - highlight where omissions exist in documentation
  - validate whether documented aspirations are realised in reality
- Roles for interview:
  - Repository Administrators
  - Hardware and Software Administrators
  - Repository Function-specific Officers
  - Depositors
  - Information Seekers
- Questionnaire templates being formulated by DCC

Observation of Practice Evidence

- Less objectively quantifiable, but nevertheless important
- Especially appropriate in terms of procedure and workflow
- Might include
  - walkthroughs
  - testing and measurement of characteristics of objects after preservation action
  - deposit and assessment of test objects (perhaps incrementally over several audits)

Regulatory constraints

- Acts of Parliament:
  - Legal Deposit Libraries Act
  - Copyright, Designs and Patents Act
- European Directives, Regulations and Decisions:
  - Directive 2001/29/EC (European Copyright Directive)
- Contractual agreements:
  - Deposit agreement with Depositor X
- Standards:
  - ISO 9000:2000 Quality Management Systems Series
  - ISO 27001:2005 Information technology - Security techniques - Information security management systems - Requirements
- Voluntary codes:
  - Repository X operations manual (2007)
  - Preferred Ingest File Formats (2006)

Examples of activities and assets

Acquisition & Ingest

Activity: Verify completeness and correctness of received content
Assets: Digital objects; list of file formats; list of levels of preservation treatment desired for that format by the owner

Activity: Monitor and ingest of SIPs
Assets: Submission package definition; checksums

Example Risk

- **Liability for regulatory non-compliance**
  - Repository is liable for failure to conduct its activities in accordance with industrial, business oriented or global regulation

- **Example manifestation**
  - Repository fails to conform to appropriate jurisdictional health and safety regulations for employees

Example Risk

- **Media degradation or obsolescence**
  - Storage media deteriorates, limiting the extent to which it can be written to and read from

- **Example manifestation**
  - Tape stored content is inaccessible or corrupted due to deterioration of magnetic tape
  - Contemporary tape drives are incapable of reading dated storage media which is prolific throughout archive

Anatomy of a risk (I)

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

Anatomy of a risk (II)

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*

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

---

Risk Management & DRAMBORA

- The toolkit refrains from prescribing specific management policies
- Instead, auditors should:
  - choose and describe risk management strategy
  - assign responsibility for adopted measure
  - define performance and timescale targets
  - reassess success recursively

Management Risk: Steps

- Auditors should:
  - identify suitable risk responses
  - identify practical responses to each risk
  - identify owners for risk management activities
  - investigate threats arising from risk management
  - prioritise risks
  - update risk register and circulate information
  - secure approval for planning and allocations

Example: Avoidance or Treatment

- Legal liability for IPR infringement
- Avoidance
  - Assess preserved materials to determine those to which IPR restrictions may apply
  - Seek legal advice to determine legality of actions
- In the event of risk's execution
  - Establish policies and procedures to follow in the event of IPR challenge

Example: Avoidance or Treatment

- Staff skills become obsolete
- Avoidance strategies
  - Establish means for staff training, and for staff to employ skills of limited *frequent* value in test environment
  - Implement staff performance reviews to identify skill levels and training req'ts
- In the event of risk's execution
  - Provide training to reverse obsolescence

Example: Transfer Strategy

- Enforced cessation of repository operations
- Transfer Strategy
  - Establish succession arrangements
  - Establish contingency plans or escrow arrangements
  - Establish exit strategy

Example: Tolerance Strategy

- Preservation strategies result in information loss
- Tolerance Strategy
  - Implement policy to define the parameters of acceptable loss resulting from these activities

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 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, Edinl [image] 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

Ludwig Boltzmann Gesellschaft

E-LIS E-prints in Library and Information Science
eprints.rclis.org

Lietuvos etnokosmologijos muziejus

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

MBooks

Gallica la bibliothèque numérique

BRITISH LIBRARY

USGS science for a changing world

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

What we are working on now

- Promotion of the assessment method and toolkit
- 1208 downloads of the toolkit
- 2052 downloads of DRAMBORA manual v1.0
- 77 registered audits
- DELOS report
- DPE Training Programme
  - Development of training materials to support self-assessment
  - Training for general public
  - Training for auditors (Prague 08, London 09, Madeira? 09)
  - Accreditation of self-auditors
- Discussion with other working groups developing repository audit checklists

Further developments for DRAMBORA

- Repository profiling

- DRAMBORA in Japan

- Dissemination in international conferences and journals

- Version 3.0 (downloadable), added visual features, translations in local languages

---

DRAMBORA Interactive

www.repositoryaudit.eu

User Administration

- Any logged in user can update their own details at any time

- You can also limit the IP addresses that this user may log in from, for security purposes; this supports wild cards
  - *.*.*.* for example permits access from any IP
  - 130.209.*.* permits access from anywhere on the 130.209.x.x network

- It is recommended that you restrict access to only your IP or local network range
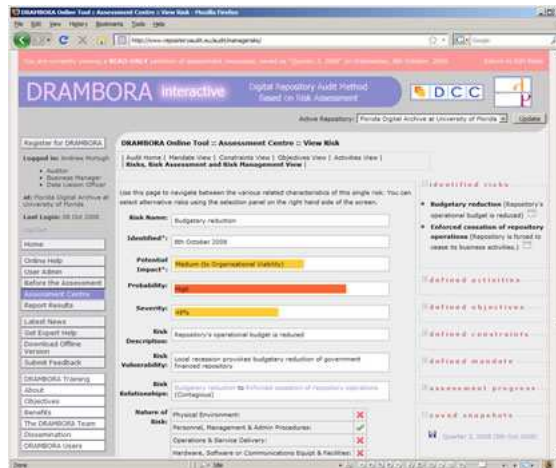
Manage Risks
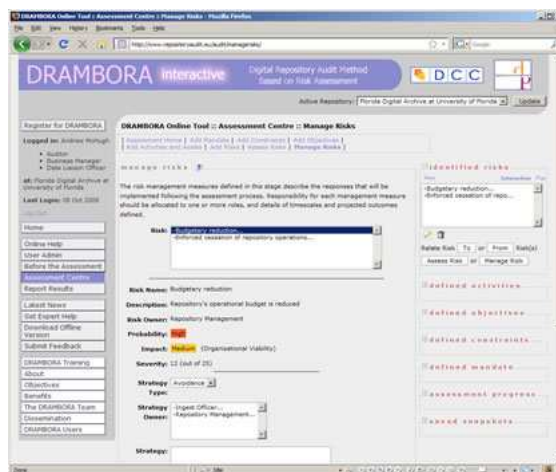
Audit Reporting
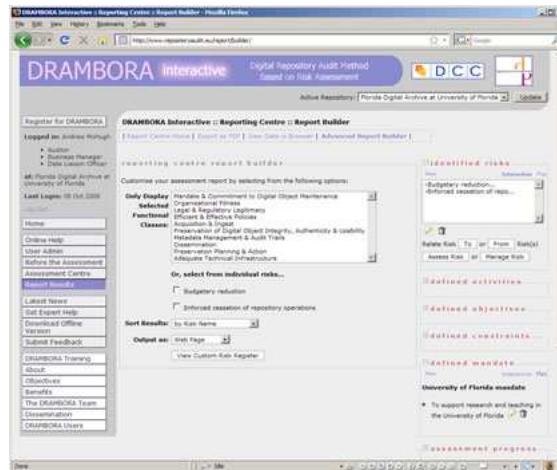
Save Audit Snapshots

- This feature lets you record the state of the repository at a particular time
- This facilitates comparison at a later date
- Can be used to track improvements (or deterioration) over time
- A read-only view of the saved responses facilitates analysis of inter-relationships between repository information – a useful reporting tool in itself

Save Audit Snapshot

Group exercise!

– Ca 5 groups (maybe your table fellows last night ☺ ?)

– Identify 2 risks for Gallica within the 2 assigned functional classes
- Group 1 *Commitment to digital object maintanance; Organisational fitness*
- Group 2 *Legal and regulatory legitimacy; Effective and efficient policies*
- Group 3 *Acquisition and ingest; Preservation of digital object integrity, authenticity and usability*
- Group 4 *Metadata management and audit trail; Access and dissemination*
- Group 5 *Preservation planning and action, Technical infrastructure and security*

– Use Gallica summary provided and check Gallica website if needed

– Group leader will report back in 30 min

Why assessing repositories 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

DCC

Think metric!

DRAMBORA:
converting uncertainties into manageable risks

www.repositoryaudit.eu

THANK YOU

DRAMBORA Auditors Training: Prague, October 2008   63