





digital preservation Europe

The DRAMBORA Toolkit: How we got here and where it can take you

Seamus Ross, Andrew McHugh,
 Raivo Ruusalepp & Hans Hofman

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

IS&T Archiving Conference, Virginia, USA, 21 May 2007




 Building Trust in Digital Repositories Using **DRAMBORA** 1

Principles of Trustworthy Repositories






digital preservation Europe


- DCC, DPE, CRL and *nestor* met in Chicago in January 2007
- Conceived a global, united perspective on trustworthiness and digital archives
- 10 General Characteristics of Digital Preservation Repositories
- <http://www.crl.edu/content.asp?l1=13&l2=58&l3=162&l4=92>




 Building Trust in Digital Repositories Using **DRAMBORA** 3




Background





digital preservation Europe

- DRAMBORA developed by Digital Curation Centre (DCC) & DigitalPreservationEurope
- Closely allied with TRAC, *nestor* criteria, & work of Centre for Research Libraries
- Work conducted by
 - Andrew McHugh (HATII/DCC/DPE),
 - Raivo Ruusalepp (NANETH/DPE/Estonian Business Archives),
 - Seamus Ross (HATII/DCC/DPE), and
 - Hans Hofman (NANETH/DPE).




 Building Trust in Digital Repositories Using **DRAMBORA** 2

Repositories 10 Principles CRL/RLG-OCLC/NESTOR/DPE/DCC





digital preservation Europe

- The repository commits to continuing maintenance of digital objects for identified community/communities.
- Demonstrates organizational fitness (including financial, staffing structure, and processes) to fulfill its commitment.
- Acquires and maintains requisite contractual and legal rights and fulfills responsibilities.
- Has an effective and efficient policy framework.
- Acquires and ingests digital objects based upon stated criteria that correspond to its commitments and capabilities.




 Building Trust in Digital Repositories Using **DRAMBORA** 4

DCC
digital preservation Centre

Repositories 10 Principles CRL/RLG-OCLC/NESTOR/DPE/DCC

- Maintains/ensures the integrity, authenticity and usability of digital objects it holds over time.
- Creates 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.
- Fulfills requisite dissemination requirements.
- Has a strategic program for preservation planning and action.
- Has technical infrastructure adequate to continuing maintenance and security of its digital objects.

Building Trust in Digital Repositories Using DRAMBORA 5

DCC
digital preservation Centre

Establishing Trust in a Repository

- How is it established?
- How is it maintained?
- How is it secured?
- What happens when it is lost?
- How can it be verified?
- Can repositories *do* what the say and *show* that they do what they say?
- Have they thought about what they are doing?

Building Trust in Digital Repositories Using DRAMBORA 7

DCC
digital preservation Centre

Critical Services Require Trust

- Task Force on Archiving of Digital Information asserted in 1996:
“a critical component of digital archiving infrastructure is the existence of a sufficient number of trusted organizations capable of storing, migrating, and providing access to digital collections.”
- RLG/OCLC “Trusted Digital Repositories – Attributes and Responsibilities” (2002)
 - depositors trust information holders
 - information holders trust third party service providers
 - users trust digital assets provided by repositories

Building Trust in Digital Repositories Using DRAMBORA 6

DCC
digital preservation Centre

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

Building Trust in Digital Repositories Using DRAMBORA 8

The Challenge







- Independent measuring of repositories is seen as essential aim
- Taken as axiomatic that audit is a mechanism for establishing the trustworthiness of a repository
- We seek to develop the debate on the evidence required for objective and transparent assessment
- Two earlier pieces form a backdrop to this talk:
 - S Ross and A McHugh, 2006, 'The Role of Evidence in Establishing Trust in Repositories', D-Lib Magazine, July/August, v.12, n7/8 (Also published in *Archivi e Computer*, August 2006), <http://www.dlib.org/dlib/july06/ross/07ross.html>
 - S Ross and A McHugh, 2005, 'Audit and Certification: Creating a Mandate for the Digital Curation Centre', *Diginews*, 9.5, ISSN 1093-5371, http://www.rig.org/en/page.php?Page_ID=20793#article1







Building Trust in Digital Repositories Using **DRAMBORA**
9

Existing Standards Context







- Efforts must also fit gracefully alongside:
 - ISO 9000 series (Quality Assurance)
 - ISO 17799 & 27001 (Information Security)
 - ISO 15489 (Institutional Records Management)
 - ISO 14721 (Reference Model for an Open Archival Information System)
 - COBIT 4.1 (2007)







Building Trust in Digital Repositories Using **DRAMBORA**
11

Defining Activities and Context







- DCC and DPE collaborations include:
 - Trustworthy Repository Audit and Certification (TRAC) Criteria and Checklist Working Group
 - <http://www.crl.edu/PDF/trac.pdf>
 - Center for Research Libraries (CRL) Certification of Digital Archives Project
 - <http://www.crl.edu/content.asp?l1=13&l2=58&l3=142>
 - Network of Expertise in Long-term storage of Digital Resources (nestor)
 - <http://edoc.hu-berlin.de/series/nestor-materialien/8/PDF/8.pdf>
 - International Audit and Certification Birds of a Feather Group
 - <http://www.digitalrepositoryauditandcertification.org>




Building Trust in Digital Repositories Using **DRAMBORA**
10




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




Building Trust in Digital Repositories Using **DRAMBORA**
12

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*

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

Pilot Audit Themes



- Need to describe evidence base
 - To contribute towards consistency
 - To create a mechanism that ensures conclusions can be validated and replicated
 - Practical, applicability depends on identification of objective means to demonstrate compliance
 - Efforts must probe for evidence of *concrete* processes, structures and functionality
 - Documentary, testimonial, and observational evidence
- Need to establish 'preservation pressure points' including uncertainties and risks
 - Risk awareness is low within the community

Documentation (continued)



- System Procedure Manuals
- Technical Architecture
- Maintenance Reports
- Results of Other Audits
- Other Documentation Records
- Document 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

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

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)

Approach to Assessment



- Four key principles lie at the heart of our assessment methods:
 - It should be a self-audit that repositories do themselves, based on the provided tools
 - Self-audit could be a preparatory step for external audit
 - It should be flexible and be valid for repositories of all shapes and sizes and of different contexts
 - It should be assessing how well the repository is managing the risks it is facing when it does what it does
 - It should offer advice on how to overcome the risk situations and what other repositories have done in similar situations

DRAMBORA



- Easy to say establish evidence and recognise risk, but how do you do this and then take advantage of this knowledge
- *Digital Repository Audit Method Based on Risk Assessment (DRAMBORA)*
- Provides mechanisms to facilitate internal self-assessment & reporting
 - Validates appropriateness of repository's efforts
 - Provides means to generate appropriate documentation
- External certification less of a priority currently, and less immediately viable

Not Yet Another Checklist?



- Existing methods are:
 - too static – ‘one size fits all’ approach
 - too much fixed on the OAIS reference model
 - too little emphasis on evidence in the auditing process
- Audit results should help to manage the repository better continuously, not just give a one-time evaluation

Developing DRAMBORA



- Follows lessons learned from DCC pilot audits
- A collaborative exercise between DCC and DigitalPreservationEurope
- Development will continue with a further period of pilot assessments, training workshops and the release of subsequent versions during 2007 and 2008
- You can download the toolkit at <http://www.repositoryaudit.eu>

Core Aspects



- The Authentic and Understandable Digital Object
- Based upon established risk management principles
- Bottom-up approach to assessment (in contrast with TRAC and *nestor methodologies*)
- *Not about benchmarking, but could be used alongside benchmarking standards or criteria*
- *Proactive and retroactive applications*

Risk and Digital Preservation



- Transforming uncertainties into manageable risks
- ERPANET Risk Communication Tool
 - <http://www.erpanet.org/guidance/docs/ERPANETRiskTool.pdf>
- Cornell University Library VRC
 - <http://irisresearch.library.cornell.edu/VRC/methods.html>

Assessing risk



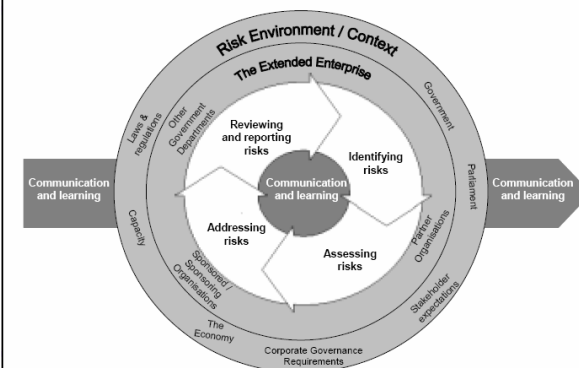
- Most risk assessment exercises are based on a benchmark that is established first
- By defining what success means first it is easy to assess how far from this measure you currently are
- Enterprise risk management is emerging
- Australian Risk Management Standard AS/NZS 4360, latest version is from 2004

Principles



- Appropriateness of auditor
- Measurability of assessment
- Documentation (evidence)
- Flexibility/fluidity to suit a diverse range of repository environments

Risk Management Model



DRAMBORA Stages

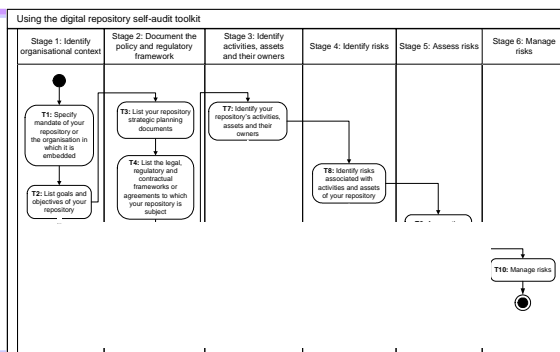
DRAMBORA requires auditors to undertake the following 6 stages:

1. Identification of objectives
2. Identification of policy and regulatory framework
3. Identification of activities and assets
4. Identifying risks related to activities and assets
5. Assessing risks
6. Managing risks

Ten Tasks

- What is the mandate of your repository?
- What are the goals and objectives of your repository?
- What policies does your repository have in place to support and regulate how these goals and objectives are to be achieved?
- What legal, contractual and other regulatory requirements / confines does your repository operate in?
- What standards and codes of practice does your repository follow?
- Any other things that influence how your repository does the what it is supposed to be doing?

DRAMBORA Workflow



Ten Tasks

- What are the activities that your repository does to achieve its goals and objectives within the context and confines set by the regulatory environment, and what assets do you use and produce in the course of these activities, including staff, skills, knowledge, technology?
- What are the risks associated with all of the above?
- How would you assess these risks?
- How do you manage these risks?

DRAMBORA Outcomes



- Documented organisational self-awareness;
- Catalogued risks;
- Understanding of infrastructural successes and shortcomings;
- Preparation for full scale external audit.

Anticipated applications



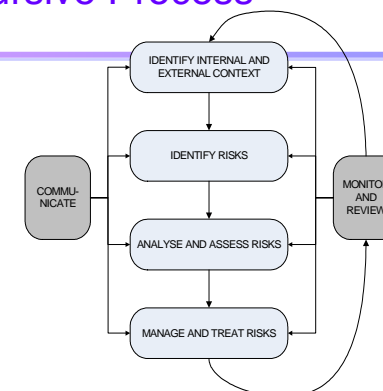
- Validatory: Internal self assessment to confirm suitability of existing policies, procedures and infrastructures
- Preparatory: A precursor to extended, possibly external audit (based on e.g., TRAC)
- Anticipatory: A process preceding the development of the repository or one or more of its aspects

Interpreting Results



- The self-audit produces a composite risk score for each of eight functional classes.
- This numeric result can be compared with risk scores of other functional classes and allows the identification of the areas of repository work that are most vulnerable to threats.

A Recursive Process

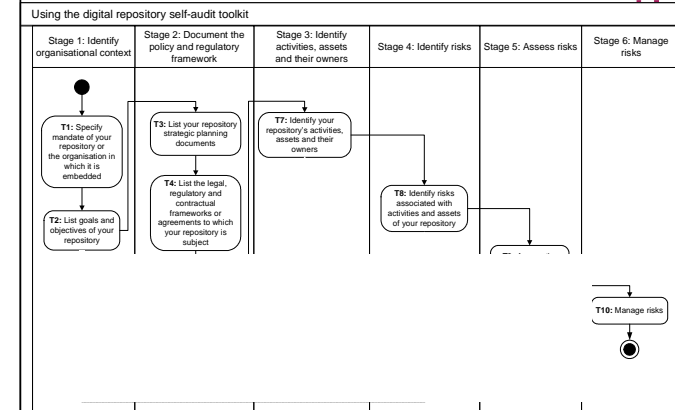


DRAMBORA Stages



- Establish organisational profile
- Develop contextual understanding
- Identify and classify repository activities and assets
- Derive registry of pertinent risks
- Undertake assessment of risks (and existing management means)
- Commit to management strategies

DRAMBORA Workflow



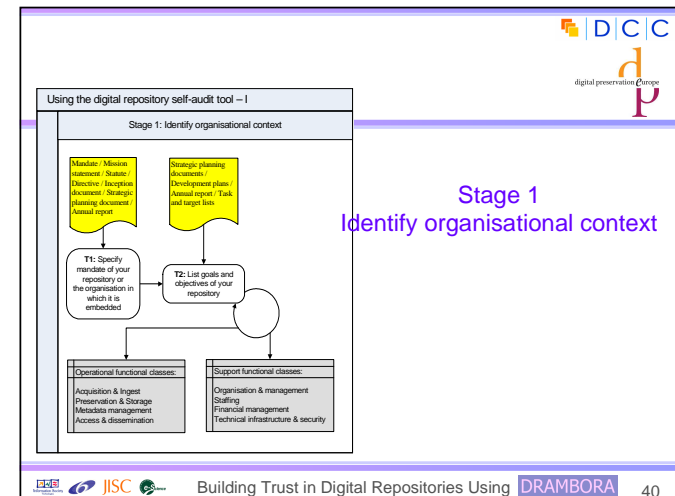
Your role



We would like you to:

- Learn today how to use the audit toolkit
- Use it in a test-audit on any digital repository
- Tell us:
 - what results did you get?
 - where do you think the methodology should be improved and how?
 - what functionality should the on-line tool have?

Stage 1 Identify organisational context



Organisational Context



- The first stage in developing an organisational profile
- Building a platform to facilitate risk awareness
- Success reflects organisational characteristics and aspirations

Organisational Mandate



- Example Mandate:
 - The role of *[repository_name]* is to assist researchers to locate, access and interpret *[type_of_data]* produced by *[named_data_creator_group]* and to ensure its long term integrity.

Stage 1: Tasks

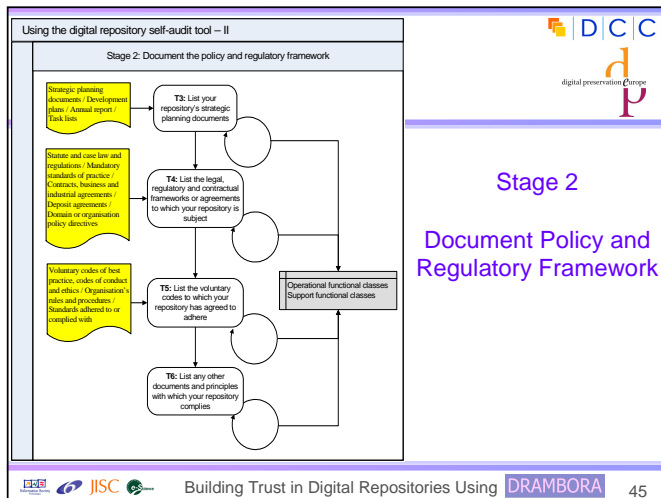


- Identify organisational mandate
 - derived from mission statement or enacting instrument
- Identify organisational goals
 - why does organisation exist?
- Well established means for subsequent risk definition and assessment
- Success demands access to personnel and documentation

Organisational Goals



- Associated with one of 8 functional classes
 - Acquisition & Ingest
 - Preservation & Storage
 - Metadata Management
 - Access & Dissemination } operation classes
 - Organisation & Management
 - Staffing
 - Financial Management
 - Technical Infrastructure & Security
- } supporting classes



Strategic Planning Documents

- Identified within:
 - procedural or operational manuals
 - intranet or shared network storage
 - wikis
- Includes
 - Policies
 - Procedures

Document policy and regulatory framework

- Aimed at ensuring the repository:
 - operates correctly with respect to regulatory frameworks
 - has an efficient and effective policy framework
 - is aware of societal, ethical, juridical and governance frameworks
 - is aware of legal, contractual and regulatory requirements to which it's subject

Legal, regulatory, contractual frameworks

- Including:
 - Statute, case law and regulations
 - Mandatory standards of practice
 - Domain specific regulations
 - Contractual obligations and service level agreements
- Inferred by determining:
 - nature of repository; its domain area; relevant legislation (e.g. enacting legislation); third party contracts

Voluntary codes & other documents



- Voluntary codes:
 - Standards imposed upon or adopted by repository
 - Standards forming the basis for other audits
 - Formal compliance programmes
 - Existing risk management programmes
- Other documents
 - e.g., Internal memorandums

Activities, Assets and Owners



- Building conceptual model of what the repository does
 - split broad level mission and goals into more specific activities or work processes
 - assign to individual responsible actors
 - link to one or more key assets
 - **clues within:** business process re-engineering; imaging & workflow automation; activity-based costing or management; business classification development; quality accreditation; systems implementation

Using the digital repository self-audit tool – III



Stage 3: Identify activities, assets and their owners

T7: Identify your repository's activities, assets and their owners

Strategic objectives and goals listed under Tasks 1 and 2/ Policy and regulatory framework from Tasks 3 - 6

Operational functional classes
Support functional classes

Stage 3

Identify Activities, Assets and their Owners

Instructions for this stage



- Hierarchical analysis
 - breaking up organisation's activities into logical parts and sub-parts
 - charter
 - what makes organisation unique?
 - functions and operations
- Process Analysis
 - look in more detail at how repository conducts its business and what is involved

Organisational Assets



- Includes:
 - information (databases, data files, contracts, agreements, documentation, policies and procedures)
 - software assets
 - physical assets
 - services and utilities
 - processes
 - people
 - intangibles, such as reputation

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

Using the digital repository self-audit tool – IV



Stage 4: Identify risks associated with activities and assets

T8: Identify risks associated with activities and assets of your repository

Strategic objectives and goals listed under Tasks 1 and 2 / Activities, assets and owners listed under Task 7

Operational functional classes
Support functional classes


Stage 4
Identify Risks


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

Anatomy of a Risk







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
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




Building Trust in Digital Repositories Using **DRAMBORA**
57

Using the digital repository self-audit tool – V





Stage 5: Assess risks




T9: Assess the identified risks


Risks listed under Task 8 / Risk calculation principles


Operational functional classes
Support functional classes

Stage 5




Assess Risks




Building Trust in Digital Repositories Using **DRAMBORA**
59







Risk Relationship	Definition of Risk Relationship
Explosive	where the simultaneous execution of n risks has an impact in excess of the sum of each risk occurring in isolation
Contagious	where a single risk's execution will increase the likelihood of another's
Complementary	where avoidance or treatment mechanisms associated with one risk also benefit the management of another
Domino	where avoidance or treatment associated with a single risk renders the avoidance or treatment of another less effective
Atomic	where risks exist in isolation, with no relationships with other risks







Building Trust in Digital Repositories Using **DRAMBORA**
58

Assess Risks





- Fundamental issues are:
 - probability of risks
 - potential impact of risks
 - Relationships between / groupings of risks
- A risk assessment must be undertaken for each identified risk




Building Trust in Digital Repositories Using **DRAMBORA**
60

Risk Assessment



- For each risk auditors must record:
 - example manifestations of risk
 - probability of its execution
 - potential impact of its execution
 - relationships with other risks
 - risk escalation owner
 - severity of risk (quantification of seriousness, derived as product of probability and impact)

Risk Impact Score	Interpretation
0	<i>Zero</i> impact, results in zero loss of ability to ensure digital object authenticity and understandability.
1	<i>Negligible</i> impact, results in isolated but fully recoverable loss of digital object authenticity and understandability
2	<i>Superficial</i> impact, results in widespread but fully recoverable loss of digital object authenticity and understandability
3	<i>Medium</i> impact, results in total but fully recoverable loss of digital object authenticity and understandability
4	<i>High</i> impact, results in isolated loss, including unrecoverable loss of digital object authenticity and understandability
5	<i>Considerable</i> impact, results in widespread loss, including unrecoverable loss or loss that is recoverable only by third party of digital object authenticity and understandability
6	<i>Cataclysmic</i> impact, results in total and unrecoverable loss of digital object authenticity and understandability

– Note that we use understandability in its broadest sense to encapsulate technical, contextual, syntactical and semantic understandability.

Risk Impact Score	Interpretation
0	<i>Zero</i> impact, results in zero deterioration of ability to ensure digital object authenticity and understandability
1	<i>Negligible</i> impact, results in isolated, non-serious and recoverable deterioration of ability to ensure digital object authenticity and understandability
2	<i>Superficial</i> impact, results in isolated but non-serious and/or fully recoverable deterioration of ability to ensure digital object authenticity and understandability
3	<i>Medium</i> impact, results in widespread or organisation-wide but non-serious and/or fully recoverable deterioration of ability to ensure digital object authenticity and understandability
4	<i>High</i> impact, results in isolated, serious and non-recoverable deterioration of ability to ensure digital object authenticity and understandability
5	<i>Considerable</i> impact, results in widespread, serious deterioration of ability to ensure digital object authenticity and understandability, which is unrecoverable or recoverable only by third party intervention
6	<i>Cataclysmic</i> impact, results in organisation-wide, terminal, and unrecoverable loss of ability to ensure digital object authenticity and understandability

Risk Impact

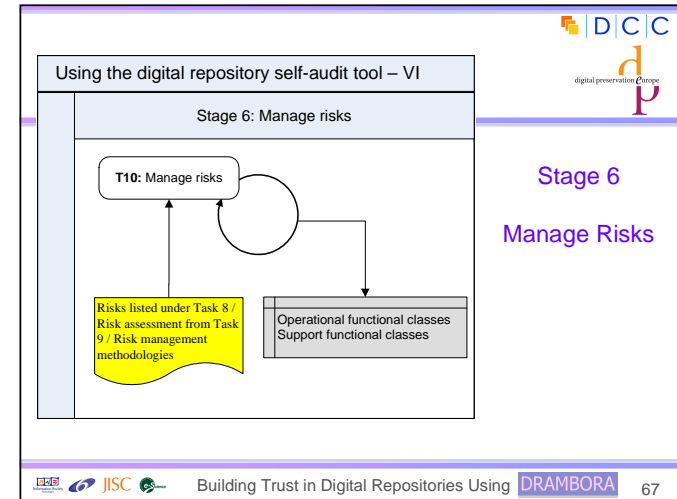


- Impact can be considered in terms of:
 - impact on repository staff or public well-being
 - impact of damage to or loss of assets
 - impact of statutory or regulatory breach
 - damage to reputation
 - damage to financial viability
 - deterioration of product or service quality
 - environmental damage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

DCC
digital preservation Centre

Risk Probability Score	Interpretation
1	Minimal probability, occurs once every 100 years or more
2	Very low probability, occurs once every 10 years
3	Low probability, occurs once every 5 years
4	Medium probability, occurs once every year
5	High probability, occurs once every month
6	Very high probability, occurs more than once every month

Building Trust in Digital Repositories Using DRAMBORA 65



- DCC
digital preservation Centre
- ## Determining impact and likelihood
- Consider:
 - Historical experiences
 - Mitigation/avoidance measures already in place
 - Experiences beyond repository itself
 - Relevant research
 - Expert opinion (e.g. legal, technical, environmental)
 - Experiences of comparable organisations
- Building Trust in Digital Repositories Using DRAMBORA 66

- DCC
digital preservation Centre
- ## 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
- Building Trust in Digital Repositories Using DRAMBORA 68

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

Interpreting the Audit Result



- Composite risk score enables quantification of risks' severity
 - illustrates vulnerabilities
 - facilitates resource investment
- Online tool will feature rich reporting mechanisms
 - what should this consist of?

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

After the audit



- Improvement requires ongoing activity
 - are risk management strategies working?
 - are risks within a satisfactory tolerance level?
 - risk exposure must be reassessed on an ongoing basis
 - risk management strategies must be re-evaluated
 - management must be informed of developments

What we'd like to know



- What features would you like to see within the toolkit's online version?
- What have you learned about your repository following DRAMBORA assessment?
- Have you combined DRAMBORA effectively with other tools/check-lists?

Closing Questions?



- If you have any further questions please email us at feedback@repositoryaudit.eu
- We'd be delighted to hear of your own experiences using the DRAMBORA toolkit

DRAMBORA Future



- Test audits and feedback on the methodology – Spring-Summer 2007
- Version 2.0 to be released in September, as an interactive on-line tool
- Produce a formal audit report at the end of the self-audit
- Version 3.0 in Spring 2008
- Certification of self-auditors in 2008 (?)