



Chiara Cirinnà

Building Trust in Digital Repositories Using DRAMBORA

Tutorial: Long Term Preservation of digital assets: basics concepts and practices
Florence 14 December 2009

DRAMBORA

DRAMBORA = Digital Repository Audit Method
Based On Risk Assessment

Self-audit toolkit

to facilitate internal audit by providing repository administrators with a means to assess their **capabilities**, identify their **weaknesses**, and recognise their **strengths**

What Digital Preservation Europe is?



Coordination Action financed by EC [FP6]

Two macro objectives:

to foster collaboration and synergies among
on-going projects and existing
initiatives across the ERA

[repositories and audit and certification tools]

to raise up awareness on digital preservation challenges
among different user communities

[different level of awareness on the subject
and its strategic significance]

DRAMBORA - Activities and Context

DCC and DPE collaborations include:

- Trustworthy Repository Audit and Certification (TRAC) Criteria and Checklist Working Group
- Network of Expertise in Long-term storage of Digital Resources (nestor)
- Center for Research Libraries (CRL) Certification of Digital Archives Project

DCC Pilot Audits

Digital Curation Centre (DCC) engaged in a series of pilot audits in diverse environments in 2006/07

- 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
 - establish a methodology and workflow for audit

Filling a Gap

Existing methods are:

- too static - 'one size fits all' approach
- no associated metrics
- too little emphasis on evidence in the auditing process

International consensus on methodology and criteria for auditing digital repositories remains an essential outcome

Objectives

The purpose of the DRAMBORA toolkit is to facilitate the auditor in:

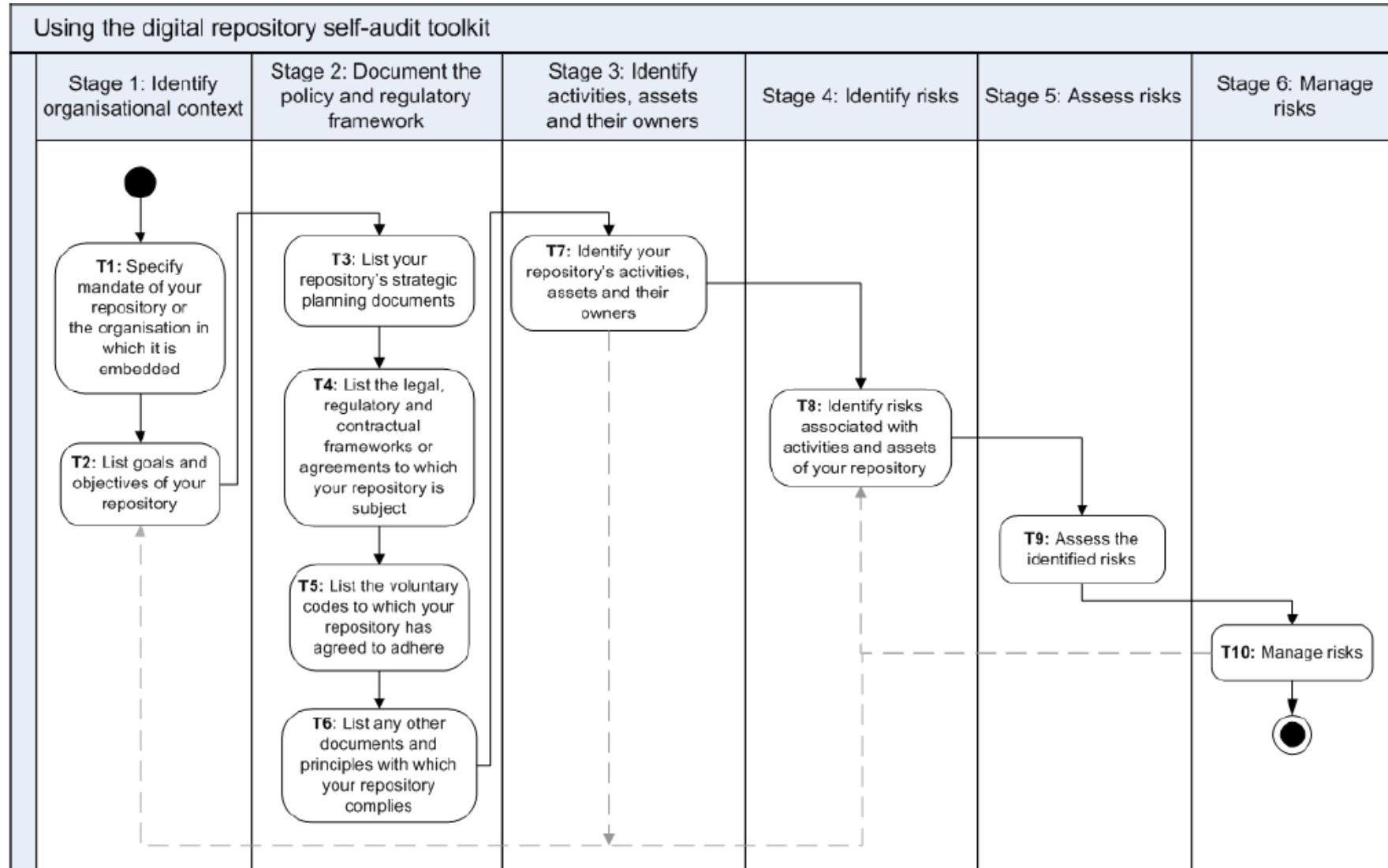
- defining the mandate and scope of functions
- identifying the activities and assets
- identifying the risks and vulnerabilities associated
- assessing and calculating the risks
- defining risk management measures
- reporting on the self-audit

A risk management approach

“Digital curation is about taking organisational, procedural, technological and other uncertainties and transforming them into **manageable risks**”

RISK = exposure to the consequences of uncertainty, or potential deviations from what is planned or expected

DRAMBORA workflow



DRAMBORA STAGE 1

Identify organisational context

STAGE 1 - Identify organisational context

Tasks:

1. Identify organisational mandate (T1)
2. Identify organisational goals and objectives (T2)

In order to:

- define the scope of the repository work
- verify awareness of the organisational framework
- ensuring that appropriate supporting documentation exists

STAGE 1 - Identify organisational context

1. Identify organisational mandate (T1)

“An organisation’s mandate is its legal basis or a formally expressed intention issued by an organisation or its parent to achieve a particular goal or goals”

STAGE 1 - Identify organisational context

2. Identify organisational goals and objectives (T2)

Associated with 8 **functional classes**:

- Acquisition & Ingest
- Preservation & Storage
- Metadata Management
- Access & Dissemination

operational classes

- Organisation & Management
- Staffing
- Financial Management
- Technical Infrastructure & Security

supporting classes

STAGE 1 - Identify organisational context

T2 Example:

*List goals and objectives of your repository
(Operational class: **Acquisition & Ingest**)*

- Preserve original files exactly as submitted, with demonstrated integrity, viability and authenticity
- Achieve and maintain certification as a Trusted Digital Repository

STAGE 1 - Identify organisational context

T2 Example:

*List goals and objectives of your repository
(Operational class: **Preservation & Storage**)*

- Preserve original files exactly as submitted, with demonstrated integrity, viability and authenticity
- Document all changes to archived content

DRAMBORA STAGE 2

Document policy and regulatory framework

STAGE 2 - Document policy and regulatory f.

Tasks:

3. List the strategic planning documents (T3)
4. List the Legal, regulatory, contractual frameworks (T4)
5. List the voluntary codes(T5)
6. List other documents (T6)

3. List the strategic planning documents (T3)

Includes:

- Policies
- Procedures

Identified within:

- procedural or operational manuals
- intranet or shared network storage
- Wikis

STAGE 2 - Document policy and regulatory f.

4. List the Legal, regulatory, contractual frameworks (T4)

Includes:

- 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

5. Voluntary codes (T5)

- Standards imposed upon or adopted by repository
- Standards forming the basis for other audits
- Formal compliance programmes
- Existing risk management programmes

6. Other documents (T6)

- e.g. Internal memorandums

DRAMBORA STAGE 3

Identify Activities, Assets and their Owners

STAGE 3 - Identify Activities, Assets and their Owners

Tasks:

7. Identify your repository's activities, assets and their owners (T7)

Building conceptual model of what the repository does:

- split broad level mission and goals into more specific activities or work processes
- assign activities to individual responsible actors
- link to one or more key assets of the repository

STAGE 3 - Identify Activities, Assets and their Owners

Organisational Assets

Includes:

- **Information**: databases, data files, contracts, agreements, documentation, policies and procedures
- **software assets**: application software, system software etc.
- **physical assets**: computer/communication equipment, removable media etc.
- **services and utilities**: computing and communication services, general utilities
- **processes**, eg. Application-specific activities
- **people and their qualifications**, skills and experience
- **intangibles**, such as reputation of the organisation

STAGE 3 - Identify Activities, Assets and their Owners

Owner

The term 'owner' identifies an individual or entity that has approved management responsibility for controlling the production, development, maintenance, use and security of the assets

STAGE 3 - Identify Activities, Assets and their Owners

T7 Example:

Identify Activities, Assets and their Owners (Staffing)

- **Activity:** Appoint a sufficient number of appropriately qualified staff
- **Assets:** Staff; training library
- **Owner:** Personnel/HR

- **Activity:** Define roles, responsibilities and their relationship
- **Assets:** Staff; organisational review documents
- **Owner:** Personnel/HR

DRAMBORA STAGE 4

Identifying Risks

STAGE 4 - Identifying Risks

Tasks:

8. Identify risks associated with activities and assets of your repository (T8)

To derive from organisational activities and assets a comprehensive selection of pertinent risks faced by the repository

- Auditors must build a structured list of risks, according to associated activities and assets
- Assign a risk owner
- No single methodology - brainstorming structured according to activities/assets is effective

STAGE 4 - Identifying 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 (modification, corruption, destruction, unavailability or loss)

STAGE 4 - Identifying Risks

Organisation Management

No.	Risk title
R01	Management failure
R02	Loss of trust
R03	Activity is overlooked or allocated insufficient resources
R04	Business objectives not met
....

Staffing

No.	Risk title
R21	Loss of key member(s) of staff
R22	Staff suffer skill loss
R23	Staff skills become obsolete
....

DRAMBORA STAGE 5

Assess Risks

STAGE 5 - Assess Risks

Tasks:

9. Identify risks associated with activities and assets of your repository (T9)

*To characterise the risks and risk relationships derived within the previous Stage, and to assess the **severity** of each*

STAGE 5 - Assess Risks

For each risk, auditors are required to provide the following:

- example **manifestations** of risk
- **probability** of its execution
- **potential impact** of its execution
- **relationships** with other risks
- risk escalation **owner**
- **severity** or risk (quantification of seriousness)

STAGE 5 - Assess Risks

Example manifestations of risk

- Loss of key member(s) of staff

Individuals with roles, responsibilities or aptitudes vital to the achievement of business objectives part company with the repository, rendering achievement of those objectives less straightforward

- Example manifestation

Repository head systems administrator, the sole individual with knowledge of the system's root password, leaves the organisation to work elsewhere

STAGE 5 - Assess Risks

Risk Probability

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

STAGE 5 - Assess Risks

Risk Impact Score	Interpretation
0	<i>Zero</i> impact, results in <u>zero loss</u> of digital object authenticity and understandability
1	<i>Negligible</i> impact, results in <u>isolated but fully recoverable loss</u> of digital object authenticity and Understandability
2	<i>Superficial</i> impact, results in <u>widespread but fully recoverable</u> loss of digital object authenticity and Understandability
3	<i>Medium</i> impact, results in <u>total but fully recoverable loss</u> of digital object authenticity and understandability
4	<i>High</i> impact, results in <u>isolated loss</u> , including unrecoverable loss of digital object authenticity and Understandability
5	<i>Considerable</i> impact, results in <u>widespread loss</u> , 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 <u>total and unrecoverable loss</u> of digital object authenticity and Understandability

STAGE 5 - Assess Risks

Risk Relationship

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

STAGE 5 - Assess Risks

Risk escalation owner

- Individuals with responsibility to deal with a particular risk
- In almost all cases this will be the same as the original activity and risk owner

STAGE 5 - Assess Risks

Severity or risk: quantification of seriousness

It is derived as the product of the chosen probability and potential impact values

Low probability (occurs once every 5 years)	▶	3	X
High impact (results in isolated loss)	▶	4	

Risk Severity	12
----------------------	-----------

DRAMBORA STAGE 6

Manage Risks

STAGE 6 - Manage Risks

Tasks:

9. Manage Risks (T10)

Risks must be managed appropriately. Once a risk has been assessed, a business decision must be made to determine how the risk is to be approached.

STAGE 6 - Manage Risks

Several strategies:

- **Avoid circumstances** in which risk arises
- **Limit the likelihood** of the risk, to reduce the probability of the negative outcomes
- **Reduce potential impact** of risk
- **Share the risk**, involving another party or parties
- **Retain the risk** and tolerate

STAGE 6 - Manage Risks

Auditors should:

- choose and describe **risk management strategy**
- assign **responsibility** for adopted measure
- define **performance** and **timescale** targets
- reassess success **recursively**

STAGE 6 - Manage Risks

Principal outcome

A **risk register** with risk management features included

The self-audit produces a composite risk score for the 8 functional classes which enables quantification of risks' severity:

- illustrates vulnerabilities
- facilitates resource investment

STAGE 5 - Assess Risks

Risk Identifier:	R24
Risk Name:	Inability to evaluate staff effectiveness or suitability
Mitigation strategy(ies):	<p>Avoidance strategies:</p> <ul style="list-style-type: none"> • Establish internal means of assessment including risk management • Seek relevant external certification in order to demonstrate staff competence • Undertake regular staff development reviews
Risk Relationships:	<p>→R01 [contagious] →R02 [contagious] →R19 [contagious]</p>
Risk Probability:	4
Risk Potential Impact:	3
Risk Severity:	12
Owner:	Management
Escalation Owner:	Management
Stakeholders:	Management; financiers; staff; depositors; users; producers

Closing Questions?

If you have any further questions please email us at
feedback@repositoryaudit.eu

Chiara Cirinnà
cirinna@rinascimento-digitale.it