User Guide

Martin Donnelly
Perla Innocenti
Andrew McHugh
Raivo Ruusalepp

Glasgow, 2009
# Table of contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>INTRODUCTION</td>
<td>4</td>
</tr>
<tr>
<td>ABOUT DRAMBORA</td>
<td>4</td>
</tr>
<tr>
<td>THE DRAMBORA WORKFLOW</td>
<td>5</td>
</tr>
<tr>
<td>DRAMBORA INTERACTIVE</td>
<td>6</td>
</tr>
<tr>
<td><strong>REGISTRATION</strong></td>
<td>7</td>
</tr>
<tr>
<td>REGISTRATION PROCESS</td>
<td>7</td>
</tr>
<tr>
<td>NOTE ON NAVIGATING THE SYSTEM</td>
<td>8</td>
</tr>
<tr>
<td><strong>A. BEFORE THE ASSESSMENT</strong></td>
<td>9</td>
</tr>
<tr>
<td>A1. EDIT REPOSITORY (DEFINING THE SCOPE OF YOUR AUDIT)</td>
<td>9</td>
</tr>
<tr>
<td>A2. DEFINE ASSESSMENT SCOPE</td>
<td>10</td>
</tr>
<tr>
<td>A3. DEFINE FUNCTIONAL CLASSES (DETERMINING THE STRUCTURE FOR THE AUDIT)</td>
<td>11</td>
</tr>
<tr>
<td>A4. ADD STAFF</td>
<td>12</td>
</tr>
<tr>
<td>A5. ADD ROLE, EDIT ROLE, ROLE ASSIGNMENT</td>
<td>13</td>
</tr>
<tr>
<td>NOTE ON USER ADMIN</td>
<td>14</td>
</tr>
<tr>
<td><strong>B. ASSESSMENT CENTRE</strong></td>
<td>16</td>
</tr>
<tr>
<td>B1. ADD MANDATE</td>
<td>17</td>
</tr>
<tr>
<td>B2. ADD CONSTRAINTS</td>
<td>18</td>
</tr>
<tr>
<td>B3. ADD OBJECTIVES</td>
<td>19</td>
</tr>
<tr>
<td>B4. ADD ACTIVITIES AND ASSETS</td>
<td>20</td>
</tr>
<tr>
<td>B5. ADD RISKS</td>
<td>21</td>
</tr>
<tr>
<td>B6. ASSESS RISKS</td>
<td>24</td>
</tr>
<tr>
<td>B7. MANAGE RISKS</td>
<td>25</td>
</tr>
<tr>
<td><strong>C. REPORT RESULTS</strong></td>
<td>26</td>
</tr>
<tr>
<td><strong>ADDITIONAL FEATURES</strong></td>
<td>28</td>
</tr>
<tr>
<td>APPENDIX 1: GLOSSARY</td>
<td>29</td>
</tr>
<tr>
<td>APPENDIX 2: QUICKSTART GUIDE</td>
<td>31</td>
</tr>
<tr>
<td>APPENDIX 3: SAMPLE DOCUMENTATION</td>
<td>33</td>
</tr>
</tbody>
</table>
Index of figures

FIGURE 1 - DRAMBORA WORKFLOW .................................................................................................................. 5
FIGURE 2 - DRAMBORA INTERACTIVE HOMEPAGE .............................................................................................. 6
FIGURE 3 - REPOSITORY REGISTRATION PAGE ....................................................................................................... 7
FIGURE 4 – EDIT REPOSITORY PAGE ..................................................................................................................... 9
FIGURE 5 – DEFINE ASSESSMENT SCOPE PAGE ...................................................................................................... 10
FIGURE 6 – DEFINE FUNCTIONAL CLASSES PAGE .................................................................................................. 11
FIGURE 7 – ADD STAFF PAGE ...................................................................................................................................... 12
FIGURE 8 – EDIT ROLE PAGE ...................................................................................................................................... 13
FIGURE 9 – ROLE ASSIGNMENT PAGE .................................................................................................................. 14
FIGURE 10 - USER ADMIN PAGE .......................................................................................................................... 15
FIGURE 11 - ORGANISATIONAL MANDATE PAGE .................................................................................................... 17
FIGURE 12 - ADD CONSTRAINTS PAGE ................................................................................................................... 18
FIGURE 13 - ADD OBJECTIVES PAGE ..................................................................................................................... 19
FIGURE 14 - ADD ACTIVITIES AND ASSETS PAGE ................................................................................................ 20
FIGURE 15 - ADD RISK PAGE: CREATING A NEW RISK FROM SCRATCH................................................................. 22
FIGURE 16 - ADD RISK PAGE: SELECTING AN OFF-THE-SHELF RISK ................................................................. 23
FIGURE 18 - MANAGE RISK PAGE ........................................................................................................................ 25
FIGURE 19 - REPORT BUILDER PAGE ..................................................................................................................... 27
FIGURE 20 - EXAMPLE OF SAVED SNAPSHOT ...................................................................................................... 28
INTRODUCTION

About DRAMBORA

Developed jointly by the Digital Curation Centre (DCC) and DigitalPreservationEurope (DPE), the Digital Repository Audit Method Based on Risk Assessment (DRAMBORA) represents the main intellectual outcome of a period of pilot repository audits undertaken by the DCC throughout 2006 and 2007.

It presents a methodology for self-assessment, encouraging organisations to establish a comprehensive self-awareness of their objectives, activities and assets before identifying, assessing and managing the risks implicit within their organisation.

Within DRAMBORA, digital curation is characterised as a risk-management activity; the job of a digital curator is to rationalise the uncertainties and threats that inhibit efforts to maintain digital object authenticity and understandability, transforming them into manageable risks.

Six stages are implicit within the process. Initial stages require auditors to develop an organisational profile, describing and documenting the repository's mandate, objectives, activities and assets. Latterly, risks are derived from each of these, and assessed in terms of their likelihood and potential impact. Finally, auditors are encouraged to conceive of appropriate risk management responses to the identified risk.

The process enables effective resource allocation, enabling repository administrators to identify and categorise the areas where shortcomings are most evident or have the greatest potential for disruption.

The process itself is an iterative one, and therefore subsequent recursions will evaluate the effectiveness of prior risk management implementations.

DRAMBORA Interactive is an on-line tool built to facilitate the assessment process and guide the auditor through the stages of the methodology.

DRAMBORA can be used at http://www.repositoryaudit.eu/.
The DRAMBORA Workflow

The DRAMBORA workflow is structured in 10 steps (Figure 1)

Figure 1 - DRAMBORA Workflow
Before beginning the assessment, you should conduct a preliminary analysis of the repository documentation, and arrange appointments with repository staff for onsite interviews and visits to the repository site.

After completing the assessment, you will have two distinct outputs:

1. a risk register of your repository, produced using the automatic DRAMBORA reporting system;
2. an audit report structured along the ten characteristics of digital preservation repositories as defined by the CRL/OLC/nestor/DCC/DPE meeting in January 2007. This report is produced using the documentation and information collected and analysed for the assessment.


**DRAMBORA Interactive**

Combining a methodology and an online interactive application, the DRAMBORA toolkit, enables organisations to assess and monitor how well they are preserving and curating their digital assets. By following a step by step approach, this document shows how to use DRAMBORA Interactive (Figure 2).²

As you work your way through this guide, you will learn how to manage the necessary documentation for repository assessment, and how to build a risk profile of the assessed repository.

² DRAMBORA Interactive: [http://www.repositoryaudit.eu/](http://www.repositoryaudit.eu/)
REGISTRATION

In order to use DRAMBORA Interactive, you need to register for the DRAMBORA Interactive online tool and complete a series of audit responses to correspond with a sample repository.

Registration process

1. Visit http://www.repositoryaudit.eu and click Register for DRAMBORA in the top-left of the screen (Fig.3). Enter the name of your repository, and fill in the subsequent fields which describe it.

![Repository registration page](image)

Figure 3 - Repository registration page

2. If you are already logged in to the system, you can simply link the new repository to your own user name. Alternatively, you can create a new DRAMBORA Interactive user. Enter your details in the corresponding fields. If necessary, further users can be associated with the repository later in the process. During registration it is essential that you provide an email address. Following registration you will receive an email, which you must respond to in order to validate your user, and to log in.

3. Finally you must create corresponding staff details for this user. You can enter the name of any position.

4. Now check your email and click on the enclosed link in order to log into the DRAMBORA system.

---

For security purposes, you can limit the IP addresses that users may log in from. This supports wildcards: for example, **.*.*.* permits access from any IP, while 130.209.*.* permits access only from the 130.209.x.x network. It is recommended that you restrict access to only your own IP or local network range.
Note on Navigating the System

The DRAMBORA Interactive tool has three main sections:

A. Before the Assessment
B. Assessment Centre
C. Report Results

Although it is recommended that you follow a linear path through the audit process, you can save your progress as a snapshot if you choose to move between sections.

You'll notice that the boxes in the right-hand column have plus-signs next to them. Clicking these allows the boxes to be expanded, thereby increasing the amount of information available on the screen at any time. Expanding the sections also allows you to edit inline. If you find your screen becoming cluttered with the amount of information on it, you can collapse these sections by clicking on the minus-signs.

Tip: DRAMBORA Interactive also has a Save Snapshot function, which enables you to compare your repository at different stages in its development. More on this feature later…
A. BEFORE THE ASSESSMENT

First click on the left hand menu link Before the Assessment in order to submit some details about your repository. The most important initial steps before the assessment of your repository are to:

A1. Refine the repository characteristics
A2. Make explicit the audit scope and purpose
A3. Determine the structure for the audit managing the functional classes
A4. Define staff
A5. Allocate roles accordingly
A6. User administration

These details can be updated at any time, but it is worth spending some effort before your assessment in order to get a reasonably full set of responses. Let's see the steps in details:

A1. Edit Repository (defining the scope of your audit)

If you have any changes to make to the repository characteristics you can click on the Edit Repository link to do so (Fig. 4). Otherwise, click on the link to Define Assessment Scope.

Figure 4 – Edit Repository page
A2. Define Assessment Scope

The assessment should firstly be defined in terms of its chronological relationship with the repository. Is the assessment taking place before the repository is active, or does it take a retrospective look at efforts already underway?

Read the text and select the type of audit you want to undertake (e.g. validatory) and describe the extent of the assessment planned for the repository (Fig. 5). Try to be explicit about which individual organisational units are being assessed, and which are beyond the scope of this analysis.

Tip: Click on the link at the foot of this screen to view some sample documentation types that may usefully contribute to your audit. The list is also included in this document at Appendix 3.
A3. Define Functional Classes (determining the structure for the audit)

Functional classes are a means of categorising audit information to facilitate the process and make reports more meaningful. In this section you will select how you are going to structure your audit responses and outcomes.

You must select at least one functional class at this stage, and it is recommended that you spend some time here to ensure your choice is comprehensive. If you feel that the predefined functional classes are insufficient you can define your own additional ones, although a default set of ten is provided (and recommended).

Click Manage Functional Classes to see the available descriptors (Fig. 6); the ten default classes correspond with the ten principles of digital repositories on which DRAMBORA is structured. Click select all to choose these ten, and then click the Save button.

Tip: You may wish to structure the definition process according to your own bespoke Functional Classes, or use a subset or superset of the ten default exemplars. This can all be configured via the Define Functional Classes screen. While any part of the DRAMBORA process can be returned to at a later time, as a fundamental aspect of the repository it is suggested that the set of Functional Classes should not be altered once it has been defined.
A4. Add Staff

Next, click on the link to Add Staff (Fig. 7). Enter details for each member of repository staff. Staff are the real people that occupy the various roles in your repository. You can choose to create new (or associate existing) DRAMBORA Interactive users to link with each staff member. This is not absolutely necessary, but it permits these staff members to provide hands-on contributions to the audit process. Each member of staff will need his or her own user accounts to log into the DRAMBORA tool.

Staff members can be defined as either coordinators or contributors. In common with other repository administration activities, only coordinator users can create and edit staff members.

Figure 7 - Add Staff page
A5. Add Role, Edit Role, Role Assignment

Roles have a special meaning within DRAMBORA, and are distinct from job titles. Roles describe broad functions with associated responsibilities; many staff members can therefore occupy a single role.

In DRAMBORA, roles are characterised by their function (e.g. Ingest, Dissemination, Financial Management, Preservation Planning). Their relationship to staff members is 1 to n. Therefore, many staff members can perform single roles. Roles are used to associate activities, risks and risk management responsibilities with specific individuals or sets of individuals.

Click Add Role and enter the key roles that will exist within the repository (Figs. 8 and 9). If these are not clear-cut then you may choose to use the main functions provided within OAIS as a guide (e.g. Ingest, Data Management, Archival Storage, Preservation Planning, Administration, and Access). Roles allow the auditor to assign particular challenges and risks to specific individuals or groups of individuals.

Finally in this section, you can assign roles to individual staff members by following the Role Assignment link. Once this is done, click Assessment Centre in the left-hand navigation column to begin the audit.

Figure 8 – Edit Role page
Note on User Admin

In DRAMBORA Interactive, logged-in users can update their own details at any time via the User Admin screen (Fig. 10).

For security purposes, it is possible to limit the IP addresses that users may log in from; 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 your own IP address, or to your local network range.
Figure 10 - User Admin page
B. ASSESSMENT CENTRE

The Assessment Centre is the pivotal stage of the audit. The constituent steps in this process are:

B1 Add Mandate
B2 Add Constraints
B3 Add Objectives
B4 Add Activities and Assets
B5 Add Risks
B6 Assess Risks
B7 Manage Risks

Tip: Asterisked fields are mandatory within the Assessment Centre. Remember that DRAMBORA Interactive is a recursive process, so stages can be returned to at any time.
**B1. Add Mandate**

The first requirement is to define the mandate of the audited repository.

The mandate describes the repository's mission, or reason for existence. This is the general statement that legitimises the repository, and broadly describes its objectives. Because repositories are unlikely to exist in a vacuum, multiple mandates can be described, corresponding to different hierarchical levels within which the repository exists (e.g., you may have separate (but hopefully compatible) mandates associated with repository, departmental, and organisational levels).

Click **Add Mandate** and enter the details, then describe the scope to which this particular mandate applies (Fig. 11). If you need to add additional mandates (e.g., to represent an organisational hierarchy) then this can be done by reselecting the **Add Mandate** link. The mandates you have entered can be viewed by expanding the **defined mandates** box at the right of the screen. You can edit or delete these sections 'inline' using this view.

---

**Figure 11 - Organisational mandate page**
**B2. Add Constraints**

Repository constraints take many forms, and can be succinctly described as any factor that compels or influences the repository to operate in a particular fashion. These can originate externally (e.g. legislation prohibiting release of particularly materials) or internally (e.g. policies describing particular protocols for information ingest).

Define any constraints which your repository is subject to or influenced by clicking **Add Constraints** (Fig. 12). This should include any relevant factor that influences or informs the repository’s objectives or activities (e.g. policies, laws, technical constraints, or even less tangible cultural considerations such as lack of financial confidence). Try to come up with a variety of constraints that correspond to the categories available. You can upload files or include web links that describe individual constraints in more detail. External files can be linked to offer further information.

![Figure 12 - Add Constraints page](image-url)
B3. Add Objectives

Objectives are measurable strategic aims of the repository, and can correspond with any of its business areas. These are the outcomes that the repository pursues, and can be contrasted with the specific strategies employed to facilitate their achievement (called activities within DRAMBORA). Adding a quantitative dimension to each objective will facilitate its measurement and the subsequent identification of risks.

Define each of your repository’s objectives by clicking Add Objectives (Fig. 13). You should aim to come up with a number of objectives corresponding to a variety of functional classes. You can associate these with constraints defined in the previous stage. Ideally, your objectives will have a degree of measurability.4

---

B4. Add Activities and Assets

Activities are the practical and tangible things that the repository does in order to achieve its objectives. These may be associated with assets that are either required to enable their completion or are generated as an outcome, but this is not obligatory. Each activity must be associated with one or more roles to indicate where responsibility for its completion resides.

In this stage you will create a selection of corresponding specific repository activities that are undertaken within your organisation in order to meet individual objectives (Fig. 14). You can also add details of required or related assets for each activity to take place, and an owner (a role) that has responsibility for each activity. Please note that assets are anything that is required to facilitate the achievement of particular objectives, tangible or otherwise (i.e. the repository’s reputation, specific competencies of your staff, etc.).
B5. Add Risks
Risks describe challenges or threats that impede the achievement of repository objectives, obstruct activities and prejudice the continued availability of essential assets. The risk identification stage is the most important in DRAMBORA Interactive.

Clicking Add Risks offers a choice of three ways to attach risks to your repository:

- Creating a new risk from scratch (Fig. 15)
- Modifying another risk already attached to your repository
- Adapting an off-the-shelf risk (Fig. 16)

Tip: To avoid duplicating effort unnecessarily, it is recommended that you inspect the list of pre-defined lists before creating new risks from scratch.

Each risk must be given a name. You can also describe:

- Vulnerabilities,
- Consequences
- Avoidance strategies
- Treatment strategies
- Causal relationships it may have with other risks
- Notes on the nature of the risk itself.
Figure 15 - Add Risk page: creating a new risk from scratch
Tip: When modifying a pre-defined risk, select the “Store Original Management Measures” tick-box to carry the vulnerabilities and risk consequences across from the template. These can then be edited as you require.
B.6 Assess Risks

Once you have identified all of your repository’s risks, the next step is to undertake a risk assessment in order to determine their severity. Risk assessment can be done on a selection of risks at a time, either by functional class, or a custom grouping defined by the user.

This measurement represents a combination of the risk’s frequency and its potential impact. Weightings should be applied to each to describe their proportionate scale. Impact can be manifested in numerous ways, so in order to ensure the comparability of results, you should select a risk impact expression descriptor from the drop-down list, and weight your responses accordingly.
B.7 Manage Risks

The final stage of the audit is to define an appropriate set of risk management measures, and to set targets that might limit the likelihood and the impact of their occurrence.

Click Manage Risk (Fig. 18), and for each risk you should record details of treatment or avoidance measures, anticipated outcomes, and set a date at which the risk should be reassessed.

Figure 18 - Manage Risk page

This concludes the Risk Assessment element of DRAMBORA Interactive. The next (and final) stage is to produce the Risk Register report.
C. REPORT RESULTS

Your risk register should now be complete, and you will probably wish to see the results of your work!

There are a number of ways to format and export your report. Click Report Results on the left hand side of the screen (Fig. 18), and select one of the following options:

- Export as PDF
- View Assessment Data in Browser
- Advanced Report Builder

Choosing Export as PDF offers a further three options:

- Generate Risk Register PDF (all current risks, page per risk)
- Generate Risk Register PDF (all current risks, landscape tabular)
- Advanced Risk Register Builder

Choosing View Assessment Data in Browser offers two options:

- Generate Risk Register (all current risks, new window)
- Advanced Risk Register Builder

The Advanced Report Builder option allows you to customise your report in several ways. You can choose to display only those risks that are linked to a subset of the functional classes, or selecting individual risks to display. There are also options to order risks alphabetically by name, by owner, by severity, or by date of identification.

Finally, the Advanced Report Builder allows you to output your Risk Report as a Web page.
Figure 19 - Report Builder page
SECTION 6: ADDITIONAL FEATURES

ADDITIONAL FEATURES

The **Save Snapshot** feature lets you record the state of the repository at a particular time. This enables comparison at a later date, and 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, which can be a useful reporting tool in itself.

You can save a snapshot of the assessment status at any time. To do so, use the **Saved Snapshot** panel and click on **New Snapshot** at the foot of the right hand side of the screen (Fig 20). You can then view and navigate the responses corresponding to this particular time, and analyse the interrelationships between the accumulated information.

![Figure 20 - Example of Saved Snapshot](image-url)
APPENDICES

APPENDIX 1: GLOSSARY

Asset
Anything that has value to the organisation (ISO/IEC 13335-1:2004).

Digital repository
An organisation (or organisational unit) that has responsibility for the long-term maintenance of authentic and understandable digital resources. A digital repository is expected to adhere to the following ten criteria:  

i) Commits to continuing maintenance of digital objects for its identified community (or communities).

ii) Demonstrates organisational fitness (including financial, staffing, structure, processes) to fulfil its commitment.

iii) Acquires and maintains requisite contractual and legal rights and fulfils responsibilities.

iv) Has effective and efficient policy framework.

v) Acquires and ingests digital objects based upon stated criteria that correspond to its commitments and capabilities.

vi) Maintains/ensures the integrity, authenticity and usability of digital objects it holds over time.

vii) 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.

viii) Fulfils requisite dissemination requirements.

ix) Has strategic programme for preservation planning and action.

x) Has technical infrastructure adequate for continuing maintenance and security of digital objects.

DRAMBORA Interactive does not pre-suppose any specific type of digital resources or the repository having any particular type of organisational structure: the risk-based self-assessment will be undertaken within the confines of the mandate of the repository, whether it be an archive, digital library, data archive, or e-Science collection.

Likelihood
Used as a general description of probability or frequency. (AS/NZS 4360:2004)

Mandate
Legal basis or a formally expressed intention issued by an organisation or its parent to achieve a particular goal (or goals).

Objectives
General and continuing, and specific, time bound statements of intended future results. Organisation’s objectives often identify broad functional areas and descriptions of major programmes and their budgets. Objectives are usually revised every three to five years.

---

Owner
An individual or entity that has approved management responsibility for controlling the production, development, maintenance, use and security of the repository’s assets. (ISO 27001:2005)

Risk
Risk refers to uncertainty that surrounds future events and outcomes. It is the expression of the likelihood and impact of an event with the potential to influence the achievement of an organisation’s objectives.

Risk assessment
Systematic process of estimating the magnitude of risks as a combination of likelihood and impact scores.

Risk avoidance
A decision not to become involved in, or to withdraw from, a risk situation. (ISO/IEC Guide 73:2002)

Risk communication
Exchange or sharing of information about risk between the decision-maker and other stakeholders. (ISO/IEC Guide 73:2002)

Risk identification
Process of identifying risks considering business objectives, activities and assets, and their threats and vulnerabilities as the basis for further analysis.

Risk management
Coordinated activities to direct and control an organisation with regard to risk. (ISO/IEC Guide 73:2002)

Vulnerability
Weakness of an asset or group of assets that can be exploited by one or more threats. (ISO/IEC 13335-1)
APPENDIX 2: QUICKSTART GUIDE

1. When logged in a box in the top right of the screen displays the name of your registered 'active' repository. Your currently active repository will always be displayed in this section of the screen. You may register as a staff member at as many repositories as you wish, but if doing so you should ensure that the correct repository is currently active.

2. The first thing you should do after registering a new repository is to visit the Assessment Preparation centre, in order to add some important details about your repository. From this part of DRAMBORA interactive you should complete the following simple stages:
   a. Make any further edits you wish to your repository profile
   b. Add/edit details of all of the staff members that you have within your repository
   c. Add/edit details the roles that exist within your repository (N.B. this is vital, since DRAMBORA Interactive relies on role information to associate risks and responsibilities with particular owners.)
   d. Associate staff members with specific roles

3. After finalising some details about your repository you are ready to begin the assessment. To do so, you should visit the Assessment Centre index page. This is the starting point for the assessment.
   a. Functional Classes: The first item to decide upon is the set of functional classes, or information categories, that you will use to structure your responses and reporting capabilities within the assessment process. This choice is particularly important, because it will determine the flexibility that you will subsequently have within the assessment
   b. Mandate: The mandate section allows you to express the reason for the repository's existence, its formal expression of legitimacy and purpose. Multiple mandates can correspond to a single repository, relating to the missions and mandates of different levels of the organisational hierarchy within which the repository finds itself
   c. Constraints: Constraints are limits that restrict or influence the objectives and activities of the repository. These can relate to strategic plans, legislation or regulations, technical requirements or policy. These must be documented to relate to objectives and ultimately to risks
   d. Objectives: Objectives are the strategic aims of the repository, structured according to the functional classes decided upon earlier. These should be expressed in suitably specific terms, ideally with an associated quantitative target to facilitate understanding of their achievement
   e. Activities and Assets: These are the practical actions and resources that the repository has in place to meet the objectives stated above.
   f. Identify Risks: At this stage assessors should detail each of the risks that relates to the organisation. Assessors can 'recycle' pre-existing risks, making necessary changes to suit their own specific context
   g. Assess Risks: Assessors should determine the probability and potential impact of each identified risk, in order to determine the most severe risks in need of the most urgent attention
SECTION 7: APPENDICES

h. Manage Risks: At this stage, the final point of the self assessment process, you should devise appropriate risk management techniques in order to alleviate the vulnerabilities that your repository is exposed to.

4. Once the assessment stages are finalised you may view the various reporting options. Through the Report Centre you may export the results of the assessment to the web or to a PDF document. You may export all the identified risks or a structured and ordered subset.
APPENDIX 3: SAMPLE DOCUMENTATION

Numerous different kinds of documentation may come in useful during the audit process. The following list provides some idea of potentially relevant documentation that organisations undertaking self assessment with DRAMBORA may aggregate to support the process. Needless to say, this list is neither exhaustive nor in its entirety compulsory. Some documents may be more or less relevant depending on the organisation. The technological characteristics of the repository are just one of various considerations that also include its organisational, procedural and contextual attributes.

- Examples of strategic planning documents (e.g., business plans, departmental development plans);
- Annual reports;
- Examples of documents and/or legislation that define the repository's mandate;
- Relevant legislation
- Examples of deposit agreements/contracts that you might have available;
- Example job descriptions;
- A recent organisational chart, including details of training commitments;
- Example staff profiles or résumés;
- Copies of financial reports or business plans;
- A copy of the repository's risk register, disaster plan or exit strategy;
- Documents detailing policy in key areas such as designated community definition and associated service levels; preservation strategies; guidelines for selection and ingest; access; and disaster recovery;
- System documentation/procedural manuals and system work flows;
- Documents describing the technical architecture in place;
- Results of any other relevant audits, organisational assessments or self-assessments;
- Documentation describing the institutional spacing within which the repository fits, including details of its mandate, funding cycle and the commitment of or dependency upon its parent organisation.

A specific list of policies that ought to be documented within a trustworthy digital repository is provided in Appendix 3 of the Trustworthy Repositories Audit and Certification Criteria and Checklist Document (TRAC). The number adjacent to each indicates the corresponding metric within this check-list. Each of these, where available, would be of considerable interest during the assessment. It's been our experience that one of the useful things about this process is identifying where gaps exist in documentation, and it's therefore worthwhile to note down not only the documents that you do have available.

- A1.2 Contingency plans, succession plans, escrow arrangements (as appropriate);
- A3.1 Definition of designated community(ies), and policy relating to service levels;
- A3.3 Policies relating to legal permissions;
- A3.5 Policies and procedures relating to feedback;
- A4.3 Financial procedures;
- A5.5 Policies/procedures relating to challenges to rights (only if likely to be needed);
- B1 Procedures related to ingest;
- B2.10 Process for testing understandability;
- B4.1 Preservation strategies;
- B4.2 Storage/migration strategies;
B6.2 Policy for recording access actions;
B6.4 Policy for access;
C1.7 Processes for media change;
C1.8 Change management process;
C1.9 Critical change test process;
C1.10 Security update process;
C2.1 Process to monitor required changes to hardware;
C2.2 Process to monitor required changes to software;
C3.4 Disaster plans.