Digital Repository Audit Method

Based on Risk Assessment

DRAMBORA

Digital Curation Centre (DCC)

&

DigitalPreservationEurope (DPE)

Draft for Public Testing & Comment

Release: Version 1.0 (draft)

Date: 28 February 2007

Legal Notices

Catalogue Entry

Title	Digital Repository Audit Method Based on Risk Assessment
Creator	Digital Curation Centre (DCC)
Creator	DigitalPreservationEurope (DPE)
Subject	Information Technology; Science; Technology–Philosophy; Computer Science; Digital Preservation; Digital Records; Science and the Humanities
Description	DCC/DPE *Digital Repository Audit Method Based on Risk Assessment* (DRAMBORA) provides a methodological framework, guidelines and audit tools to support the identification, assessment and managing of risks in a digital repository.
Publisher	Digital Curation Centre (DCC) and DigitalPreservationEurope (DPE)
Contributor	Andrew McHugh
Contributor	Raivo Ruusalepp
Contributor	Seamus Ross
Contributor	Hans Hofman
Date	28.02.2007 (creation)
Type	Text
Format	Adobe Portable Document Format v. 1.3
Language	English
Rights	© Digital Curation Centre Partners and DigitalPreservationEurope Partners

Citation Guidelines

Digital Curation Centre and DigitalPreservationEurope, (February 2007), "*DCC and DPE Digital Repository Audit Method Based on Risk Assessment*, v1.0.", retrieved 28.02.2007, from http://www.repositoryaudit.eu/download

Document Release Control

Version	Date	Change Made (and if appropriate reason for change)	Initials of Commentator(s) or Author(s)
1.0	28/02/07	Initial Release Version of *Digital Repository Audit Method Based on Risk Assessment*	AM, RR, SR, HH

Authors and Author Affiliation Details

Author Initials	Name of Author	Institution
AM	Andrew McHugh	Digital Curation Centre (DCC) and HATII, University of Glasgow
RR	Raivo Ruusalepp	National Archives of Netherlands, DigitalPreservationEurope (DPE), and Estonian Business Archives
SR	Seamus Ross	Digital Curation Centre (DCC), DigitalPreservationEurope (DPE), and HATII, University of Glasgow
HH	Hans Hofman	National Archives of Netherlands and DigitalPreservationEurope (DPE)

1 EXECUTIVE SUMMARY

This is the first iteration of the DCC/DPE *Digital Repository Audit Method Based on Risk Assessment* (DRAMBORA) and will be followed by revised versions during 2007 and 2008 following each of the formal testing phases of the toolkit and public comment on it. The construction of this toolkit is a dynamic process and this is the second stage in this process. The DRAMBORA toolkit represents the latest development in an ongoing international effort to conceive criteria, means and methodologies for audit and certification of digital repositories. The intention throughout its development has been to build upon, extend and complement existing efforts. A key requirement has been to establish a toolkit that contributes towards a single process for repository assessment. The importance of international cooperation and collaboration, and the potential dangers associated with divergence were acknowledged very early on within the DCC and DPE's work in this area.

Perhaps the most notable efforts to date within this context are those invested within the RLG/NARA Task Force and the nestor working group to develop criteria for audit and certification of trustworthy digital repositories. Further significant work was led by the Center for Research Libraries (CRL). The results of these efforts have been foremost within our considerations throughout the development of this toolkit, and in the DCC-led pilot audits that preceded it. The DCC/DPE working group has engaged with representatives of other groups to agree upon a set of principles, representing the fundamental, objective baseline criteria for preservation repositories and these, and their underlying concepts, are profoundly important within the toolkit. It is anticipated that self-audit based on DRAMBORA can be facilitated if undertaken in association with one or both of the check-lists, and vice versa. The risk-based approach assists efforts to match a repository against these lists of requirements. Only with a clear view of an organisation's business context and its implicit risks can an auditor effectively utilise these requirements. The toolkit contextualises these lists so they can be more effectively applied. In addition to these resources, we have also sought to incorporate and adapt ideas and concepts from an additional, diverse range of sources, including a wide range of international information standards, many with their basis in the risk management industry aiming to broaden ever further the perspectives that our international colleagues have already established.

2 TABLE OF CONTENTS

Foreword

The term "digital repository" has a broad range of uses. Some use it for any collections of digital material. Many use it to refer to digital collections (often of ePrints) where the metadata is shared with a particular protocol. A few apply it only to collections of digital material that are intended to survive in an understandable way for very long periods into the future. It is specifically to this last definition that the Open Archival Information System (OAIS) standard applies.

An OAIS is "an archive, consisting of people and systems, that has accepted responsibility to preserve information and make it available to a Designated Community ... [meeting] responsibilities defined in [the OAIS standard]"[1] Work has continued over the past several years to define attributes of such Trusted (or Trustworthy) Digital Repositories, and the criteria that might be used to audit them. Note that trustworthy here is used in a specialist sense.

However, most current digital repositories, and most databases and collections used to help curate scientific data, do not have specific mandates for long term preservation, nor do they have the necessary long-term budgets. Instead, they are mandated to support access and re-use in the near-term future. Long term preservation may be one of their aims, or at least hopes and wishes, but it is not (yet) a responsibility. Much of the work on attributes and criteria referred to above is not oriented to this large group of repositories, although parts of it may prove helpful.

This toolkit aims to complement other repository audit and certification work by addressing the full range of repositories, whether they aim for long term preservation or not. It may where necessary be augmented by other tools and processes in the specific cases of digital repositories where long term preservation is a fully mandated responsibility.

Chris Rusbridge
Director of the Digital Curation Centre
28 February 2007

[1] ISO 14721:2003 Space data and information transfer systems -- Open archival information system -- Reference model, shttp://public.ccsds.org/publications/archive/650x0b1.pdf, (1.1 Purpose and Scope1-1)

3 INTRODUCTION

This document introduces the Digital Curation Centre (DCC) and DigitalPreservationEurope (DPE) audit toolkit for digital repositories. It is intended to facilitate internal audit by providing repository administrators with a means to assess their capabilities, identify their weaknesses, and recognise their strengths. Digital repositories are still in their infancy and this model is designed to be responsive to the rapidly developing landscape. The development of the toolkit follows a concentrated period of repository pilot audits undertaken by the DCC, conducted at a diverse range of organisations including national libraries, scientific data centres and cultural and heritage data archives. The ability of the DCC and DPE to collaborate on the development of this toolkit owes much to the generosity of these institutions who allowed the DCC to conduct these pilot audits (see Acknowledgements in Appendix 1). These have been enormously beneficial, informing the understanding of issues of organisational compliance, evidence and what it means in practical terms for a repository to be trusted and trustworthy. These test audits have also provided valuable insight into the factors that have already motivated members of our community to seek a formal means of assessment.

Within this toolkit the authentic and understandable digital object is positioned at the centre of a risk-based approach to audit; digital curation is 'characterised as a process of transforming controllable and uncontrollable uncertainties into a framework of manageable risks', classified according to a repository's activities, assets and regulatory context. To this end, this methodology seeks to determine whether the repository has made every effort to avoid and contain the risks that might impede its ability to receive, curate and provide access to authentic, and contextually, syntactically and semantically understandable digital information. The audit tool will encourage repository staff to identify and classify the risks posed at every stage of their activities, to assess the probability of their occurring, to appreciate their potential impact if they should arise, and to consider how well they are being dealt with. In this framework evidence is afforded considerable significance; repositories are expected not only to identify risks and manage them appropriately, but also to demonstrate their ability to do so, even if only internally.

We anticipate that this toolkit will be used primarily by repository administrators seeking both assurances of the adequacy of their current efforts and a structured indication of where resources could be most effectively deployed in order to enhance their capabilities. Repository funders, depositors, and users will increasingly expect that repositories can demonstrate that they are effectively and efficiently managing the risks associated with the process of curating digital materials. The DRAMBORA toolkit provides a mechanism for meeting this expectation.

Eschewing a strict benchmarking approach the toolkit seeks to facilitate a self-assessment exercise based largely on the specific and subjective goals of the organisation undertaking the process. Throughout a series of interactive stages, auditors are expected to develop a comprehensive image of their organisational objectives, the regulatory context within which they operate and the activities that must consequently be undertaken. From this starting point auditors are expected to derive a catalogue of pertinent risks; for each

risk that is identified a number of risk attributes are defined, including its owner, probability and potential impact scores, and proposed or implemented measures for avoidance, mitigation and treatment. The resulting risk register is a fundamentally useful tool, enabling organisations to identify their highest-priority business concerns and effectively allocate resources to resolve them, as well as ensuring the completeness of coverage of their activities with respect to overall goals. The process prepares organisations to meet the requirements of subsequent assessment; the tasks themselves are broadly equivalent to the preparatory work that would be required prior to an externally led audit, and the outcomes of such internally run audits can provide invaluable evidence for external auditors.

In order to facilitate the process of risk derivation and identification, subdivisions are introduced between individual classes of repository functions. The first group includes the mainly workflow oriented functions of the repository, associated with its primary functions of receiving, keeping, documenting and disseminating authentic usable objects. These are identified as baseline or prerequisite functions for all repositories, archives or infrastructures that will use this audit toolkit. Additional, supporting functional classes are also defined, associated with organisation management, staffing, finances and technical infrastructure and security.

Risks faced by organisations can be about things happening or not happening. This might be categorised in terms of threats whereby the risk (and associated negative impact) is of occurrence; and of opportunities, where the risk is associated with non-occurrence. The toolkit describes such circumstances as risk execution. Internal risks are characterised by their placing, and are both posed and manageable at the level of enterprise, archive, collection or item and are subject to further subdivision. External risks are those that originate from beyond these controllable parameters and, although they can be mitigated to some extent, they are generally surrounded by increased degrees of uncertainty, a consequence of the lesser extent to which they can be controlled. Recognition of the placing of risks as intrinsic or extrinsic to the repository can inform the mechanisms for risk management, whether manifest in strategies to avoid, mitigate or treat risks.

The document has seven core components:

- PART I introduces the concepts of repositories, the thinking that underlies a risk-based approach to audit, and the previous work that has informed the development of this toolkit.
- PART II lays out the audit process and describes the six stages of audit.
- PART III describes how we see the toolkit being further refined and how we hope the community will be engaged in the process of developing it.
- Appendix 1, the acknowledgement section, is a core component because of the tremendous significance that community involvement played in helping the team that produced this toolkit to understand how different types of digital repositories work in diverse environments and the processes involved in successfully running them.

- Appendix 2 incorporates a suite of templates to support the process of conducting the self-audit.
- Appendix 3 is intended to provide auditors with a mechanism to kick-start their thinking on risk. Initially it was not intended to include an example risk register table because several of those developing the toolkit felt that to do so would reduce the self-reflection that is essential in the self-audit process as it could lead repositories merely to derive their risk assessments from the examples provided in the toolkit. The result of this could be a failure on the part of the repository to internalise the risks they face and a failure to think about the special types of risks or unique characteristics of risks within particular organisational contexts. After reflection we decided both to include example risks and to provide an online tool to enable users of the toolkit to add example risks to the toolkit's risk register and to suggest amendments to the risk register provided in the toolkit. Our experiences working with the repository community has led us to the conclusions that developing a robust and informative risk register is best done by the repository community as a whole.
- Appendix 4 provides an example of how an audit report might usefully be structured.

The DRAMBORA toolkit, itself consists of, PART II, Appendix 2, and Appendix 4.

In addition to releasing this document we are releasing on 30th of March 2007 an online tool to assist institutions in completing audits using the *DCC/DPE Digital Repository Audit Method Based on Risk Assessment*.

3.1 COLLABORATION ON TOOLKIT DEVELOPMENT

This toolkit was developed as a collaboration between the Joint Information Systems Committee and Core eScience funded Digital Curation Centre (DCC) in the United Kingdom and the European Commission co-funded initiative DigitalPreservationEurope (DPE). These two initiatives will continue to work together to test and refine the toolkit, to manage the online tool, which is available at http://www.repositoryaudit.eu, and to foster its widest possible take-up within the United Kingdom, Europe and broader international contexts.

3.1.1 About the Digital Curation Centre

The JISC-funded Digital Curation Centre (DCC)[2] provides a focus on research into digital curation expertise and best practice for the storage, management and preservation of digital information to enable its use and re-use over time.[3] The project represents a collaboration between the

[2] http://www.dcc.ac.uk

[3] C Rusbridge, P Burnhill, S Ross, P Buneman, D Giaretta, L Lyon, M Atkinson, 2005, 'The Digital Curation Centre: A Vision for Digital Curation', In *Proceedings IEEE's Mass Storage and Systems Technology Committee Conference on From Local to Global: Data Interoperability--Challenges*

University of Edinburgh, the University of Glasgow through HATII, UKOLN at the University of Bath, and the Council of the Central Laboratory of the Research Councils (CCLRC). The DCC relies heavily on active participation and feedback from all stakeholder communities. The DCC is not itself a data repository. Rather, based on insight from a vibrant research programme that addresses wider issues of data curation and long-term preservation, it has developed and offers programmes of outreach and practical services to assist those who face digital curation challenges. It also seeks to complement and contribute towards the efforts of related organisations, rather than duplicate services.

3.1.2 About DigitalPreservationEurope

DigitalPreservationEurope (DPE)[4] is a three-year project (2006-2009), co-funded by the European Commission (IST-2006-034762), and comprising nine partner organisations from eight European countries. It fosters collaboration and synergies between existing national initiatives across the European Research Area. DPE addresses the need to improve coordination, cooperation and consistency in current activities to secure effective preservation of digital materials. DPE's project partners lead work to:

- raise the profile of digital preservation;
- promote the ability of European Union Member States acting together to add value to digital preservation activities across Europe;
- use cross-sectoral cooperation to avoid redundancy and duplication of effort;
- ensure auditable and certificated standards for digital preservation processes are selected and introduced;
- facilitate skills development through training packages;
- enable relevant research coordination and exchange;
- develop and promote a research agenda roadmap;
- help both citizens and specialist professionals recognise the central role that digital preservation plays in their lives and work.

DPE's success will help to secure a shared knowledge base of the processes, synergy of activity, systems and techniques needed for the long-term management of digital material. Developing mechanisms to support collaboration between repositories and audit to enable repositories to ensure that they are performing to the highest possible standards are two of the core areas in which DPE operates. DPE builds on the success of ERPANET, a key preservation initiative supported by the European Commission under the Fifth Framework Programme.[5]

and Technologies, an online version is at:
http://eprints.erpanet.org/archive/00000082/01/DCC_Vision.pdf

[4] http://www.digitalpreservationeurope.eu

[5] http://www.erpanet.org

4 PART I, BACKGROUND TO AUDIT METHODS

4.1 A WORKING PERSPECTIVE OF DIGITAL REPOSITORIES

An increasing range of content collections are referred to as 'repositories' in a variety of areas of the information environment. Increasingly widespread use of a term goes hand in hand with increasing diversity of meanings. A recent study commissioned by JISC proposed that a digital repository be differentiated from other digital collections by the following characteristics:[6]

- 'content is deposited in a repository, whether by the content creator, owner or third party;
- the repository architecture manages content as well as metadata;
- the repository offers a minimum set of basic services, e.g. put, get, search, access control;
- the repository must be sustainable and trusted, well-supported and well-managed.'

An often-cited general definition of a digital repository proposed originally by the Research Library Group (RLG) describes a digital repository as:[7]

> 'An organisation that has responsibility for the long-term maintenance of digital resources, as well as for making them available to communities agreed on by the depositor and the repository.'

The Reference Model for an Open Archival Information System (OAIS) standard defines the archive as an organisation that intends to preserve information for access and use by a designated community. The TRAC *Criteria for Measuring Trustworthiness of Digital Repositories and Archives: Audit Checklist* (forthcoming) has based its concept of a digital repository on the OAIS definition of an archive: an organisation responsible for long-term digital preservation.

In the course of test-audits carried out by the DCC, evidence was accruing to support the understanding that not all repositories with valuable digital collections are alike, created for the same purpose or delivering a similar range of services. Repositories form an intersection of interest for different communities of practice: digital libraries, research, learning, e-science, publishing, commercial data exploitation, records management, preservation. Within these communities the motivation for creating repositories differs, and the key services that repositories might provide range over several functional areas:

- Enhanced access to resources;
- New modes of publication and peer review;

[6] Rachel Heery, Sheila Anderson, *Digital Repositories Review* (2005), p. 2.

[7] Cf. http://www.bl.uk/about/strategic/glossary.html

- Corporate information management (records and content management systems);
- Data sharing (re-use of research data, learning objects, etc.).
- Preservation of digital resources (for the long term).

The digital repository self-audit toolkit, therefore, aims to encompass a broader range of digital repositories of all sizes and purposes. In January 2007 the Center for Research Libraries (CRL)[8] hosted a meeting of projects developing mechanisms and standards to support the audit, certification and accreditation of repositories. This meeting resulted in the development of a common set of criteria to which all digital preservation repositories, regardless of their mission, business model and source of funding, should adhere:

1. Commits to continuing maintenance of digital objects for its identified community(ies).
2. Demonstrates organisational fitness (including financial, staffing, structure, processes) to fulfil its commitment.
3. Acquires and maintains requisite contractual and legal rights and fulfils responsibilities.
4. Has effective and efficient policy framework.
5. Acquires and ingests digital objects based upon stated criteria that correspond to its commitments and capabilities.
6. Maintains/ensures the integrity, authenticity and usability of digital objects it holds over time.
7. 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.
8. Fulfils requisite dissemination requirements.
9. Has strategic programme for preservation planning and action.
10. Has technical infrastructure adequate for continuing maintenance and security of digital objects.

A key premise underlying these ten principles is that repositories will be of many types and sizes, and that preservation requirements must be scaled to the needs and means of a particular repository's identified community or communities.

Another significant distinction should be made between the repositories that are organisations whose core business is acquisition, preservation and dissemination, and repositories that form part of a larger organisation with a potentially very different mission. This categorisation becomes significant in the context of risk analysis and management: a digital repository that is an independent organisation (for example, a subject-based data centre) is

[8] http://www.crl.edu

responsible for all aspects of repository work and will have to define a full range of risk management measures; a digital repository that forms a unit within a larger organisation (for example, a digital data collection within a pharmaceutical company) can delegate some of its functions and transfer some of the risks to the organisation it is part of. However, in the latter instance the mandate and mission of the digital repository will have to be defined and looked at not only in the context of the actual repository work, but also in the context of what the repository's role is in achieving the aims of the wider organisation.

In order to support these different situations in auditing practice, the self-audit toolkit has defined a total of eight broad 'functional classes' of activities of a digital repository. These are further grouped into 'operational' and 'support' functional classes to represent the core functions of a digital repository: acquisition and ingest, preservation and storage, description and metadata management, access and dissemination; and functions that can be found in any organisation: organisation and management, staffing, finance management, technology support and security. When defining key activities, assets and identifying risks related to these, the auditors will have greater flexibility in choosing the areas of repository work that fall under their direct responsibility. The last of these categories has relatively higher significance for digital repositories as the main assets of the repository business – the digital information it preserves – are heavily dependent on a sound and secure technical infrastructure.

As noted in the Introduction, this audit tool will encourage repository staff to identify and classify the risks posed at every stage of their activities, to assess their probability and potential impact, and to consider how well they are being dealt with. Evidence is afforded considerable significance, with repositories expected not only to identify risks and manage them appropriately, but also to demonstrate their ability to do so, if only internally.

4.2 INTRODUCING A RISK-BASED APPROACH TO AUDIT

Risk management is not new. It is an integral component of good management and decision-making at all levels. All organisations manage risk continuously, whether they realise it or not – sometimes more rigorously and systematically, sometimes less so. More rigorous risk management occurs most visibly in the areas of protection of the environment and public health and safety, business continuity, and security of information systems.

Over the years risk management has evolved into a well-defined discipline. By adopting risk management strategies organisations, large and small, private and public, have learned to prevent losses and improve their business performance, quality of products and services, and safety. Risk management systems have emerged as a tool to complement existing management information tools and systems and can assist an organisation to achieve predefined objectives and strategies related to core business functions, asset management and projects.[9]

According to the Australian and New Zealand standard for Risk Management (AS/NZS 4360:2004, p. V), managing risks involves:

> 'managing to achieve an appropriate balance between realizing opportunities for gains while minimizing losses. […] It is an iterative process consisting of steps that, when undertaken in sequence, enable continuous improvement in decision-making and facilitate continuous improvement in performance.
>
> Risk management involves establishing an appropriate infrastructure and culture and applying a logical and systematic method of establishing the context, identifying, analysing, evaluating, treating, monitoring and communicating risks associated with any activity, function or process in a way that will enable organizations to minimize losses and maximize gains. […] Organizations that manage risk effectively and efficiently are more likely to achieve their objectives and do so at lower overall cost.'

The concept of risk is often interpreted in terms of threats, hazards, loss and other negative impacts. In the general organisational context, it is more fruitful to consider the risk as exposure to the consequences of uncertainty, or potential deviations from what is planned or expected.

> 'Good risk management allows stakeholders to have increased confidence in the organisation's corporate governance, accountability and ability to deliver. Whatever the purpose of the organisation is, the delivery of its objectives is surrounded by uncertainty which both poses threats to success and offers opportunity for increasing success. Risk is defined as this uncertainty of outcome, whether positive opportunity or negative threat, of actions and events. The risk has to be assessed in respect of the combination of the likelihood of something happening, and the impact which arises if it does actually happen. Risk management includes identifying and assessing risks and then responding to

[9] Victoria Lemieux, *Managing Risks for Records and Information* (2005), p. 2.

them.'[10]

Risk management is usually presented as a cycle that consists of individual stages. The stages can be ordered hierarchically.[11]

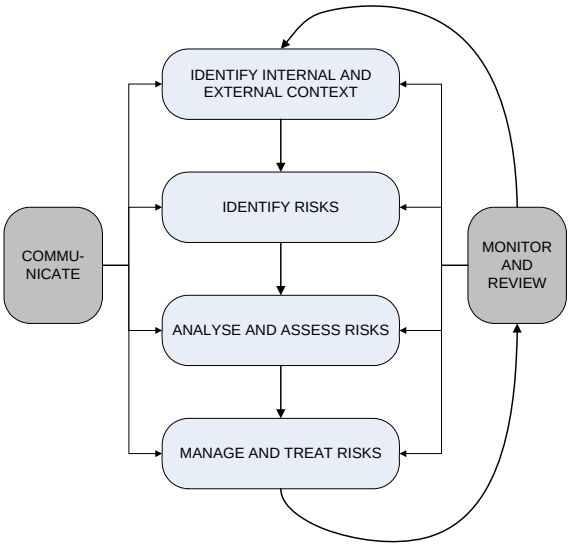


Figure 1: Example Graphical Hierarchical Ordering of Risk Management Stages

Or the risk management activities can be shown to form a circle where different stakeholders are involved in different stages:

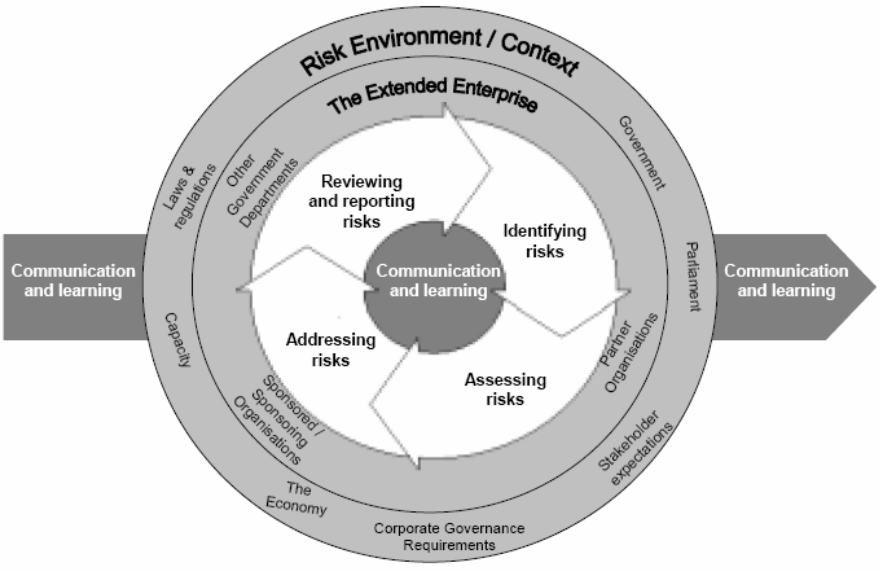


Figure 2: Risk Management Model (from Orange Book. *Management of Risk--Principles and Concepts*, © Crown copyright 2004)

[10] UK Treasury, *Orange Book. Management of Risk – Principles and Concepts* (2004), p. 7.

[11] Alternatively see for example AS/NZS 4360:2004, p. 9

Any risk management exercise will include these stages:

- Identifying the context where risks have to be managed.
- Identifying risks.
- Assessing and evaluating risks.
- Defining measures to address and manage risks.

Risk management is about being proactive. Risk means being exposed to the possibility of a bad outcome. Risk management means taking deliberate action to shift the odds in your favour – increasing the odds of good outcomes and reducing the odds of bad outcomes. The resources available for managing risks are finite and the aim is therefore to achieve an optimum response to risks, prioritised in accordance with an evaluation of the risks. Risk is unavoidable, and every organisation needs to take action to manage risk in a way that it can justify to a level that is tolerable. The amount of risk that is judged to be tolerable and justifiable is the 'risk appetite'.

Digital preservation is nowadays often defined as a risk management exercise where the aim is to convert the uncertainty about maintaining usability of authentic digital objects into quantifiable risks. The purpose of a digital repository is to do everything it can to mitigate the risks that impede its ability to provide access to authentic digital information. The measure of success of a repository's work is the 'quality' of information it releases to its users.

4.3 CONTEXT SURROUNDING AND FACILITATING THIS WORK

4.3.1 Risk and Digital Preservation

The issue of risk has been considered from a number of perspectives within the context of digital curation and preservation. For instance, a variety of work has sought to analyse the risks associated with particular file formats, perceiving the risk as something intrinsic to what a digital repository does, based upon the technical challenges associated with maintaining the usability of digital files and storage media. More recently some authors, such as Ross (2006) and Ross and McHugh (2006), have described the inherent uncertainty associated with digital preservation. A repository's task is therefore to identify and assess surrounding uncertainties, transform them into measurable risks and to define and implement means by which they can be effectively combated and mitigated. It is easy to see that the risks are not only technological but also organisational, staff and systems related, and connected with the external factors arising from the environment where the digital repository operates. Like any organisation, digital repositories can benefit from risk analysis and risk management techniques to support both their general management and their core business of digital curation and preservation.

In 2003 the ERPANET project published its *Risk Communication Tool*,[12] asserting that 'digital preservation is still an immature process from both an economic as well as a technical standpoint, and the lack of sufficient experience and evidence can be problematic'. This tool consequently aimed to provide advice to digital repositories to enable them to:

- highlight what digital resources are at risk within their organisation;
- highlight the risks to which these digital resources were exposed;
- highlight the risks to organisations posed by threats to digital resources (e.g. reputation, cessation of business);
- categorise and prioritise risks in order to facilitate their management;
- facilitate communication within the organisation about areas of risk;
- stimulate risk management strategy development.

Risk analysis methodology has also been employed within the context of website preservation, with the Cornell University Library adopting a risk management model for the purposes of monitoring and evaluating changes to web resources over time. The Cornell University Library Virtual Remote Control (VRC) tool[13] was developed to predict the probability of loss based on the presence or absence of key indicators that may enable or inhibit the longevity of web resources. Relying upon principles of risk management, as well as fundamental principles of records management, the VRC tool

[12] http://www.erpanet.org/guidance/docs/ERPANETRiskTool.pdf

[13] http://irisresearch.library.cornell.edu/VRC/methods.html

defined a series of stages that should be completed by organisations when selecting, monitoring and curating web resources.

4.3.2 Existing Approaches to Repository Assessment

Key audit and certification efforts to date, most notably those led by the taskforces established by The Research Libraries Group (RLG) and National Archives and Records Administration (NARA)[14] and nestor[15], were taken as a starting point in conducting the background research that underlies this tool. This work has concentrated on the establishment of check-lists to document the principal criteria that should be identifiable within a successful, and ultimately trustworthy, repository. The work of the RLG and NARA Digital Repository and Certification Task Force, more recently renamed TRAC, has led the development of a key approach to the assessment of digital repositories. This work also resulted in support by the Andrew W. Mellon Foundation for a project led by the Center for Research Libraries (CRL) on the Certification of Digital Archives to develop processes and methods for auditing and certifying digital archives. The Digital Curation Centre developed its approach to audit activities initially in conjunction with CRL.

4.3.3 Digital Curation Centre Pilot Audit Programme

Between April 2006 and January 2007 the Digital Curation Centre (DCC) conducted a series of pilot repository audits to determine an optimal methodology for the assessment of preservation repositories, and to evaluate the applicability and robustness of the RLG-NARA and nestor audit check-lists. A primary objective was to conceive an understanding of the evidential basis for demonstrating a repository's successful compliance with check-list criteria.

In total five repositories agreed to participate in the activity; a key requirement was that the chosen organizations demonstrated a degree of diversity to ensure that the principles derived and conclusions reached were widely representative. This was emphatically achieved, with scientific data centres, national libraries and cultural heritage archives among the audited repositories. Furthermore, the activity was truly international, with three continents represented between the five participants. Diversity of scale was also achieved, with operational budgets of participating repositories ranging from a few thousand pounds to upwards of eight or nine million pounds.

The first audited organization was the British Atmospheric Data Centre at the Council for the Central Laboratory of the Research Councils, responsible for the curation of large and often complex data originating from research funded by the Natural Environment Research Council and relied upon by thousands of meteorology research scientists. Following this was an

[14] http://www.rlg.org/en/page.php?Page_ID=20769

[15] http://nestor.cms.hu-berlin.de/tiki/tiki-index.php?page=wg-repositories

assessment of the Beazley Archive, established at the University of Oxford. With its origins in the late 1970s this collection of databases of pottery and gemstone digital images and associated data also serves a large user base, of mainly academics, although the quality of its content is also frequently exploited by major London based auction houses. The National Digital Archive of Datasets was the next repository to be exposed to assessment; a contractor of the UK's National Archives NDAD is responsible for the preservation and dissemination of datasets originating from UK government departments. Following this, the National Library of New Zealand's proposed National Digital Heritage Archive underwent formal assessment, including a comparison with the interim system that is in place until this ambitious project to establish a repository for accommodating the digital memory of New Zealand is complete. Finally, the Florida Digital Archive, at the Florida Center for Library Automation, which aims to provide long term preservation archival services for digital materials originating from any of Florida's state university libraries, was exposed to the audit mechanisms which, by that stage, were fairly well established.

The results of the audits have been, or are at the time of publication, in the course of being documented within a series of audit reports (Ross and McHugh, forthcoming a). Further conclusions have been documented in work undertaken by Ross and McHugh (2006) and Ross and McHugh (forthcoming b)[16].

The use of existing tools to underpin the DCC audits exposed difficulties with the practical applicability of these instruments. In their current form these instruments do not have associated metrics for determining the extent and effectiveness of organisational compliance; as a result, it remains difficult to conceive reliable means for comparing and assessing repositories that are heterogeneous in terms of their scale, scope or mission. International consensus on methodology and criteria for auditing digital repositories remains an essential outcome. Rather than representing a straightforward alternative (and therefore competitive) means for repository assessment, the DCC/DPE work aims to provide a complementary approach that can be used in association with the efforts of both TRAC and nestor.

This approach does not attempt to present a comprehensive list of best practice criteria or a benchmark based on specific standards. Instead, building on risk management work that has been undertaken within the digital preservation domain and beyond, the toolkit guides auditors through a series of tasks, categorised according to core institutional characteristics and activities. It encourages repository administrators and staff to identify the risks that carry the most profound implications with respect to their own organisation's business continuity, to determine the success with which they are able to anticipate, avoid, mitigate and treat risks, and to maintain appropriate evidential documentation to ensure that

[16] Seamus Ross, Andrew McHugh, *The Digital Curation Centre Repository Pilot Audits: Results and Lessons*, (forthcoming a). Seamus Ross, Andrew McHugh, *Preservation Pressure Points: Evaluating Diverse Evidence for Risk Management*, (forthcoming b). Seamus Ross, Andrew McHugh, *The Role of Evidence in Establishing Trust in Repositories. D-Lib Magazine*, July/August, vol. 12, nos 7/8 (Also published in *Archivi e Computer*, August 2006), http://www.dlib.org/dlib/july06/ross/07ross.html

any conclusions of this assessment are verifiable, even if only needed internally. This is a versatile tool and it can support pro-active and re-active approaches to risk. It is a critical starting in developing or validating the effectiveness of a digital preservation and curation strategy within a repository.

4.4 PRINCIPLES OF THE RISK-BASED APPROACH TO SELF-AUDIT

The success of self-audit depends to a large extent upon the commitment of the organisation undertaking the process. Every effort has been made to design the toolkit's implicit tasks to ease the process of identifying objectives and activities and deriving consequent risks. The anticipated value of the toolkit is as a device to facilitate the internal audit process. Recommendations are suggested based on responses submitted during the audit process. The primary value for repositories comes from the completion of the audit process, itself, and the development of the risk register and associated reports that represent its primary outputs.

As noted above, success or failure within the context of this tool does not correspond to a single objectively defined benchmark. Instead, repositories themselves must determine their metric for success based upon the anticipated outcomes of their business. The tool aims to ensure that auditors provide a comprehensive set of responses by referring to activities and risks originating from other work, and ultimately to the answers provided by other similar organisations that have already undertaken the audit process. Nonetheless, the toolkit is not prescriptive, and instead it simply suggests issues that may be relevant for a particular self-auditing organisation. Through defining the context of their own organisation, populating this definition with the activities and risks identified through the process of internal analysis, and supplementing this effort by referring to external sources the audit toolkit provides mechanisms to catch issues that may have been overlooked. The toolkit will assist auditors in developing a suite of comprehensive responses, and the development of a rich organisational picture. As more and more organisations undertake the self-audit process, an increasingly rich understanding can be formed about the specific risks faced by particular kinds of organisations. Self-auditing repositories will be classified according to their mandate, funding, size and type of collections and geographical location, and, as interactive elements of the tool are increasingly refined, this information will be used to facilitate the more refined focusing of assessment processes for similar or comparable organisations. Although repositories can undertake audits off-line using this document, we hope that they will complete them online using the toolkit available at http://www.repositoryaudit.eu. The tool provided there not only supports the production of audit reports but also allows users to contribute to an international effort to better understand the risks associated with digital curation. Users of the online tool can opt to have their reports and risk tables rendered anonymous and included in the DCC/DPE repository risk database to support refinement of the audit tool.

The toolkit's immediate value is internal to the self-auditing organisation. Quick reflection on the self-audit process indicates that there is, of course, nothing in the audit toolkit to stop a repository providing incomplete or

false responses to the profiles and risk tables and concluding as a result that each of the risks faced by the repository is being adequately managed, and that risk-avoidance or treatment strategies are well-established and positioned appropriately. Whether 'the repository realistically and reasonably applied the risk-based self-audit toolkit' is a risk; like all risks it must be identified and managed. During the recent period (April 2006 to January 2007) of DCC audits it became apparent that, for most repositories, the primary rationale for seeking audit mechanisms would be to establish an internal notion of areas where they enjoy success and where improvement could and should be achieved. In order to establish these outcomes the approach presupposes an organisational determination to provide honest and complete responses. This in turn distinguishes those repositories with aspirations for self-improvement from those merely seeking a badge of endorsement to show potential external partners and customers. Nevertheless, far from being bereft of external value, the process is designed to reflect the process that repositories must undergo prior to welcoming external auditors. By responding to the toolkit's demands for documented organisational self-awareness – the provision of an evidence base – any subsequent audit process will be streamlined considerably. Similarly, the DCC pilot audit programme confirmed beliefs about the value of an organisational risk register in building an understanding of a repository's strengths and shortcomings.

A further pitfall of the self-audit process is that organisations may list a mere subset of all the risks that they face, regarding having fewer risks associated with the repository as being synonymous with greater success. The latter supposition is spurious, and, as noted below, this toolkit is about risk management, and not risk counting. There is nothing to suggest that organisations facing a smaller number of risks are inherently more capable. Only the degree to which organisations are capable of identifying, avoiding and treating risks is relevant. Similarly, no individual risk is objectively more serious than any other. The likelihood and potential impact of individual risks will inevitably vary; repositories exhibiting the greatest success will be those with a demonstrable ability to reduce both likelihood and potential impact for every risk that they might face, however many that may be.

Following the successful completion of the self-audit exercise, organisations can expect to have:

- established a comprehensive and documented self-awareness of their mission, aims and objectives, and of activities and assets intrinsic to these;
- constructed a detailed catalogue of pertinent risks, categorised according to type and inter-risk relationships, and fully described in terms ownership, probability and potential impact of each risk;
- created an internal understanding of the successes and shortcomings of the organisation, enabling it to effectively allocate or redirect resources to meet the most pressing issues of concern;
- prepared the organisation for subsequent external audit whether that audit will be based upon the TRAC, nestor or forthcoming CCSDS digital repository audit assessment criteria.

4.5 MEASURING AUDIT RESULTS

Success within the self-audit process remains difficult to quantify completely, but by defining risks with an associated impact and probability index it is possible to describe the severity of individual risks, and consequently the overall riskiness of a particular organisational environment.

As we have noted above, a smaller number of documented risks does not necessarily indicate a more capable organisation. There is little relationship between the numbers of risks faced and the competence of the repository. Instead, one must consider only the probability and impact of each of the risks being faced. These values are determined by considering the naturally occurring likelihood and impact, and then taking into account the avoidance and treatment mechanisms that have been put in place by the organisation. For instance, the risk of losing key staff members could be considered as naturally quite likely, and of potentially devastating impact. However, the repository could pursue avoidance measures by ensuring that staff salaries and conditions are favourable in comparison with those of similar organisations, and introduce treatment mechanisms to ensure that in the event of the risk's execution the remaining staff are sufficiently well (indeed cross-) trained to facilitate internal reappointment and that every aspect of the departing staff member's role is well documented.

5 PART II, THE DCC/DPE AUDIT TOOLKIT

5.1 INTRODUCTION TO THE SELF-AUDIT TOOLKIT

The purpose of the self-audit toolkit is to facilitate the auditor in:

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

The self-audit toolkit is designed to help and guide the auditor along a similar route of analysis to that which an external auditor would use to examine and analyse the work of the repository. Its design is based on the experiences of the DCC pilot audits conducted in 2006. In order to make the self-audit process as easy as possible for the auditor the second release of the self-audit toolkit will be as an interactive web-based tool with semi-automated workflow mechanisms, options for pre-filled fields, and guidance materials in the form of examples, suggestions and comparisons. The toolkit described here forms the basis of the interactive online tool.

5.2 REQUIREMENTS OF THE SELF-AUDIT PROCESS

The audit process relies heavily on the integrity, effectiveness and capabilities of the individual or individuals performing the audit. To achieve the maximum benefit from the audit process the organisation needs to select its auditor or audit team with care. As well as making certain that the individual or team is appropriately placed within the organisation it is also essential to ensure that they are provided with the right kinds of evidential materials.

5.2.1 Auditor Characteristics

The Institute of Auditors defines the auditor's role as follows:

> 'Internal Auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes. Internal auditing reviews the reliability and integrity of information, compliance with policies and regulations, the safeguarding of assets, the economical and efficient use of resources, and established operational goals and objectives.'[17]

It is generally anticipated that a single individual will take primary responsibility for conducting the self-audit process, although, as mentioned above, it is essential that the organisation as a whole invests and participates in the process. The success of the audit process benefits from the participation in the process of key players within the organisation. The primary auditor assumes responsibility for ensuring that all appropriate contributions from within the organisation are solicited, obtained and appropriately assessed. In order for the process to be internally reliable, and for its outcomes to be regarded as correct and complete, organisations should ensure that their auditors are both appropriately trained and have suitable personal skills.

5.2.2 Personal Attributes

ISO 19011 *Guidelines for quality and/or environmental management systems auditing* offers a good indication of the ideal characteristics an auditor should have and manifest:

- high ethical standards
- open-mindedness
- diplomacy
- observational skilfulness
- perceptiveness
- versatility

[17] The Institute of Internal Auditors, *Code of Ethics*

- tenaciousness
- decisiveness
- self-reliance.

5.2.3 Organisational Positioning

An ideal auditor will be centrally positioned within an organisation, with influence or responsibilities associated with as many aspects of the repository's business as possible. Breadth of knowledge should be given higher priority than in-depth understanding of specific business objectives or activities. Auditors should occupy a suitably senior role and level of trust within the organisation to facilitate engagement with organisational colleagues, and have access to a comprehensive range of internal documentation. Auditors should be granted a full range of system access privileges during the period of the audit.

5.2.4 Evidential Requirements

A range of evidence expectations are described within the audit tool, reflecting a belief that organisations must be able to demonstrate their ability to effectively manage their risks. The only risk avoidance or treatment measures that can be taken seriously are those that are based in or recorded within formal documentation. Some of the most likely sources will be an organisational mandate and mission statement; example deposit agreements; job descriptions, organisational charts and staff résumés; business plans and annual financial reports; policy documents and procedure manuals; workflow documents; technical architecture plans; maintenance reports; and the published results of other audits.[18] Within these, policy and procedure documentation is perhaps the most fertile source for risk management measures. A minimum list of documented policies that all repositories should have is provided as an appendix to the soon-to-be-published TRAC certification check-list. Auditors should aggregate each of these documents (or their equivalents) before beginning the audit process. The list includes:

- Contingency, succession or escrow plans (one of, as appropriate)
- Community definition and policy relating to levels of service
- Policies relating to legal permissions
- Policies and procedures relating to acquiring and using feedback
- Financial procedures
- Policies/procedures relating to challenges to rights
- Policies/procedures related to ingest

[18] S. Ross and A. McHugh, 2006, 'The Role of Evidence in Establishing Trust in Repositories', *D-Lib Magazine*, July/August, vol. 12, nos 7/8 (Also published in *Archivi e Computer*, 2006), http://www.dlib.org/dlib/july06/ross/07ross.html

- Preservation strategies
- Storage/migration strategies
- Policy for recording access actions
- Policy for access
- Processes for media change
- Change management process
- Critical change test process
- Security update process
- Process to monitor required changes to hardware
- Process to monitor required changes to software
- Disaster plans.

The DCC audits have demonstrated that it is within these kinds of documents that organisations have documented the means they have in place for risk management. However, this list is by no means exhaustive, and it is likely that risks associated with other aspects of policy will be faced by many, if not most, organisations. For example, staffing related issues such as training and professional development may be described and documented elsewhere. The risks associated with stagnation of skills, for instance, are potentially serious, and therefore auditors are encouraged to think beyond this list and consider first the risks, and then the associated policies that describe the means to avoid or treat them. Throughout the process auditors will complement existing documentation with the creation of a register of risks, with associated reporting mechanisms for describing and demonstrating the repository's success in both qualitative and quantitative terms.

Although documentation is crucial, it is not the only source of evidence that should be pursued. As a result of the DCC audits we have also identified experimental, testimonial and observational evidence. Assuming that a single individual is completing the self-audit process, it is unlikely that they will themselves have a comprehensive knowledge of every aspect of the repository's activities. With this in mind it is vital that the process should be an open one where a wide range of staff are capable of contributing their thoughts and noting risks for inclusion within the overall risk register. Individuals that should be consulted include the repository overall administrators; hardware and software administrators; and officers responsible for the core functions of ingest, archiving, preservation, documentation and access. Everyone from the head of the organisation to the janitor or cleaning staff can provide insights into the process of repository management. These additional contributions need not be too lengthy, but must be considered if the outcomes of the process are to be representative of the repository as a whole.

5.2.5 Estimate of Required Effort

It is anticipated that the entire self-audit process will take between 24 and forty hours (or, at 6 hours per day, four days or seven days). Each individual task is allocated an estimated effort requirement, although,

depending upon the scale and scope of repository operations, and the degree of scrutiny with which the assessment is conducted, this may vary, occasionally substantially. Additional preparation time is excluded from the four-day estimate, and it is during this period that auditors can gather the documentation that they will need to refer to during the risk identification and assessment process. The level of effort is based upon our experiences with the pilot audits. As the toolkit is used by other individuals and organisations we hope that they will provide us with an indication as to whether their audits were completed within our estimated timeframe and if not where the obstacles to achieving this timing lay.

5.3 DEFINITIONS AND GLOSSARY OF TERMS

For the purposes of this document, the following definitions are used for key terminology.

Activity
Major tasks performed by an organisation within the context of, and in order to accomplish, a function.

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

Digital repository
An organisation or its part 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:

1. Commits to continuing maintenance of digital objects for its identified community(ies).
2. Demonstrates organisational fitness (including financial, staffing, structure, processes) to fulfil its commitment.
3. Acquires and maintains requisite contractual and legal rights and fulfils responsibilities.
4. Has effective and efficient policy framework.
5. Acquires and ingests digital objects based upon stated criteria that correspond to its commitments and capabilities.
6. Maintains/ensures the integrity, authenticity and usability of digital objects it holds over time.
7. 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.
8. Fulfils requisite dissemination requirements.
9. Has strategic programme for preservation planning and action.
10. Has technical infrastructure adequate for continuing maintenance and security of digital objects.

The self-audit toolkit does not presume 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.

Functional class
A discrete group of interrelated digital repository activities. The strength of bonds between activities ranges from loosely bound to tightly coupled. In this self-audit toolkit functional classes are divided into 'operational' and 'support' categories to represent the core functions of a digital repository: acquisition and ingest, preservation and storage, description and metadata management, access and dissemination; and functions that can be found in

any organisation: organisation and management, staffing, finances management, technology support and security.

The functional classes are defined primarily to provide a structure to the audit process and the resulting risk register, and to guide the auditor through the assessment process. These functional classes are not derived from a systematic functional analysis of a repository and are not a substitute for a business classification scheme. If the repository has an up-to-date business or records classification scheme, it may benefit the interpretation of audit results if this classification is used instead of the eight functional classes offered by default in the self-audit toolkit.

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.

Owner
An individual or entity that has approved management responsibility for controlling the production, development, maintenance, use and security of the 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.[19]

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)

[19] Treasury Board of Canada, *Integrated Risk Management Framework* (2001).

Stakeholders
Those people and organisations who may affect, be affected by, or perceive themselves to be affected by a decision, activity or risk. (AS/NZS 4360:2004)

Threat
A potential cause of an incident that may result in harm to an organisation, its assets or systems.

Vulnerability
A weakness of an asset or activity that can be exploited by one or more threats.

5.4 RISK ASSESSMENT PRINCIPLES

When assessing risks, their probability and impact have to be quantified. Probability is the likelihood that the risk event will occur. The self-audit toolkit considers risk probability according to the following scale:

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**

The potential impact of risks is classified according to the following scale:

Risk Impact Score	Interpretation
0	*Zero* impact, results in **zero loss** of digital object authenticity and understandability[20]
1	*Negligible* impact, results in **isolated but fully recoverable loss** of digital object authenticity and understandability
2	*Superficial* impact, results in **widespread but fully recoverable loss** of digital object authenticity and understandability
3	*Medium* impact, results in **total but fully recoverable** loss of digital object authenticity and understandability
4	*High* impact, results in **isolated loss, including unrecoverable loss** of digital object authenticity and understandability
5	*Considerable* impact, results in **widespread loss, including unrecoverable loss or loss that is recoverable only by third party** of digital object authenticity and understandability
6	*Cataclysmic* impact, results in **total and unrecoverable loss** of digital object authenticity and understandability

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

The complete risk description that is used in the self-audit toolkit is the following, but auditors are by no means restricted to this and may choose to use a more extensive set of attributes to characterise risks in their risk register:

Risk Label	*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*
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*
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 targetted risk-severity rating plus risk reassessment date*

5.5 RISK ANALYSIS BASED SELF-AUDIT METHODOLOGY

As described above, the toolkit's fundamental philosophy is to facilitate, and not legislate. Although extensive guidance is offered to auditors, their commitment and engagement are essential in order to ensure that the results of the process are of value. The risk management exercise takes place within the context of the goals and objectives of the repository. The very first priority is therefore to conceive a definition of this context. This can be done in terms of organisational objectives, which determine the parameters within which the assessment will take place. The Australian and New Zealand *Risk Management Standard* makes explicit the importance of internal context:

- 'the major risk for most organizations is that they fail to achieve their strategic, business or project objectives, or are perceived to have failed by stakeholders;
- the organizational policy and goals and interests help define the organization's risk policy; and
- specific objectives and criteria of a project or activity must be considered in the light of objectives of the organization as a whole.' (AS/NZS 4360:2004, p. 14)

In practical terms, the self-audit process consists of a number of tasks, which, although discrete and of independent value, together contribute to an overall picture of organisational risk. Simply put, the auditor is guided through a process of identifying objectives, then specific activities, assets and people and finally associated risks.

5.5.1 Identification of Objectives

The process begins with the self-auditing organisation specifying its mandate. From this starting point, a hierarchy of fundamental objectives and activities is identified, which can be further subdivided depending on the degree of granularity that is necessary to facilitate completion of subsequent sections. It is generally acknowledged that a higher degree of granularity will make the identification and alignment of activities and risks more straightforward, although this is not strictly necessary. The *DCC/DPE Digital Repository Audit Method Based on Risk Assessment* provides a selection of example objectives to assist the participating organisation in identifying its own objectives at the appropriate 'level'.

5.5.2 Identification of Activities and Assets

Activities are mainly derived from organisational objectives; these encapsulate the ways in which the broad aims of the repository are realised in practice. Assets are the associated resources, including human resources and technology solutions, which contribute to their satisfactory achievement.

5.5.3 Aligning Risks to Activities and Assets

Following the completion of the organisational description that represents the outcome of the first two tasks, auditors are required to document the specific risks associated with each identified activity and asset. Again, examples are provided to help ensure that risks are characterised at the appropriate level of granularity. In many cases a single risk will be associated with multiple activities, and in others multiple risks will be relevant to a single activity. Both are quite acceptable. Both assist subsequent grouping of risks and their assessment. Risk groupings can be defined related to the contexts within which the risks originate, their potential effects or the means by which they may be managed. Similarly, risk relationships can be conceived at this stage. Risk relationships may be characterised as one or more of:

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
Complementry	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

In practical terms atomic risk situations are unlikely – the allocation of more resources to treat or avoid any risk will in almost every case mean that fewer resources are available to allocate elsewhere. In this sense at least, every risk has an inversely attuned relationship with every other, except where risk treatment strategies benefit the management of other risks, and the relationship is complementary.

5.5.4 Assessing, Avoiding and Treating Risks

Having completed a catalogue of relevant risks the auditor then develops for each a range of risk attributes specific to their own organisation. Mandatory fields include characterising information about the risk's probability, impact, owner, and the mechanisms or proposed mechanisms by which it can be avoided or treated. The process of characterising risks depends on the availability of documentary evidence, which will in most cases exist in the form of policy documentation.

5.5.5 Self-Audit Results

The main output from the self-audit process is an organisational risk register, which in itself represents a very useful management tool, and can form the basis for subsequent full audits. In addition, particularly as interactive features of the toolkit are increasingly realised, auditors will be able to present a range of reports based on the risk groupings they have identified, and visualise the results in a number of ways to enable them to describe accurately the areas where improvement is required, and to enable them to prioritise organisational efforts to achieve these improvements.

5.5.6 The Risk Register

The risk register lists all the identified risks and the results of their analysis and evaluation. It incorporates information on the status of each risk. These details can then be used to track and monitor their successful management as part of the activity to deliver the overarching organisational goals. Sometimes this kind of document is described as a 'risk log', although the terms are synonymous.

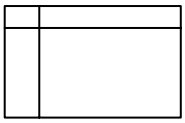
A maintained risk register provides a useful vehicle for communicating risks to the management, funders (both actual and potential) and depositors of the repository.

5.5.7 The Risk-Based Self-Audit Process

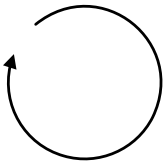
The diagram on the following page depicts the stages of the self-audit process. Diagrams in this report use the following conventions:

represents a process for which there is a separate screen in the self-audit toolkit.

represents a guidance field with typical documents and information that helps the auditor to fill in the required fields in the audit form.

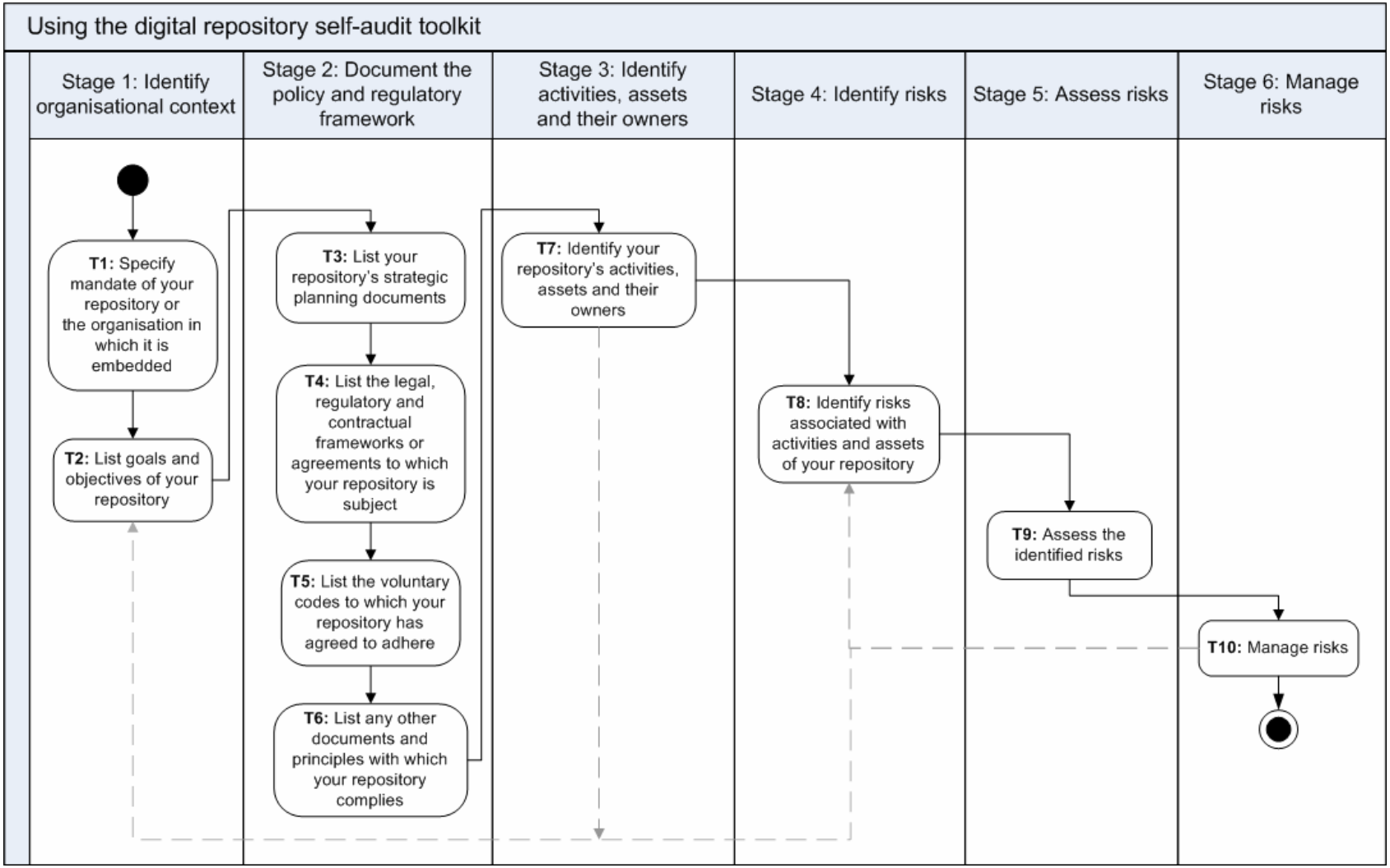


represents a list of multiple categories into which the information entered in the questionnaire form is divided.



represents a loop in the process – the question has to be repeated for each category listed in the boxes attached to the loop arrow.

represents a possible route for a continuous cycle of risk management activities.


Using the digital repository self-audit toolkit
Stage 1: Identify organisational context
Stage 2: Document the policy and regulatory framework
Stage 3: Identify activities, assets and their owners
Stage 4: Identify risks
Stage 5: Assess risks
Stage 6: Manage risks
T1: Specify mandate of your repository or the organisation in which it is embedded
T2: List goals and objectives of your repository
T3: List your repository's strategic planning documents
T4: List the legal, regulatory and contractual frameworks or agreements to which your repository is subject
T5: List the voluntary codes to which your repository has agreed to adhere
T6: List any other documents and principles with which your repository complies
T7: Identify your repository's activities, assets and their owners
T8: Identify risks associated with activities and assets of your repository
T9: Assess the identified risks
T10: Manage risks

5.6 THE STAGES OF AUDIT

The self-audit process progresses through six stages:

- Stage 1: Identify organisational context
- Stage 2: Document policy and regulatory framework.
- Stage 3: Identify activities, assets and their owners
- Stage 4: Identify risks
- Stage 5: Assess risks
- Stage 6: Manage risks

5.7 STAGE 1: IDENTIFY ORGANISATIONAL CONTEXT

In Stage 1, the audit process focuses on establishing the organisational context.

5.7.1 Aim of this Stage

The purpose of Stage 1 is to identify the repository's role, and to chart its goals and objectives. The scope of the audit will be largely determined by the repository's own scope and mandate.

In Stage 1, auditors document the mandate and derive both the goals and objectives of the repository. The ultimate purpose of this stage of the audit is to define the scope of the repository work, verifying internal awareness of the organisational framework, and at the same time ensuring that appropriate supporting documentation exists. If the repository belongs to a larger organisation or organisational structure (e.g., LOCKSS[21] or federated repositories), its place and context within the organisation are charted as part of Stage 1.

5.7.2 Tasks Associated with this Stage

Within this stage auditors must describe the overall purpose of the repository, in order to determine the characteristics that will undergo risk analysis and subsequent assessment. Tasks comprising this stage are two-fold. First, auditors must identify the repository's mandate, which, it is anticipated, will be described in an organisational mission statement or enacting documentation. The subsequent task requires auditors to identify, within that mandate, each organisational goal and objective relevant to the repository.

[21] http://www.lockss.org/lockss/Home

5.7.3 Anticipated Results of this Stage

Following the completion of this stage, auditors will have established:

- the mandate and a comprehensive list of repository goals and objectives;
- an understanding of repository and organisation goals and objectives;
- a sound basis for defining the scope of the risk analysis based audit.

This information will assist auditors in identifying and interpreting the repository's activities and assets and making effective decisions about their associated risks. It will help to place risks within the broader context of the repository or a wider organisation, and ensure that any proposed solutions are based on a firm understanding of the organisation and its environment.

5.7.4 Where Does this Stage Fit Within the Overall Audit Process?

It is advisable to complete Stages 1 and 2 of the audit simultaneously, as Stage 2 requires auditors to conceive or refer to existing supporting documentation to underpin the responses provided during Stage 1. It requires auditors to identify additional documents pertaining to the business and regulatory framework within which the repository operates.

Information provided by the auditor in this section will be referred to in subsequent sections in which organisational activities, assets and associated risks are identified.

5.7.5 What Resources are Required to Complete this Stage?

Anticipated Effort: 3 hours

Investing effort in effectively completing the tasks within this stage will have a positive impact on the overall outcome of the audits, but the level of detail and granularity of the answers determines to a significant extent the quality of risk identification and assessment at subsequent stages of the self-audit. Greater investment in the initial stages of the process is likely to contribute to a reduction of the effort required during subsequent stages.

Initial preparation time is required before commencing this stage. Pre-audit effort should be spent aggregating the documentation necessary to complete this stage of the self-audit process, and engaging with repository staff to determine the extent of organisational objectives, activities and, ultimately, risks.

Auditors may find it useful to return to the list compiled during Stage 1 at later points in order to add further information, should the need arise.

Before commencing Stage 1, auditors should:

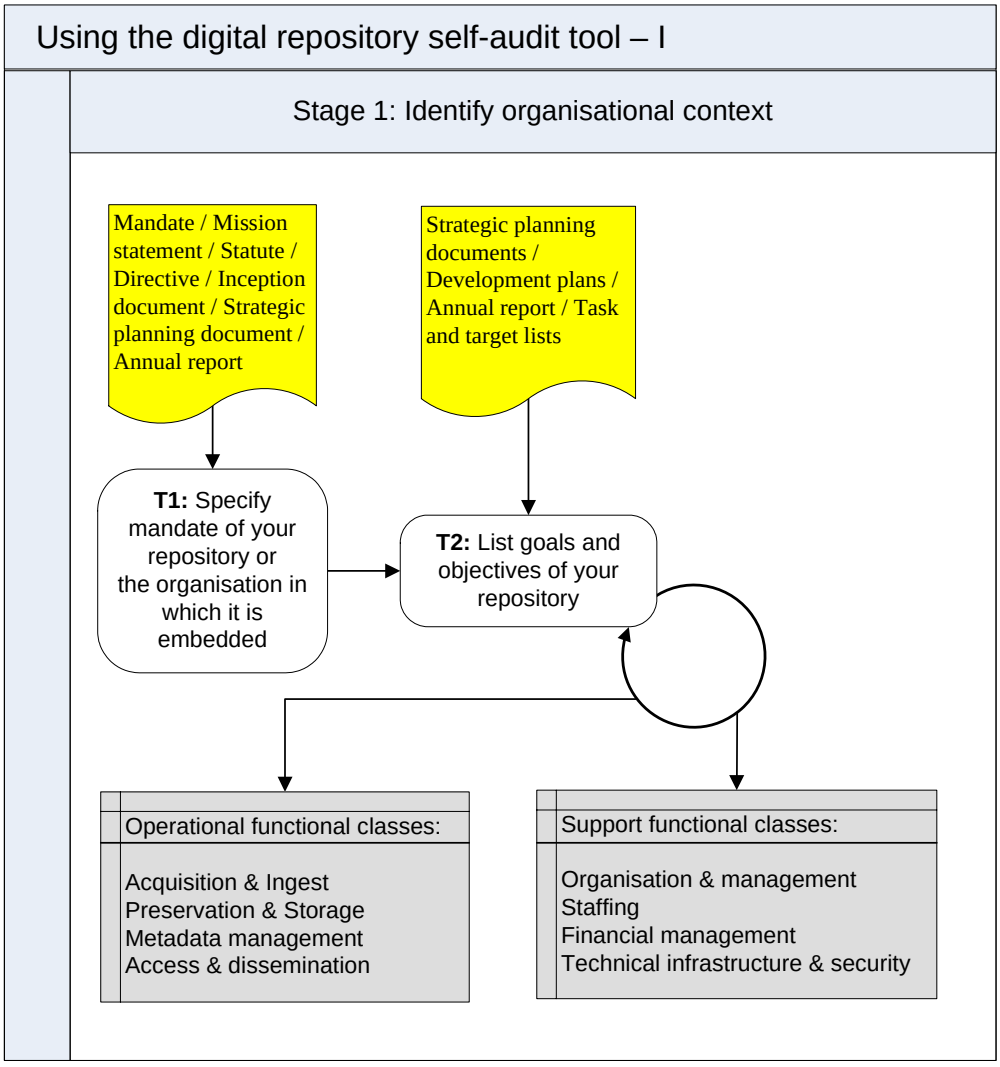
- compile a preliminary list of required documents;

- solicit input from a range of personnel within or related to the repository to acquire an increased understanding of its foundation and mission. Individuals might include, but need not be limited to, senior management, legal representatives, external stakeholders and financiers.

In order to complete Stage 1, auditors will need to ensure:

- access to internal documents, such as strategic planning documents, corporate and business plans, annual reports, target lists, and contracts;
- access to personnel with further knowledge of the goals and objectives that the organisation has set itself.

5.7.6 Diagram Depicting this Stage



5.7.7 Instructions for Completing the Stage

The initial two stages of the audit process will enable the identification of:

- the boundaries of the repository, its activities and its stakeholder community(ies);
- internal and external stakeholders whose interests the repository should take into account;
- the goals and objectives that have been established to achieve the mission of the repository;
- the legal framework that influences the operations of the repository;
- the business, social and ethical standards the community expects the repository to meet;
- the available knowledge base – state of the art in thinking and practice that exist in the repository.

Tasks in this Stage will help to focus analysis and provide a framework for the documentation of findings. Completing the tasks in this Stage will create a concise body of information about the repository to draw upon during the subsequent stages of the audit.

For fulfilling the tasks in this section, auditors should use the forms T1 and T2 (see Part III of this document). If filling in the forms manually, copies should be made of the form T2, as a form will be required for each of the eight different functional classes within which repository efforts will be described and structured.

5.7.7.1 T1: What is the mandate of your repository or the organisation in which it is embedded?

Auditors should describe their organisation's mandate in the space provided.

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. Every organisation has been established for a purpose. A typical mandate for a repository includes functions like collecting, preserving and making accessible some type of material.

An organisational mandate should be expressed to convey the organisation's official basis, and the reasons for its establishment and continued existence. It may also have been translated into a mission statement associated with specific business activities; the form this takes will depend on the mandate's interpretation, identified needs at a certain moment in time, and the availability of resources.[22] A mission statement is a

[22] Hans Hofman, Babak Hamidzadeh, Ken Hawkins, Bill Underwood, *Business-driven recordkeeping model. Version 5.0* (February 2007) (forthcoming by InterPARES-2)

succinct description of what the organisation is seeking to achieve in the long term – its raison d'être.

Typically, an organisation's mandate and mission statement can be found on the pages of its website, within its annual reports or within founding or establishing documents or in acts of law or even constitution. Examples of the latter include legal statutes (e.g., archives act), regulations, directives and agreements.

Example Task Response Excerpt:

T1:	**What is the mandate of your repository or the organisation in which it is embedded?**
Example:	The role of the [repository name] is to assist researchers to locate, access and interpret [type of data] and to ensure the long-term integrity of [type of data] produced by publicly funded research projects.

5.7.7.2 T2: List goals and objectives of your repository

In this task, auditors describe the goals and objectives of the organisation associated with each of eight functional classes. These are the four operational functional classes (Acquisition & Ingest, Preservation & Storage, Metadata management, Access & Dissemination) and a further four supporting functional classes (Organisation & Management, Staffing, Financial management, Technical infrastructure & Security). If completing the exercise on paper, a separate T2 sheet should be used to correspond to each of the eight functional classes.

In order to plan and manage the everyday work of an organisation, a set of medium- or short-term objectives is usually laid down. These are frequently found within a range of strategic planning documents, development plans, annual reports, and tasks and targets lists, but may also exist as identifiable expectations of the community to which the organisation belongs. If a list of objectives is not readily available, it can be constructed from the mandate, mission and inception documents of the organisation.

Each of the goals and objectives should be categorised according to the functional class or classes to which it corresponds most closely. An objective could be associated with more than one functional class. It is expected that some objectives and activities do not fit comfortably into the functional classes provided, in which case the auditors may find it convenient to add additional categories to the eight we propose here.

Example Task Response Excerpt:

T2:	List goals and objectives of your repository
Example:	Operational functions: Acquisition & Ingest
	File ingestion system to actively verify and validate files as depositors provide them
	Provide dataset usage statistics for data depositors
	Define acceptable submission format(s)
	Acquisition and distribution of [type of data] from [depositor] within the next 12 months
	Operational functions: Preservation & Storage
	Document all changes to archived content
	Operational functions: Metadata management
	Ensure that data handling within [repository name] is efficient
	Maintain referential integrity between metadata and archived content
	Operational functions: Access & Dissemination
	Continue serving the user community with ready access to all agreed data sets
	Provide value-added services to the users within the resources available
	Establish a new user registration and access control system
	Provide dataset usage statistics for data depositors
	Provide users with news on data sets and more general issues
	Support functions: Organisation & Management
	Continue serving the user community with ready access to all agreed data sets, ensure that data handling within [repository name] is as efficient as possible, and provide value-added services within the resources available
	Promote [repository name] and its data collection through regular representation at scientific meetings and the provision of appropriate publicity materials
	Support functions: Staffing
	Define staff roles, responsibilities and their relationships
	Support functions: Financial management
	Maintain financial viability after funding from [project name] ceases after 2007
	Support functions: Technical infrastructure & Security

	Continue to develop and enhance the infrastructure of the [repository name], including the development of underpinning work for e-science activities
	Computing system to support data storage up to 80 Tb and limited user processing of data
	Define a strategic IT plan for 2007-2009, by 1/3/07

5.7.8 What to do in the Event of Required Information Being Unavailable

5.7.8.1 T1: What is the mandate of your repository/organisation?

If the auditor is unable to locate the repository or organisation's mandate he or she should construct one, at least for the purposes of this audit. This may of course be subject to subsequent refinement, but it is necessary to have such a document at this stage of the process. The Board of Management (or similar committee) should be asked to endorse the mandate and, if necessary, contribute to its definition or refinement.

In order to define the mandate of your repository, auditors should study the organisation's inception documentation and derive a statement describing the organisational basis and purpose.

5.7.8.2 T2: List goals and objectives of your organisation

Once auditors have exhausted their available documents during the process of listing goals and objectives, they may also wish to consider these additional sources that often provide a good starting point for defining organisational goals and objectives:

- annual reports;
- strategic plans (e.g. business plan, corporate plan, departmental development plan);
- procedural manuals, operational manuals;
- recordkeeping systems and classification schemes;
- organisational charts;
- publications targeting the interests of particular stakeholders.

These kinds of documents are typically accessible through an organisation's intranet or are available on a shared file storage space.

The aim is to compile a more or less complete list of the repository's goals and objectives by the end of this stage. If appropriate, the list of main objectives should be agreed with the senior management and/or staff. However, auditors are welcome, and encouraged, to return to this list and append additional responses throughout the assessment process.

For further methodological background for answering the questions in this stage auditors may wish to consult:

- Step A of the *Design and Implementation of Recordkeeping Systems* (DIRKS) *Manual*, published by the National Archives of Australia[23]
- Section 4 of the HB 436:2004 *Risk Management Guidelines. Companion to AS/NZS 4360:2004*

5.7.9 Discussion

After identifying a set of objectives the auditors may want to match the objectives against the way the repository is structured, financed, facilitated, and staffed. This will allow them to analyse the potential and the effectiveness of the current structure and facilities, adequacy of resources and staffing, which can be a significant source for additional risks.

5.7.10 Comments

Auditors are encouraged to send comments, concerns or observations to the DCC/DPE audit and certification working group at feedback@repositoryaudit.eu.

5.7.11 Checklist

Before proceeding to the next stage, auditors should ensure that they have:

- stated the mandate of the repository;
- provided a list of short- and medium-term goals and objectives for each of the eight functional classes even if these are, by necessity aggregated;
- developed an understanding of where to find the documents in which goals and objectives are detailed.

[23] http://www.naa.gov.au/recordkeeping/dirks/dirksman/step_A.html

5.8 STAGE 2: DOCUMENT POLICY AND REGULATORY FRAMEWORK

This is the second of the six stages of self-audit.

5.8.1 Aim of this Stage

This Stage gives auditors the opportunity to provide or refer to evidence capable of supporting an assertion that the repository:

- operates appropriately with respect to relevant regulatory frameworks;
- has an efficient and effective policy framework;
- is aware of the societal, ethical, juridical, and governance frameworks;
- is aware of the legal, contractual and regulatory requirements to which the repository is subject.

These policies are not necessarily extrinsic; in some instances the regulatory framework will also be affected by the institution in which the repository is based.

A broad definition of the repository's regulatory framework is assumed, incorporating acts or provisions with both external and internal origins. Relevant extrinsic commitments and influences include statutory legislation and statutory instruments, global or business-related regulations, *de facto* or established standards and codes of practice. Internally arising commitments may be traceable to contracts, policies, strategic planning, or accepted business norms.

5.8.2 Tasks Associated with this Stage

At this Stage auditors need to:

- determine what to look for;
- collect information from documentary sources as a desk research exercise;
- compile a list of documents regulating the work of the repository;
- analyse the relevance of documentary evidence to the goals and objectives listed in the previous Stage.

5.8.3 Anticipated Results of this Stage

By completing this Stage, the auditor will have:

- a comprehensive list of internal and external documents that create the regulatory context for the repository work;

- analysed the various documents that form the regulatory framework;
- a better understanding of the conditions in which the repository is working (e.g. its contractual arrangements with its funders, its depositors or its users);
- a more comprehensive understanding of actual and potential stakeholders in the repository work.

The list of source documents and references created in this Stage will contribute to the next stages of the self-audit by acting as reference material when making effective decisions about the repository's activities and risks associated with these. It will help to define risks within the repository, and ensure that proposed solutions are based on a firm understanding of the organisation and its environment.

5.8.4 Where Does this Stage Fit Within the Overall Audit Process?

Again, documents identified and listed in this Stage will be used as reference material in subsequent self-audit stages.

The goals and objectives listed in the previous Stage and the activities, assets and technology identified in the next Stage will form a framework where risks can be identified that arise from mismatches between the stated goals and regulatory requirements, and between regulatory requirements and stated activities.

5.8.5 What Resources are Required to Complete this Stage?

Anticipated Effort: 3 hours

Stage 2 of the self-audit can be, but does not have to be, time-consuming. The time required to complete this stage will depend on the auditor's general knowledge of the repository's legal and regulatory context, knowledge of and access to contractual agreements, and knowledge of standards that may apply to the repository. The result of this Stage may separately constitute a valuable resource for the repository. The list of all legal, regulatory and contractual obligations and strategic policy documents should be presented with rich details and appropriate references. While the current audit does not explicitly require a high level of granularity in the references, it may be helpful if these were available.

The main time investment is expected to go into finding and analysing the documentation and sources to form the list of pertaining regulatory requirements.

Once these lists are compiled the organisation should undertake to keep them up-to-date, as they will provide a valuable resource for responding to the frameworks in which the organisation exists and will be required for future audits.

Before starting Stage 2, the auditor should:

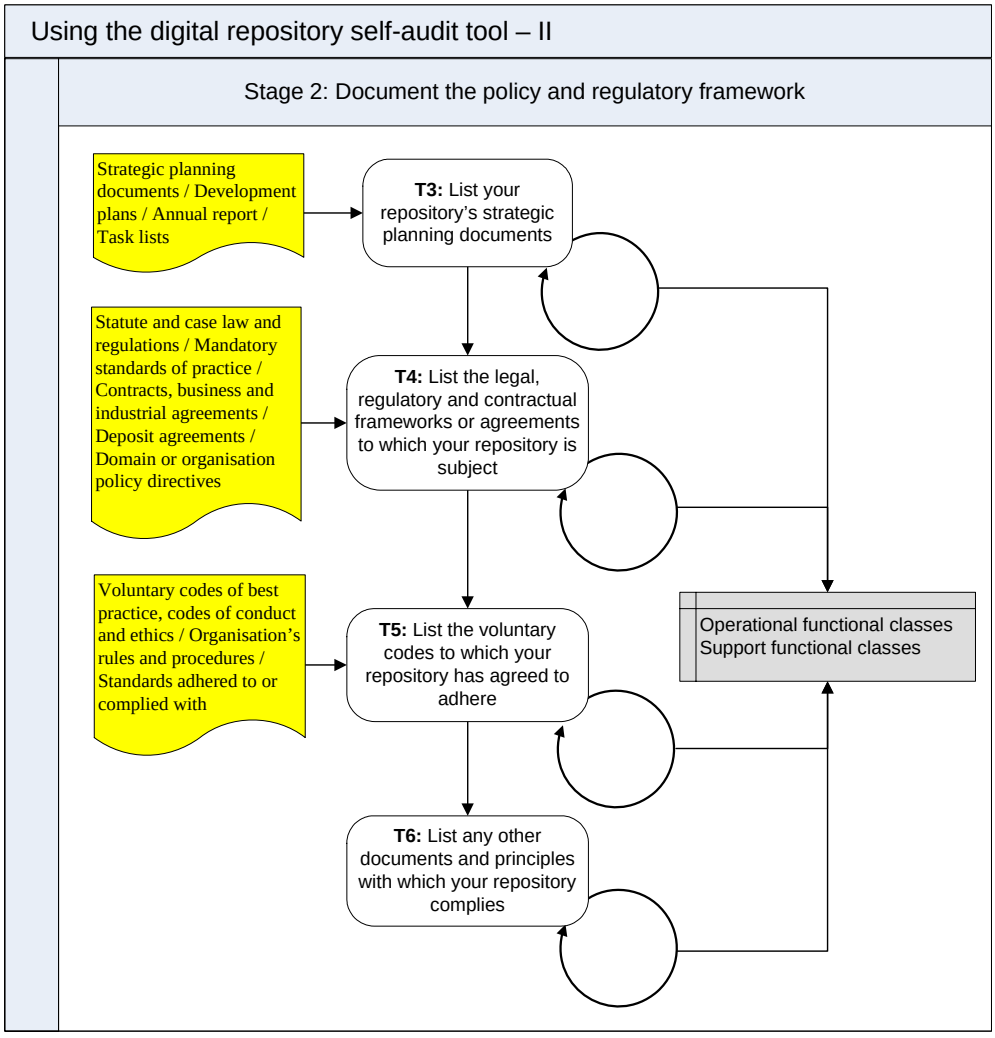
- compile a preliminary list of relevant documents (s)he is aware of;

- have access to lawyers and/or a senior manager who can give an overview of the legal and contractual obligations of the repository.

In order to complete Stage 2, the auditor will need to ensure:

- access to internal documents, such as strategic planning documents, corporate and business plans, annual reports, target lists, and contracts;
- access to external documents and sources, such as legislation, standards, codes of practice;
- possibly access to personnel with further knowledge of the legal and contractual requirements as well as the standards compliance of the repository.

5.8.6 Diagram Depicting this Stage



5.8.7 Instructions for Completing the Stage

The task of listing documentary sources as references is straightforward – auditors are expected to provide the title of the document, if necessary its version number or publication date, and a reference or link to where the document can be retrieved. If there is a need to repeat the same document in several categories, auditors are advised to conceive a document reference mnemonic and refer to multiple occurrences using this method.

To arrive at a comprehensive list of regulatory requirements can be time-consuming. In many cases the information that is required for auditors to describe repository activities and risks effectively may be only partially revealed in source documentation, but all documents that have a bearing on why or how something is done at the repository should be listed at this Stage.

5.8.7.1 T3: List your repository's strategic planning documents

Strategic planning documents can exist under various titles. Auditors are advised to look for procedural or operational manuals, refer to intranet or shared network storage facilities and ask the senior operational management for these documents.

To get started, it may be helpful to consider the current strategic focus of the repository and identify the strategic planning documents and executive statements that contribute to its establishment. It is also helpful to the repository's clients, customers and target audience to consider the policies and procedures geared towards serving these communities.

Policies explain why repositories carry out particular activities and, broadly speaking, how they should be carried out. All organisations have policies in place that have been approved by the organisation's management or that apply to its industrial or business domain as a whole. A policy may relate to a specific function, part of a function, aspects of several functions or all of an organisation's functions. Policy documents should provide information on specific activities undertaken by the organisation.

Procedures are often collected together in a manual that provides details of how an organisation carries out its functions at a very specific level. Manuals are often confined to one particular function, and contain procedures that relate to one activity or several activities. An individual procedure will generally relate to a particular aspect of an activity. Procedures manuals are useful for identifying components of activities. Policies and procedures relating to an organisation's unique functions or programmes should be available internally.

It is essential that auditors possess an understanding of the way their kind of organisation operates at the broadest level, as some policies and procedures may exist with global coverage and relevance.

Example Task Response Excerpt:

T3:	List your repository's strategic planning documents
Example:	Operational functions: Acquisition & Ingest
	Repository X: Core Activities (2005) http://www.xxx.org/policies/activities.pdf
	Operational functions: Preservation & Storage
	Repository X: Core Activities (2005) http://www.xxx.org/policies/activities.pdf
	Operational functions: Metadata management
	Repository X: Core Activities (2005) http://www.xxx.org/policies/activities.pdf
	Repository X Data Policy (2003) K:\Core_Documents\DataPolicy.rtf
	Operational functions: Access & Dissemination
	Repository X: Core Activities (2005) http://www.xxx.org/policies/activities.pdf
	Support functions: Organisation & Management
	Repository X: Core Activities (2005) http://www.xxx.org/policies/activities.pdf
	Repository X Risk Register (2006) Intranet/Risk/Risk_Register.html
	Support functions: Staffing
	Support functions: Financial management
	Repository X Risk Register (2006) Intranet/Risk/Risk_Register.html
	Support functions: Technical infrastructure & Security
	Repository X Risk Register (2006) Intranet/Risk/Risk_Register.html

5.8.7.2 T4: List the legal, regulatory and contractual frameworks or agreements to which your repository is subject

The requirements of the regulatory environment within which the repository functions can vary, often substantially, between different organisations. This section should include documents that are external to

the audited organisation, but have an influence upon the way in which it operates.

It may be easier to begin the analysis by identifying relevant legislation (including pending legislation) before going on to consider relevant regulatory instruments and contractual obligations of the organisation. The hierarchy of elements comprising the regulatory framework is likely to resemble the following:

- statute and case law and regulations;
- mandatory standards of practice;
- sector- or domain-specific regulations;
- contractual obligations and service level agreements.

Auditors can answer some simple questions to assist in the establishment of boundaries for the scope of analysis, and provide a degree of orientation to the landscape of influential legal acts:

- What type of organisation is the repository? For example, is it private, public, a department, a statutory body, a non-statutory body, a corporation, or a university?
- What does the repository do or what sector does it belong to? For example, what is the general area of business or the industry sector that the repository occupies (e.g. scientific research, pharmaceuticals, education) and major outputs, services and products provided by the repository?
- What legislation influences the role or the operation of the repository?
- What legislation is administered by the organisation?
- Has the repository contracted out any aspects of its business activity?
- Are any of the repository's business areas immersed in a demonstrable culture of litigiousness?

It is worth noting that legal acts have been created for a variety of other purposes and may have a bearing on the repository's work only in passing.

If the organisation is constituted under legislation, its functions and powers will be outlined in the current version of the relevant act. Significant terms will be defined, clarifying organisational purpose, and amendments will be detailed to illustrate whether the organisation's identity or business activities have been affected by legislative changes.

For organisations that were not established within legislation, auditors may need to look at a variety of other sources to obtain information about its origins or evolution. These may include:

- administrative arrangements orders;
- charters;

- media releases; and
- ministerial statements.

In addition to enabling legislation, organisations may be directly responsible for administering other pieces of legislation or satisfying unique obligations set out in legislation administered by other organisations. Legislation administered by the audited organisation can usually be found by exploring the results of annual reporting mechanisms.

Example Task Response Excerpt:

T4:	**List the legal, regulatory and contractual frameworks or agreements to which your repository is subject**
Example:	Operational functions: Acquisition & Ingest
	Data Protection legislation
	Intellectual property protection
	Electronic commerce and the civil and criminal legal framework
	Deposit agreement with depositor Z
	Operational functions: Preservation & Storage
	ISO 9001 quality management principles
	Operational functions: Metadata management
	Operational functions: Access & Dissemination
	Data Protection legislation
	Freedom of Information Legislation
	Privacy legislation, identity theft
	Intellectual property protection
	Electronic commerce and the civil and criminal legal framework
	EC Consumer Protection and Distance Selling Directive
	Data use license agreements
	Support functions: Organisation & Management
	ISO 9001 quality management principles
	Electronic commerce and the civil and criminal legal framework
	EC Electronic Signatures Directive

	Council of Europe, Convention on CyberCrime
	Support functions: Staffing
	Support functions: Financial management
	Support functions: Technical infrastructure & Security
	ISO 27001 information security management system

5.8.7.3 T5: List the voluntary codes to which your repository has agreed to adhere

This section should list documents that your repository has developed and enacted to manage and control the way the repository operates. These could include voluntary codes of best practice, codes of conduct and ethics, organisation's rules and procedural manuals, and any standards being adhered to or complied with.

Within this section, auditors should ask themselves the following questions:

- Are there standards that have been imposed upon or adopted by the repository? This may include mandatory and voluntary standards (or parts thereof) including best practice, technical or industry standards.
- Has the repository or any facet of its business been the subject of any recent internal or external audits? What standards were these audits based on?
- Does the repository have a formal compliance programme or strategies and/or procedures in place to ensure compliance with laws, standards and regulation?
- Does the repository already have a formal risk management programme in place?

Example Task Response Excerpt:

T5:	**List the voluntary codes to which your repository has agreed to adhere**
Example:	Operational functions: Acquisition & Ingest
	Repository X Operations Manual (2006) Intranet/Operations/OpManual.html Preferred Ingest File Formats (2006)
	Operational functions: Preservation & Storage

	Repository X Disaster Plan (2004) Contingency Plan (2005)
	Operational functions: Metadata management
	Recommended Data Documentation Standard (2003) ISO 15489 Records Management
	Operational functions: Access & Dissemination
	Support functions: Organisation & Management
	Support functions: Staffing
	Support functions: Financial management
	Support functions: Technical infrastructure & Security

5.8.7.4 T6: List any other documents and principles with which your repository complies

In case the previous questions did not exhaust the list of documents that are pertinent to how the repository operates, auditors should provide references to any additional documents below.

Example Task Response Excerpt:

T6:	**List any other documents and principles with which your repository complies**
Example:	Operational functions: Acquisition & Ingest
	Operational functions: Preservation & Storage
	Operational functions: Metadata management
	Operational functions: Access & Dissemination
	Support functions: Organisation & Management
	Support functions: Staffing
	Support functions: Financial management
	Support functions: Technical infrastructure & Security
	A common understanding recorded in an internal memorandum that staff should turn off their computer screens when not at their desks

5.8.8 What to do in the Event of Required Information Being Unavailable

Most of the information required in this Stage of the audit is or should be available internally within the repository or publicly. Should auditors have difficulties in gaining access to the relevant documents, they should contact their senior manager and explain the importance of being able to access them in order to complete the audit exercise.

Some documents that should be listed in this Stage may be confidential or commercially sensitive, such as example contracts and previous audit results, and they should be treated appropriately; for instance, their title should be rendered anonymous, and information about their physical location withheld.

Information provided by the auditor in this Stage will be referred to during the stages. However, if some source documents are unattainable or the list remains incomplete, auditors may not be able to identify some risks, most specifically those related to the inadequacy of organisational activities to fulfil the repository's regulatory requirements and other obligations.

5.8.9 What has been Provided by Other Repositories

Repositories operate with well-defined legal and regulatory frameworks. By way of example we provide for the UK a far from exhaustive list of relevant acts and sources of commitments that may form part of regulatory framework within which a repository in the UK would be likely to operate. Although the suggestions correspond principally to the UK context, auditors can extrapolate equivalencies within their own jurisdiction's legal and regulatory framework.

UK Acts of Parliament

- The Freedom of Information Act 2000
- The Data Protection Act 1998
- Electronic Communications Act 2003
- Human Rights Act 1998
- National Minimum Wage Act 1998
- Working Time Regulations 1998
- Employment Act 2002
- Disability Discrimination Act 1995
- Legal Deposit Libraries Act 2003
- Companies Act 1985
- Copyright, Designs and Patents Act 1988

UK Regulations

- Employment Equality Regulations 2003
- The Management of Health and Safety at Work Regulations 1999
- Consumers Regulations 2000
- UK Generally Accepted Accounting Principles (UK GAAP)

- The Privacy and Electronic Communications (EC Directive) Regulations 2003

European Directives, Regulations and Decisions

- Directive 2001/29/EC (European Copyright Directive)
- Fourth and Seventh Company Law Directives on annual and consolidated accounts

Standards

- ISO 9000:2000 Quality Management Systems Series
- ISO 27001:2005 Information technology — Security techniques — Information security management systems — Requirements

5.8.10 Comments

Auditors are encouraged to send comments, concerns or observations to the DCC/DPE audit and certification working group at feedback@repositoryaudit.eu.

5.8.11 Checklist

Before proceeding to the next Stage, auditors should:

- check with their repository's recordkeeping system to ensure that they have identified all the strategic planning documents the repository has in place;
- check whether the list of goals and objectives in Stage 1 requires any amendments based on the analysis of the documents identified and studied during this Stage;
- check that they can locate and access the source documents listed in this Stage, should the need to consult them arise in subsequent Stages.

This Stage is now complete and auditors should progress to the next Stage of the audit in order to identify the key activities, assets and systems the repository uses to achieve its goals and objectives, and their owners.

5.9 STAGE 3: IDENTIFY ACTIVITIES, ASSETS AND THEIR OWNERS

This is the third of the six stages of self-audit.

5.9.1 Aim of this Stage

The purpose of Stage 3 is to develop a conceptual model of what the repository does and how it does it, by examining its activities and work processes, key assets and technology, and the staff involved.

This Stage requires auditors to split the broad-level mission and goals of the repository into more specific activities or work processes that the repository carries out in order to achieve its aims. Each of these activities is usually carried out by a number of staff members, and an individual should be assigned with responsibility for this activity (called owner in this self-audit toolkit). Each activity is linked to one or more key assets of the repository. Furthermore, each activity is supported by a number of technological systems and solutions that members of staff rely upon. Technology, software and various support systems are included in the assets category in this self-audit. For example a web server may be used to offer one or more key repository services, including the dissemination of digital content to users by the user services department.

The next Stage of the self-audit process will identify risks that are associated with the activities, assets and their owners listed in this Stage. The risks are associated not only with activities and work processes but also with key assets and technologies that may be at risk or are crucial to the continued functioning of the repository.

5.9.2 Tasks Associated with this Stage

Throughout this task the auditor will develop a structured list of activities, assets and their owners that help the repository to achieve its stated goals and objectives. The organisation's mandate, goals and objectives will be used as reference material when compiling the list in this Stage, and the various internal planning and external regulatory documents should also be consulted throughout the process.

The compilation of the list is based on a table structure provided on the form T7 (see Appendix 1 of the self-audit toolkit).

5.9.3 Anticipated Results of this Stage

The list of repository activities, assets and their owners will form the main basis for identifying risks the repository is subject to. The comprehensiveness of the list prepared in this Stage plays a crucial role in achieving a complete list of potential risks at the next Stage.

The main output from this Stage will be a table listing key activities or work processes of the repository, assets that are linked to these activities, and people who are responsible for the activities and assets.

5.9.4 Where Does this Stage Fit Within the Overall Audit Process?

The compilation of the list of activities should be undertaken with consideration for the scope of the mandate, goals and objectives of the repository and of the contextual framework of regulatory requirements. The information derived from the previous Stages of the audit will be used as guidance and reference material for completing this Stage.

The list of key activities and assets developed in this Stage will form the basis for a subsequent risk identification and assessment exercise.

The list of the repository's key activities, assets, technology solutions and staff involved can be used as a separate output from the audit process to help the management of the repository work or as an inventory of assets.

5.9.5 What Resources are Required to Complete this Stage?

Anticipated Effort: 2-4 hours

Analysing the organisation's activities is a rigorous and resource-intensive process. This section of the self-audit is a crucial stage in order to arrive at a comprehensive list of risks that the repository is exposed to and has to manage.

The main time investment is expected to go into identifying the repository's activities and into considering activities, assets and staff as an interlinked organism. Unless existing and up-to-date business classification schemes and inventories of assets and technology are available, these will have to be created as part of this Stage.

Auditors can return to the list developed during this Stage at a later point during the assessment process in order to add to it or refine it.

Before starting Stage 3, auditors should:

- have a general understanding of the organisation and the contexts within which it operates;
- obtain managerial support to undertake the analysis of business activity;
- acquire a list of repository staff and their responsibilities;
- determine whether the organisation has previously analysed and documented its activities and work processes.

If the repository has been analysed for other purposes it may be possible to draw on the results of such work, rather than starting from scratch. Projects that may involve an analysis of activities include:

- business process re-engineering;
- imaging and work flow automation;
- activity-based costing or management;

- business classification development;
- quality accreditation;
- systems implementation.

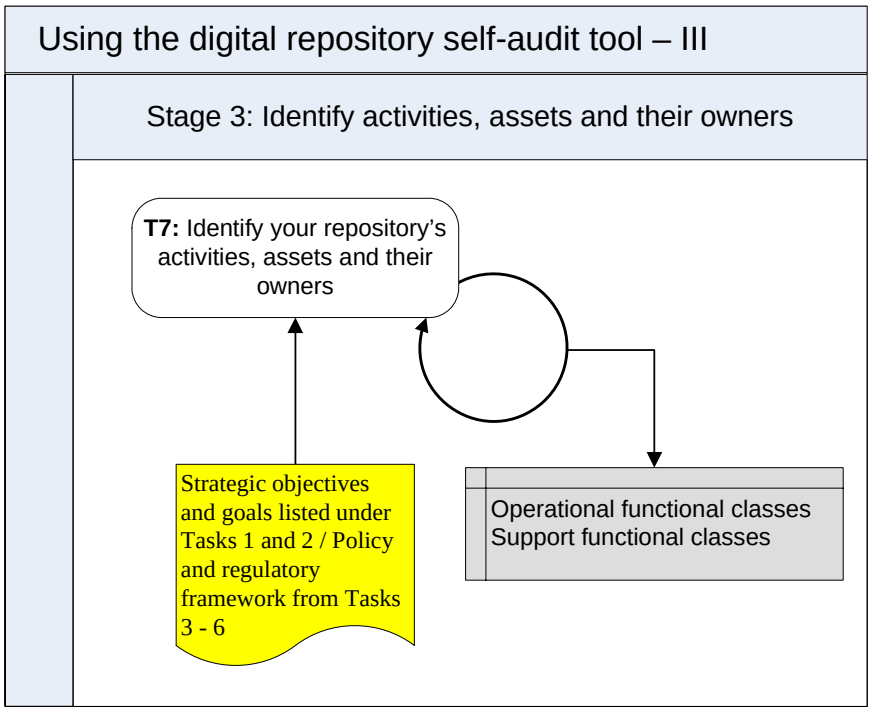
If the analysis arising from such projects is available, auditors will need to consider how, why and when the projects were undertaken to determine whether their findings are applicable for the purposes of this audit.

Lists, registers or inventories of assets and technology may have been compiled for various purposes during analyses of business, compliance studies and audits, contingency planning exercises, etc. Most organisations maintain an inventory of IT hard- and software and their licenses; inventories of other tangible assets (e.g. repository furniture) may be attainable from the finances or estates section of the organisation.

In order to complete Stage 3, auditors:

- must have access to internal documents, such as operational manuals, procedural guides, task and target lists, organisational structure charts, lists of assets, technology and systems;
- may need to have access to managerial and IT personnel with further knowledge of the activities, assets, technology and systems and their owners.

5.9.6 Diagram Depicting this Stage



5.9.7 Instructions for Completing the Stage

The two most commonly used methodologies for identifying functions and activities in an organisation are hierarchical analysis and process analysis.

Hierarchical analysis involves breaking down what the organisation does into a series of logical parts and sub-parts. This process is also known as 'functional analysis'. The process starts with a 'big picture' view of the organisation's business and breaks it down into more detailed component parts, which are, in descending order, functions, activities and transactions. A function is a high-level aggregate of the organisation's activities that is tied directly to the organisation's mandate. The major tasks performed by an organisation within the context of, and in order to accomplish, a function are called activities. A transaction is the smallest unit or level of activity.

In order to conduct the hierarchical analysis, auditors will need to consider:

- the organisation's charter or mission;
- what makes the organisation unique;
- what functions the organisation manages;
- what operations the organisation carries out;
- what actions the organisation is responsible for;
- how actions are carried out within the organisation;
- whether certain activities are confined to specific areas or programmes or shared across the entire organisation;
- how the organisation transacts business internally and with external clients and partners.

If the repository has a business or records classification scheme, auditors may use this as the basis for listing the activities. If a business classification scheme has not yet been developed, auditors may consider this as an additional value-added result of the self-audit.

For further details on the methodology of analysis for records classification, see the National Archives of Australia 'DIRKS Manual',[24] section B, or the Business Activity Structure Classification System (BASCS) Guidance offered by Collections Canada.[25] Both of these sources have been used for instructions for this Stage.

Whereas hierarchical analysis provides a useful overview of what the organisation does, process analysis looks in more detail at how it conducts its business and what assets, systems and people are involved in carrying out the activities. Process analysis, sometimes also referred to as sequential analysis, involves looking at the ways organisational tasks cut across functional and structural boundaries. To do this it is helpful to draw on the top-down hierarchical analysis and then start to investigate in detail how activities are carried out.

[24] http://www.naa.gov.au/recordkeeping/dirks/dirksman/step_B.html

[25] http://www.collectionscanada.ca/information-management/002/007002-2089-e.html

An asset is something that has value or utility for the organisation, its business activities and their continuity. Therefore, assets need protection to ensure correct activities and business continuity. The proper management and accountability of assets is vital, and should be a major responsibility of all management levels. There are many types of assets, including:

- information: databases and data files, contracts and agreements, system documentation, research information, user manuals, training material, operational or support procedures, business continuity plans, fallback arrangements, audit trails and archived information;
- software assets: application software, system software, development tools and utilities;
- physical assets: computer equipment, communications equipment, removable media and other equipment;
- services: computing and communications services, general utilities, e.g. heating, lighting, power and air-conditioning;
- processes: business processes, application-specific activities;
- people, and their qualifications, knowledge, skills and experience;
- intangibles, such as reputation and image of the organisation.

Inventories of assets help to ensure that effective asset protection takes place, and may also be required for other business purposes, such as health and safety, insurance or financial (asset management) reasons.

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.

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

Based on the mandate, goals and objectives identified in the previous Stages of the self-audit, auditors are required to list the activities within the repository. The goals and objectives, as well as the regulatory instruments that govern them, will be presented according to the operational and supporting functional classes. Auditors should list as many activities as possible at this Stage, identifying their owners, key assets that they are linked with, and supporting technological solutions.

Example Task Response Excerpt:

T7:	Identify your repository's activities, assets and their owners		
Functional Class:	**Acquisition and Ingest**	**Assets**	**Owners**
Activities:	Prepare deposit agreements with depositors	Deposit agreement text	Legal
	Agree submissions with depositors		Acquisition
	Sign submission agreements with depositors	Submission agreement text	Legal
	Transfer submissions via different communication channels	FTP server; DVD; submission control software solution	Acquisition
	Check transferred data for viruses	Virus control software; security of the processing area	IT
	...	...	...

5.9.8 What to do in the Event of Required Information Being Unavailable

The information on activities and assets of the repository should be made available to the auditor in a complete and unabridged form. If this proves difficult, senior management should be contacted and the necessary authorisations acquired to gain access to the required information. Further usage restrictions can be agreed for the list of activities and assets that is created in this Stage in order to protect the sensitive information it may contain. Not having or not being able to access the information on what the repository is doing can be considered as a considerable risk in and of itself.

The completeness of the list depends on the level of granularity and detail with which the activity and asset identification process is conducted. During this Stage, auditors are advised to give some consideration to the potential risks of the activities and assets that will be derived and listed during the subsequent Stage. The notion of what is perceived to be at risk will help to determine the level of granularity used in this Stage.

5.9.9 What Has Been Provided by Other Repositories?

The following generic list of activities and associated assets has been derived from an analysis of the TRAC check-list and the nestor criteria catalogue, and ISO 27001:2005 Information technology – Security techniques

– Information security management systems – Requirements. Auditors may wish to incorporate a selection of the following activity examples in their response or, if appropriate, to reword their own equivalent responses to correspond:

Functional Class*	Associated Activity(ies) and Asset(s)	Owner
S1. Organisation Management (S):	S1A1. Define mission statement and organisational objectives	Management
	Associated Assets: Mission statement;	
	S1A2. Plan for continuation of preservation activities beyond repository's lifetime	Management
	Associated Assets: Succession, contingency or escrow arrangements;	
	S1A3. Document and review identified community definition	Management
	Associated Assets: Identified community definition;	
	S1A4. Define, document and review policy for meeting identified community's understandability requirements	Management
	Associated Assets: Organisation's reputation;	
	S1A5. Establish and utilise mechanisms for soliciting feedback from identified community	Management
	Associated Assets: Email; Other feedback mechanisms; trustworthiness	
	S1A6. Define significant characteristics of digital content for information preservation	Management
	Associated Assets:	
	S1A7. Define, document and review policies and procedures governing each aspect of business activities	Management
	Associated Assets: Policy and procedure documents;	
	S1A8. Negotiate and fulfil legal agreements with producers, depositors and users	Management
	Associated Assets: Contracts;	
	S1A9. Fulfil responsibilities related to	Legal

	legislative or regulatory requirements	
	Associated Assets:	
	S1A10. Utilise means for organisational assessment, including external and internal audit and risk analysis	Management
	Associated Assets: Certificates awarded; risk register; organisational reputation	
S2. Staffing (S):	S2A1. Appoint a sufficient number of appropriately qualified staff	Personnel / HR
	Associated Assets: Staff;	
	S2A2. Define roles, responsibilities and their relationships	Personnel / HR
	Associated Assets: Staff; organisational overview documents	
	S2A3. Define and implement mechanisms to identify and satisfy ongoing staff training requirements	Personnel / HR
	Associated Assets: Resources allocated to training; staff	
	S2A4. Utilise means for staff assessment, including external and internal audit and risk analysis	Management
	Associated Assets: Certificates awarded; risk register; organisational reputation	
S3. Financial Management (S):	S3A1. Define, implement and review short and long-term business plans	Management
	Associated Assets: Business planning documents; turnover;	
	S3A2. Monitor for and invoke means to address financial shortfalls	Management / Budget
	Associated Assets: Turnover; financial planning	
	S3A3. Comply with jurisdictional finance laws	Legal
	Associated Assets:	
	S3A4. Utilise means for financial assessment, including external and internal audit and risk	Management

	analysis	
	Associated Assets: Financial audit outcomes; risk register; organisational reputation	
S4. Technology Infrastructure and Security (S):	S4A0. Define a strategic IT plan	Technical
	Associated Assets: IT planning documents	
	S4A0.1. Define the information architecture	Technical
	Associated Assets: System hardware, software and communications infrastructure	
	S4A1. Monitor to ensure ongoing suitability and appropriateness of hardware and software infrastructure	Technical
	Associated Assets: Software and Hardware	
	S4A2. Implement measures to perform hardware and media refreshment	Technical
	Associated Assets:	
	S4A3. Maintain systems, installing security patches and software updates when appropriate	Technical
	Associated Assets: Software update mechanisms	
	S4A4. Test effects of critical system changes, reversing them if necessary	Technical
	Associated Assets: Test software and hardware environment	
	S4A5. Implement security measures within IT and physical infrastructure	Technical / Physical Security
	Associated Assets: Security infrastructure (e.g. security doors; security staff; passcards; encryption software; passwords; security testing tools)	
	S4A6. Maintain redundant data and storage and offsite backups	Technical
	Associated Assets: Backup mechanisms; backup tapes;	
	S4A7. Conceive and test disaster recovery and business continuity plans	Management
	Associated Assets: Continuity, disaster or exit	

	plans	
	S4A8. Utilise means for technical and security assessment, including external and internal audit and risk analysis	Management
	Associated Assets: Certificates awarded; risk register; organisational reputation	
C1. Acquisition and Ingest (C):	C1A1. Define acceptable submission format(s)	Ingest
	Associated Assets: Submission package definition;	
	C1A2. Monitor, record and where possible validate integrity of received content	Ingest
	Associated Assets: Checksums; algorithms for checksum comparison	
	C1A3. Verify completeness and correctness of received content	Ingest
	Associated Assets: Digital objects	
	C1A4. Establish physical and technical control over received content	Ingest
	Associated Assets: Digital objects	
	C1A5. Establish mechanisms to report back to producers and depositors to indicate acceptance or rejection of preservation responsibility	Ingest
	Associated Assets: Email; other reporting mechanisms	
	C1A6. Perform transformation of submitted content to archival form	Ingest
	Associated Assets: Transformation tools; Digital objects	
	C1A7. Dispose of submissions that will not be transformed into archival form	Ingest
	Associated Assets: Disposal tools	
	C1A8. Utilise means for functional assessment, including external and internal audit and risk analysis	Management / Ingest
	Associated Assets: Certificates awarded; risk register; organisational reputation	

C2. Preservation and Storage (C):	C2A1. Assign unique, persistent identifiers to archived content	Preservation
	Associated Assets: Identifier scheme; digital objects	
	C2A2. Document all changes to archived content	Preservation
	Associated Assets: Change management tools; digital objects	
	C2A3. Monitor and validate integrity of archived content at object and collection level	Preservation
	Associated Assets: Checksums; checksum comparison tools; digital objects	
	C2A4. Implement and review strategies for physical archival storage and migration	Preservation
	Associated Assets: Migration tools; media; digital objects	
	C2A5. Define, review and implement preservation plans	Preservation
	Associated Assets: Preservation strategies; preservation tools;	
	C2A6. Utilise means for functional assessment, including external and internal audit and risk analysis	Management / Preservation
	Associated Assets: Certificates awarded; risk register; organisational reputation	
C3. Metadata Management (C):	C3A1. Acquire preservation metadata for archived content	Documentation
	Associated Assets: Preservation metadata records	
	C3A2. Establish, document and monitor semantic and technical context necessary to ensure understandability of archived objects	Documentation
	Associated Assets: Representation information records; registry of representation information	
	C3A3. Capture or create appropriate descriptive metadata to facilitate discovery	Documentation

	Associated Assets: Descriptive metadata records	
	C3A4. Maintain referential integrity between metadata and archived content	Documentation
	Associated Assets: Digital objects; metadata records; software for maintaining associations	
	C3A5. Utilise means for functional assessment, including external and internal audit and risk analysis	Management / Documentation
	Associated Assets: Certificates awarded; risk register; organisational reputation	
C4. Access and Dissemination (C):	C4A1. Provide mechanisms to discover, select and access content	Dissemination
	Associated Assets: Dissemination systems (web server; application)	
	C4A2. Implement authentication and authorisation subsystems to reflect agreed access rights and restrictions	Dissemination
	Associated Assets: Authentication and authorisation systems; contracts	
	C4A3. Perform transformation of archived content to dissemination form (as requested by users, expected by the user community)	Dissemination
	Associated Assets: Transformation mechanisms	
	C4A4. Disseminate a complete and authentic object as originally submitted (that is traceable to originally submitted, corresponding object)	Dissemination
	Associated Assets: Digital object; comparison mechanisms	
	C4A5. Utilise means for functional assessment, including external and internal audit and risk analysis	Management / Dissemination
	Associated Assets: Certificates awarded; risk register; organisational reputation	

* Note: (C) = Operational Functional Class, (S) = Supporting Functional Class

5.9.10 Discussion

It is recommended that an analysis of the adequacy of the organisational structure and the allocated resources is also undertaken. The comparison of repository's objectives and activities and assets will be revealing in terms of potential risks.

5.9.11 Comments

Auditors are encouraged to send comments, concerns or observations to the DCC/DPE audit and certification working group at feedback@repositoryaudit.eu.

5.9.12 Checklist

Before proceeding to the next stage, auditors should ensure that they have:

- identified the repository's activities, assets and their owners;
- where necessary, updated the list of goals and objectives and regulatory documents created during previous Stages;
- validated the findings with senior management.

5.10 STAGE 4: IDENTIFY RISKS

This is the fourth of the six stages of self-audit.

5.10.1 Aim of this Stage

The aim of this Stage is to derive from organisational activities and assets a comprehensive selection of pertinent risks faced by the repository. Some risks can be derived from examining the mandate and objectives, regulatory environment and the model of the repository's work (activities, assets, staffing, technology solutions). This principal outcome is the definition of an organisational 'worry radius', detailing the parameters within which risk management must be undertaken. The assessment of risk impact and likelihood will be undertaken during the following Stage of the self-audit process.

5.10.2 Tasks Associated with this Stage

Activities and assets identified within the previous Stage will inevitably be associated with vulnerabilities, characterised within the context of this toolkit as risks. Throughout this task, auditors will develop a structured list of risks, according to organisational objectives and the activities and assets that contribute towards their completion. There is no single universal methodology for identifying risks. The most valuable approach is to list all potential risks in a brain-storming exercise before refining, grouping and splitting them as is deemed appropriate. Once auditors have developed an initial list they will be exposed to further risk examples originating from both external sources and assessments undertaken by comparable organisations. Self-auditors can use these risks to fill any remaining gaps and ensure that a comprehensive range of risks is documented.

The adjacent forms provide auditors with an opportunity to describe pertinent risks, and also to assign a risk owner (as a default value, the identified owner of the particular asset or activity should be provided) and risk stakeholders. Auditors may also document risk relationships by detailing the risks associated with each entry.

When deriving risks, we recommend that auditors consider the following kinds of risks associated with particular activities and assets:

- The assets or activities fail to achieve or adequately contribute towards the relevant organisational goal(s) and objectives.
- Internal threats present obstacles to the success of one or more activities.
- External threats present obstacles to the success of one or more activities.
- Threats result in unauthorised disclosure, modification, corruption, destruction and unavailability or loss of repository's assets.

Risks should be considered in terms of a possible effect, rather than dwelling on possible causes. These will be addressed in the manifestations of the risk that will be subsequently documented.

5.10.3 Anticipated Results of this Stage

This is the first of three Stages that represent the risk-centric activity of the self-audit process. In one sense this is the most critical, since it demands that auditors derive a comprehensive selection of risks faced within every aspect of the repository. Anything less than this outcome will render the work that follows incomplete.

The following results should be achieved before moving on to the next Stage of the audit process:

- a comprehensive list of risks categorised according to functional class, organisational objectives and the activities and assets identified to ensure their completion;
- an initial insight into pertinent relationships between identified risks;
- for each risk, a subset of attributes describing, as a minimum, its owner and type classification, and optionally its relationships with other risks (the latter will be subject to continued development within the subsequent self-audit Stage).

The list of risks derived during this Stage will be developed further in subsequent Stages of the self-audit process; in particular, each risk will be subject to more detailed individual description. The output represents the nascent risk register, although, until appropriate risk assessments are undertaken, the value of the resource in this initial form is negligible.

5.10.4 Where Does this Stage Fit Within the Overall Audit Process?

This Stage takes the organisational description constructed throughout previous Stages of the audit process and derives a comprehensive catalogue of risks relevant to the self-audited repository.

Risks identified during this Stage will be subject to assessment and more detailed description, with risk relationships further developed and documented.

5.10.5 What Resources are Required to Complete this Stage?

Anticipated Effort: 4 hours

Stage 4 of the self-audit is likely to be quite time-consuming; auditors must be confident of the comprehensiveness of their response before advancing to Stage 5. It is feasible that it will be necessary to return to this Stage to implement corrections or append additional risks, and this is quite cceptable (indeed, it is encouraged). The straightforwardness with which risks can be derived will be strongly influenced by the degree of granularity with which the auditor has defined activities and assets. Risks might be derived more efficiently from a greater number of more finely defined activities than from a handful of very broadly stated examples. In order to facilitate this process, it is suggested that the level at which activities and assets are provided should correspond to that of the examples provided within the previous Stage.

Auditors can return to this Stage later and add or amend information, should the need arise.

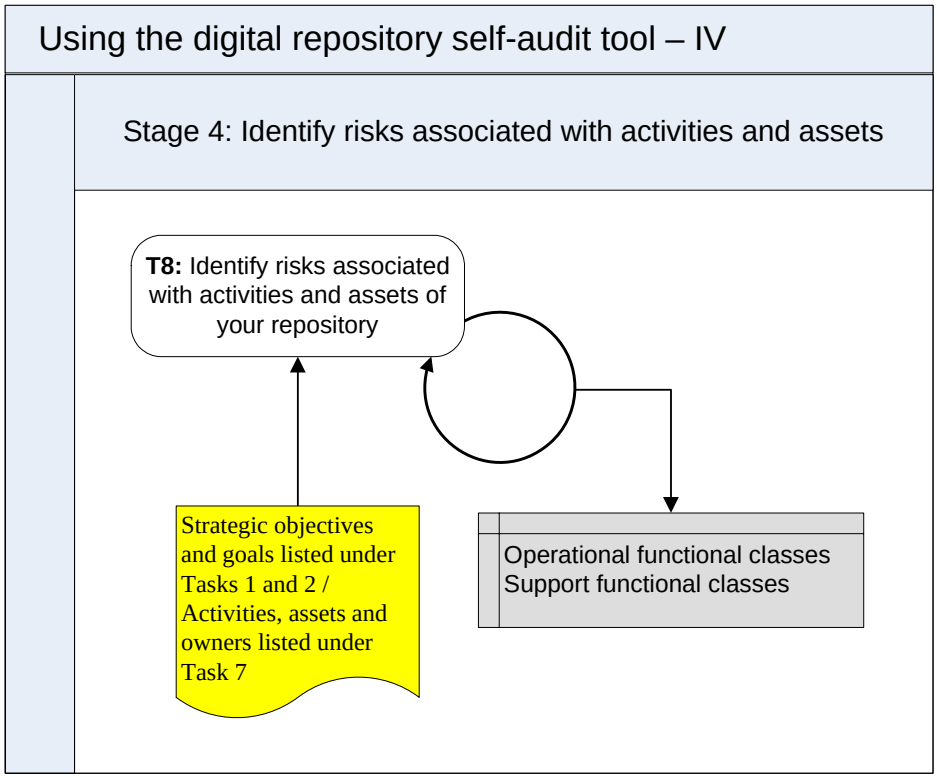
Before starting Stage 4, auditors should:

- engage with appropriate repository colleagues to seek an endorsement of the completeness and correctness of identified activities and assets;
- solicit suggestions from appropriate repository colleagues of pertinent risks, classified according to their association with particular activities and assets;
- refer to the results of any risk-assessment exercises that have already been undertaken within the organisation, or to any continuity plans already conceived.

In order to complete Stage 4, auditors will need:

- access to internal policy documentation;
- access to external documents and sources, such as legislation, standards, codes of practice;
- access to additional repository personnel with further knowledge of risks associated with particular aspects of the repository.

5.10.6 Diagram Depicting this Stage



5.10.7 Instructions for Completing the Stage

The task of deriving risks from organisational assets and activities is straightforward, but the development of a comprehensive response may require considerable effort.

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

The risk derivation process is structured in terms of the functional classes; within each of these, the inherent organisational objectives, and the associated assets and activities that contribute towards their success are mapped to risks and groups of risks. Self-auditors should refer to their responses from the previous three Stages in order to structure and complete a picture of organisational risk.

Risks are not only linked with activities in general, but may also be included in the activity itself, its objects/deliverables and the way the activity is organised. Furthermore risks can also be associated with lack of staff, unskilled staff, lack of knowledge or lack access to relevant knowledge bases, and lack of appropriate tools.

Example Task Response Excerpt:

T8:	**Identify risks associated with activities and assets of your repository**	
Functional Class:	**Acquisition and Ingest**	**Owner**
Activities & Risks:	Prepare deposit agreements with depositors	Legal
	Agree submissions with depositors	Acquisition
	Sign submission agreements with depositors	Legal
	Transfer submissions via different communication channels	Acquisition
	Check transferred data for viruses	IT
	...	...

Risk Identifier:	R1	
Risk Name:	Legal liability for breach of contractual obligations	
Related Activities:	• Prepare deposit agreements with depositors • Sign submission agreements with depositors	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	X
	Operations and service delivery	
	Hardware, software or communications equipment and facilities	
Owner:	Legal	
Stakeholders:	Depositor; Producer	
Related Risks:	R5, R6	
Risk Identifier:	R2	
Risk Name:	Structural non-validity or malformation of received packages	
Related Activities:	Agree submissions with depositors	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	
	Operations and service delivery	X
	Hardware, software or communications equipment and facilities	
Owner:	Ingest, Preservation	
Stakeholders:	Depositor; Producer	
Related Risks:	R3, R4	

5.10.8 What to do in the Event of Required Information Being Unavailable

The absence or non-availability of internal policy and external regulatory documentation and of staff capable of describing pertinent organisational risks should itself be regarded as a potentially serious risk to the repository's ongoing viability. This should therefore be documented, prior to its assessment and the conception of avoidance and treatment mechanisms within the subsequent Stages of the audit process.

5.10.9 What has been Provided by Other Repositories?

The following generic list of risks has been derived from an analysis of activities intrinsic to the TRAC and *nestor* check-lists and the ISO 27001 standard. Auditors may wish to incorporate a selection of the following risk examples within their response or, if appropriate, to re-word their own equivalent responses to correspond with these.

Please note, although the risks presented here are categorised according to functional class, some may conceivably relate to more than one group, and the possibility of this should not be disregarded.

No.	*Risk Title*
Organisation Management	
R01	Management failure
R02	Loss of trust
R03	Activity is overlooked or allocated insufficient resources
R04	Business objectives not met
R05	Repository loses mandate
R06	Community requirements change substantially
R07	Community requirements misunderstood or ineffectively communicated
R08	Enforced cessation of repository operations
R09	Community feedback not received
R10	Community feedback not acted upon
R11	Business fails to preserve essential characteristics of digital information
R12	Business policies and procedures are unknown
R13	Business policies and procedures are inefficient
R14	Business policies and procedures are inconsistent or contradictory
R15	Legal liability for IPR infringement
R16	Legal liability for breach of contractual responsibilities
R17	Legal liability for breach of legislative requirements
R18	Liability for regulatory non-compliance
R19	Inability to evaluate repository's successfulness
R20	False perception of the extent of repository's success
Staffing	
R21	Loss of key member(s) of staff
R22	Staff suffer skill loss
R23	Staff skills become obsolete
R24	Inability to evaluate staff effectiveness or suitability
Financial Management	
R25	Finances insufficient to meet repository commitments
R26	Misallocation of finances
R27	Liability for non-adherence to financial law or regulations
R28	Financial shortfalls or income restrictions
R29	Budgetary reduction
Technical Infrastructure and Security	
R30	Hardware failure or incompatibility

R31	Software failure or incompatibility
R32	Hardware or software incapable of supporting emerging repository aims
R33	Obsolescence of hardware or software
R34	Media degradation or obsolescence
R35	Exploitation of security vulnerability
R36	Unidentified security compromise, vulnerability or information degradation
R37	Physical intrusion of hardware storage space
R38	Remote or local software intrusion
R39	Local destructive or disruptive environmental phenomenon
R40	Accidental system disruption
R41	Deliberate system sabotage
R42	Destruction or non-availability of repository site
R43	Non availability of core utilities (e.g. electricity, gas, network bandwidth, water)
R44	Loss of other third-party services
R45	Change of terms within third-party service contracts
R46	Destruction of primary documentation
R47	Inability to evaluate effectiveness of technical infrastructure and security
Acquisition and Ingest	
R48	Structural non-validity or malformation of received packages
R49	Incompleteness of submitted packages
R50	Externally motivated changes or maintenance to information during ingest
R51	Archival information cannot be traced to a received package
Preservation and Storage	
R52	Loss of confidentiality of information
R53	Loss of availability of information and service
R54	Loss of authenticity of information
R55	Loss of integrity of information
R56	Unidentified information change
R57	Loss of non-repudiation of commitments
R58	Loss of information reliability
R59	Loss of information provenance
R60	Loss or non-suitability of backups
R61	Inconsistency between redundant copies
R62	Extent of what is within the archival object is unclear
R63	Inability to validate effectiveness of ingest process
R64	Identifier to information referential integrity is compromised
R65	Preservation plans cannot be implemented
R66	Preservation strategies result in information loss
R67	Inability to validate effectiveness of preservation
R68	Non-traceability of received, archived or disseminated package
Metadata Management	
R69	Metadata to information referential integrity is compromised

R70	Documented change history incomplete or incorrect
R71	Non-discoverability of information objects
R72	Ambiguity of understandability definition
R73	Shortcomings in semantic or technical understandability of information
Access and Dissemination	
R74	Non-availability of information delivery services
R75	Authentication subsystem fails
R76	Authorisation subsystem fails
R77	Inability to validate effectiveness of dissemination mechanism
R78	Loss of performance or service level

5.10.10 Comments

Auditors are encouraged to send comments, concerns or observations to the DCC/DPE audit and certification working group at feedback@repositoryaudit.eu.

5.10.11 Checklist

Before proceeding to the next Stage, please check that you have:

- documented a comprehensive selection of risks corresponding to each functional class, and associated with organisational activities and assets.

5.11 STAGE 5: ASSESS RISKS

This is the fifth of the six stages of self-audit.

5.11.1 Aim of this Stage

The aim of this Stage is to characterise the risks and risk relationships derived within the previous Stage, and to assess the severity of each. Each risk must be enriched with a number of additional attributes; among the most significant are values describing the probability and potential impact of each, which cumulatively offer a quantitative insight into the overall riskiness of the repository's business activities.

5.11.2 Tasks Associated with this Stage

The fundamental constituents of risk assessment are the probability and potential impact associated with each specific risk. The simple product of these values can be described as that risk's severity. These values may be influenced by the context within which the organisation operates, by the infrastructures, policies and mechanisms maintained by the organisation, and by relationships that exist with other associated risks.

Auditors must undertake a comprehensive risk assessment for each of the risks identified within the previous Stage. This is mainly a serial process, with the completion of a separate risk description form (see form T9 in Part III of the report) corresponding to each of the predefined risks. For each risk, auditors are required to provide the following:

Risk Characteristics	*Definition of Risk Characteristics*
Risk Manifestations	Examples of situations within which this risk might feasibly execute; it is anticipated that this will be provided mainly in terms of specific threats (things that could happen or not happen) and vulnerabilities (characteristics of the organisation that expose it to risks in particular circumstances).
Risk Probability Score	Corresponding to the values detailed within the grid below, this indicates the perceived likelihood of the execution of this particular risk.
Risk Impact Score	Again, corresponding to one of the values within the grid below, this indicates the perceived impact of the execution of this risk. Impact is linked with loss of the authenticity and understandability of archived digital objects, which is regarded as an ultimate practical expression of failure for repositories that are auditable using this toolkit.
Risk Severity	A derived value, this represents the product of probability and potential impact scores.
Risk Relationships	Within this field, auditors should describe each of the

	risks with which the current risk has relationships.
Risk Escalation Owner	The individual who assumes ultimate responsibility for the risk in the event of the stated risk owner relinquishing control.

Once auditors have completed risk assessments for each relevant risk, they will be exposed to further examples originating from both external sources and assessments undertaken by comparable repositories. Auditors may wish to refer to these examples in order to be reassured of the completeness and correctness of their responses.

5.11.3 Anticipated Results of this Stage

This is the second of three Stages that represent the risk-centric activity of the self-audit process. Assuming the completion of a comprehensive list of risks, this will enable auditors to develop an understanding of the highest-priority risks facing their organisation, and of where the most profound threats lie.

The following results should be achieved before moving on to the next Stage of the audit process:

- Each of the previously listed risks should be characterised according to their probability and potential impact and in terms of their relationships with other risks.
- Categorisations already applied according to functional class, organisational objectives and the activities and assets identified to ensure their completion will persist, but auditors may also group risks according to other characteristics, most notably risk relationships.
- For each risk, a quantitative severity score will be calculated based on its anticipated likelihood and potential impact scores.

5.11.4 Where Does this Stage Fit Within the Overall Audit Process?

This Stage builds upon the list of risks identified within the previous Stage, requiring auditors to undertake assessments of each of the risks facing their organisation.

Once risks are assessed, the subsequent Stage will invite auditors to describe their currently installed and proposed mechanisms for risk management. This will incorporate methods for both risk avoidance (to limit probability) and risk treatment (to limit potential impact). To some extent the current Stage presupposes a consideration of existing management measures that are in place; any assessment of risk likelihood or impact cannot be divorced from the control infrastructures that are already in place. It is difficult to conceive of neutral values for either attribute, such are their dependencies on the context within which they arise. The 'naturally occurring' likelihood of repository documentation being destroyed is very high if one doesn't consider the fact that all capable

organisations will ensure that a roof is installed to provide protection from rain damage. Nevertheless, Stage 6 makes references to all management measures much more explicit, and auditors will have the opportunity to revise their probability and impact assessment at that point.

5.11.5 What Resources are Required to Complete this Stage?

Anticipated Effort: 4 hours

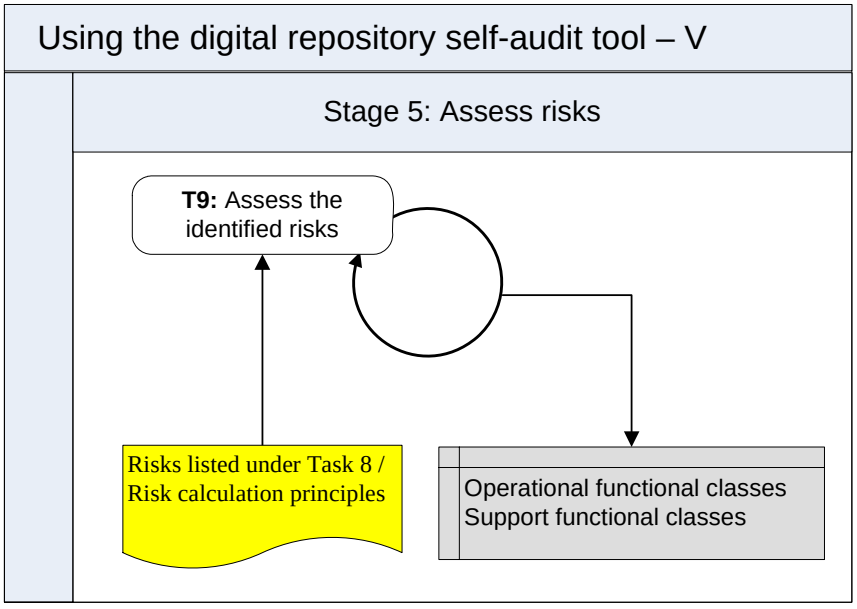
Before starting Stage 5, auditors should:

- engage with appropriate repository colleagues to seek an endorsement of the completeness and correctness of identified risks.

In order to complete Stage 5, auditors will need:

- access to internal policy documentation that describes risk avoidance and treatment mechanisms;
- access to internally or externally generated documentation that provides an evidence base or justification for probability or potential impact values;
- access to external documents and sources, such as legislation, standards, codes of practice;
- access to additional repository personnel with knowledge of risks associated with particular aspects of the repository.

5.11.6 Diagram Depicting this Stage



5.11.7 Instructions for Completing the Stage

5.11.7.1 T9: Assess the identified risks

For each stated risk, self-auditors should complete a risk table entry, adding to each risk:

- example manifestations of the risk;
- the probability of the risk's execution;
- the potential impact of the risk's execution;
- specific relationships that the risk has with other risks;
- the risk escalation owner, who assumes ultimate responsibility for the risk;
- the severity of the risk, a quantification of its seriousness, derived as the product of probability and potential impact.

By providing example manifestations of each risk, it is hoped that auditors will develop an increased understanding of their probability and potential impact. In addition, it is anticipated that better understanding of the circumstances within which risks occur will facilitate the later process of conceiving effective avoidance and treatment mechanisms. Auditors should list the kinds of threats and vulnerabilities that lead to the execution of particular risks. This entry may incorporate multiple examples; the auditor should continue when he or she feels confident that the potentially diverse circumstances within which a risk can exist have all been considered.

Probability is an expression of the likelihood of a particular risk executing. This is expressed in terms of a number of occurrences within a particular period of time. Any one of six individual probability values may be selected. The minimum probability score (the 'least likely' response) is described as minimal probability, and this is appropriate for risks that will execute once every one hundred years, or less often. The highest probability risks will be expected to execute more than once per month. As well as supplying a numerical index that corresponds to the appropriate probability description, auditors should offer a justification for their selection. This may be a reference to experience accrued or evaluations undertaken within the organisation itself or to work that has been undertaken externally. Wherever possible, the justification should refer to documentary evidence that supports the chosen value. As discussed above, any assessment of risk likelihood or impact cannot be divorced from the control infrastructures that are already in place, and therefore probability should be considered with reference to existing risk avoidance mechanisms. These will be elaborated further in the next Stage of the assessment process.

The self-audit toolkit considers risk probability according to the following scale:

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**

Risk impact is often measured only in terms of direct costs or financial loss, but, when assessing an organisation that deals with preserving digital information, the direct financial impact is probably not the most insightful measure. In a digital repository, the financial loss can occur through loss of information, unwarranted access to information, or preservation mismanagement. A repository's ability to provide access to authentic and understandable digital objects should be considered as the most critical factor in determining risk impact. Auditors should therefore only consider risk impact in the following areas initially:

- the impact on repository staff or public well-being;
- the impact of damage to, or loss of, premises, technology or information assets;
- the impact of breaches of statutory duties or regulatory requirements;
- damage to reputation of repository;
- damage to financial viability of repository;
- deterioration of product or service quality of repository;
- environmental damage.

Given these risk areas, it is the auditors' responsibility to derive the potential impact in terms of loss of digital object authenticity and understandability. From the perspective of this assessment tool, loss of these characteristics will represent the ultimate expression of repository failure. Again, since risk impact cannot be realistically considered in complete isolation, the chosen value should take into account any existing risk treatment mechanisms available to the repository. These will be further elaborated on in the next Stage of the assessment process.

The potential impact of risks is classified according to the following scale:

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

Once more, as well as supplying a numerical index corresponding to the appropriate impact definition, auditors should offer a justification for their selection. As with probability, this may be an internal or external expression, and should preferably refer to documentation capable of supporting the chosen value.

Relationships between risks may demonstrate one or more of the following characteristics.

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

In practical terms, such situations are unlikely – the allocation of more resources to treat or avoid any risk will in almost every case mean that less is available to allocate elsewhere. In this sense at least, every risk has an inversely attuned relationship with every other, except where risk treatment strategies benefit the management of other risks, and the relationship is complementary. Relationship instances may be unidirectional or bidirectional, they may be hierarchical, they may have variable strengths of risk bonding, and they may involve two or more partner risks.

Within each risk's relationship field auditors should document (using short risk identifiers) the risks with which a relationship is shared, describing the nature of that relationship and its consequences in terms of potential variation in probability, impact or manageability.

Risk escalation owners should subsequently be documented; these are the individuals with responsibility to deal with a particular risk, and the point of last resort for its management. In almost all cases this will be the same as the original activity and risk owner, but where accountability can be traced beyond this initial person this is the appropriate place to describe this chain.

The final field, the severity of the risk, is simply derived as the product of the chosen probability and impact values. Where risk relationships introduce potential ambiguity, the extent to which the risk's severity might vary should be described.

T9:	**Assess the identified risks**	
Risk Identifier:		
Risk Name:		
Risk Description:		
Example Risk Manifestation(s):		
Date of Risk Identification:		
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	
	Operations and service delivery	
	Hardware, software or communications equipment and facilities	

Owner:	
Escalation Owner:	
Stakeholders:	
Risk Relationships:	
Risk Probability:	
Risk Potential Impact:	
Risk Severity:	

5.11.8 What to do in the Event of Required Information Being Unavailable

Within many organisations it is unlikely that information will be available to explicitly indicate risk probability or potential impact. Auditors must therefore derive their responses from a range of influential sources. With respect to probability, the first consideration will be the historical experiences of the organisation. Risks that have executed frequently in the past must be regarded as likely unless circumstances surrounding and directly influencing that risk have changed. For instance, if in the recent past (last year of operations) organisations have experienced failure of hardware at least once per month, that will be an extremely significant factor in determining the organisation's probability response for that risk, unless replacement systems have been installed or the causes of the problems have been investigated and addressed appropriately. For risks that have executed at varying intervals, organisations should determine the mean time between occurrences since the most recently introduced avoidance mechanisms were put to the test. The calculation is roughly one of *mean_historical_probability – avoidance_offset*.

Potential impact can in many cases be derived similarly – for those risks that have executed in the past organisations can simply identify the impact that was recorded at the time. Assuming that other contextual variables remain consistent, they can then deduce a similar potential impact for the subsequent execution of that risk. If risk treatment mechanisms have been introduced since the most recent execution of the risk, these should be taken into account. For risks that have executed on multiple occasions in the past, organisations should calculate the mean impact of execution since the most recently introduced treatment mechanisms were put to the test. This calculation is roughly one of *mean_historical_impact – treatment_offset*.

In many more cases (particularly those risks with the most devastating degree of severity), organisations themselves will have little or no experience of the execution of those risks. It is in such circumstances that auditors are required to look beyond their own organisation at the experience of other organisations and the testbed work being done within the community. For many risks a great deal of work has been conducted. For instance, media failure is a well-researched topic and organisations

should be capable of identifying considerable amounts of literature upon which they can base their probability estimates for this risk. In other cases comparatively little documentation exists. Wherever possible, auditors should seek evidential assurances for their risk assessments. This may involve consultation with various communities. Auditors based at repositories in high-risk tornado hotspots for instance should refer to local meteorological evidence as a basis for their response. The experiences of other comparable organisations are another useful place from which to derive assessments relevant to the specific audited organisation. As this toolkit evolves and is used increasingly, it is expected that the experiences of comparable organisations will be made available anonymously, since it is acknowledged that many organisations will seek to withhold information about the problems they have experienced and disasters that have befallen them. It is anticipated that this will be especially true with regard to organisational accounts of the impact that particular risks have had.

5.11.9 What has been Provided by Other Repositories

Particular risks and their significance will vary from repository to repository. As a starting point, a list of generic risks is proposed (in Appendix 2 of this report), which has been identified through the review of published documentation and as a part of the test audits conducted. In subsequent drafts of this self-audit toolkit, it is intended to continue to enhance this list and the associated descriptive forms. Feedback on the risks from users of this toolkit, either through recommending additions to the list or helping to refine the descriptions of risks listed here, is very welcome. No particular order is currently presupposed in the interests of facilitating contributions. Only the title, dependencies, functional class(es) and categories of the risk are currently being completed, although comprehensive risk attributes will be provided for those that are included in the published document.

Other risks identified in the previous section are documented below. Each is presented as a table with an example risk description including typical entries for, among other things, manifestation examples, probability and potential impact. These risk attributes may be incorporated into a repository's response, or used to derive subjectively applicable responses for the organisation undergoing self-audit.

Please refer to Appendix 3 to see example risk description tables.

5.11.10 Comments

Auditors are encouraged to send comments, concerns or observations to the DCC/DPE audit and certification working group at feedback@repositoryaudit.eu.

5.11.11 Checklist

Before proceeding to the next Stage, auditors should ensure that:

- each of the previously listed risks is characterised according to its probability and potential impact;
- each risk is accompanied by details of example circumstances within which it may execute;
- for each risk, relationships with other risks are documented, along with details of their potential influence on risk probability, impact and manageability;
- escalation owners are identified;
- for each risk, a quantitative severity score is calculated based on its anticipated likelihood and potential impact scores, with potential fluctuation based on risk relationships also documented.

5.12 STAGE 6: MANAGE RISKS

This is the final of the six stages of self-audit.

5.12.1 Aim of this Stage

A fundamental imperative with respect to this work is that 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. This should consider the risk's potential impact, its frequency, its owners and its stakeholders. Risk mitigation strategies and tasks should be assigned, with accompanying deadlines for achieving predefined targets.

Risks can be managed through a combination of prevention and detection controls, avoidance tactics and acceptance, or by transference to another organisation. There are several strategies that an organisation can pursue to deal with the negative impact of identified risks. The Australian and New Zealand standard AS/NZS 4360:2004 *Risk management* lists the following options:

- 'Avoid the risk by deciding not to start or continue with the activity that gives rise to the risk (where this is practicable). Risk avoidance can occur inappropriately if individuals or organizations are unnecessarily risk-averse. Inappropriate risk avoidance may increase the significance of other risks or may lead to the loss of opportunities for gain.
- Change the likelihood of the risk, to reduce the likelihood of the negative outcomes.
- Change the consequences, to reduce the extent of the losses. This includes pre-event measures such as reduction in inventory or protective devices and post-event responses such as continuity plans.
- Share the risk. This involves another party or parties bearing or sharing some part of the risk, preferably by mutual consent. Mechanisms include the use of contracts, insurance arrangements and organizational structures such as partnerships and joint ventures to spread responsibility and liability. Generally there is some financial cost or benefit associated with sharing part of the risk with another organization, such as the premium paid for insurance. Where risks are shared in whole or in part, the organization transferring the risk has acquired a new risk, in that the organization to which the risk has been transferred may not manage the risk effectively.
- Retain the risk. After risks have been changed or shared, there will be residual risks that are retained. Risks can also be retained by default, e.g. when there is a failure to identify or appropriately share or otherwise treat risks.'

The audit toolkit refrains from prescribing or mandating any particular risk management strategy. Ultimately, irrespective of which approach is adopted by the audited organisation, the risk register that represents a key output of this process will be capable of supporting and informing the chosen strategy. Organisations are encouraged to choose an approach (or more than one approach) that will achieve the best results in the context within which they operate, and reflect the resources that are available. Organisations that complete this self-audit process will emerge with a structured table of risks that can be scaled up to accommodate additional information that is of value, given the specifics of particular organisational circumstances.

Factors that might also influence the risk management decision-making process are:

- the organisation's willingness to accept risks, also known as the risk tolerance or appetite for risk;
- the ease with which appropriate controls can be conceived;
- the resources available;
- the current business or technology priorities;
- organisational and management politics.

The purpose of this Stage of the audit is to provide the auditor with tools for effectively and efficiently managing the identified and assessed risks. Further suggestions for risk management are provided in the subsequent section, 'How to Improve: Risk Management Recommendations'.

5.12.2 Tasks Associated with this Stage

In this Stage, auditors are asked to:

- choose a risk management strategy;
- describe the risk mitigation measure;
- assign responsibility for the risk mitigation activities;
- set target dates and/or results for the risk mitigation activities.

Risk management tools and methods are not limited to those included within this Stage of the self-audit process. The auditors are invited to share their risk management exercise results with the senior management of the repository and utilise other risk management techniques.

Further information and guidance can be obtained from the following sources:

- AS/NZS 4360:2004 *Risk management*
- UK Office for Government Commerce, *Successful Delivery Toolkit. Risk Management*

- HM Treasury Office, *The Orange Book. Management of Risk – Principles and Concepts* (2004)

5.12.3 Anticipated Results of this Stage

A principal outcome from the successful completion of this stage is a risk register with risk management features included. The risk management exercise cannot and should not stop with the creation of a risk register. Ongoing review and monitoring is essential to ensure that the risk management plan remains relevant. Factors affecting the likelihood and consequences of a risk may change, as may the factors that affect the suitability or cost of the risk mitigation measure. Also the repository's business, regulatory or social context will change over time and therefore some risks may disappear or become less important while other new risks may emerge. It is therefore necessary to repeat the risk management cycle regularly and review the target outcomes when their deadlines are reached.

Actual progress against risk mitigation plans provides an efficient performance measure and should be incorporated into the organisation's performance management, measurement and reporting system. Monitoring and review also involves learning lessons from the risk management process, by reviewing events, the treatment plans and their outcomes.

Risk communication is part of effective risk management and for ensuring organisation-wide involvement with the risks. Further guidance on risk communication issues can be found in the risk management standards and in the ERPANET *Risk Communication Tool*.[26]

The results of the risk analysis may also form an input to preservation policies and strategies for the repository, as well as renewed definitions of internal mandates and responsibilities.

5.12.4 Where Does this Stage Fit Within the Overall Audit Process?

Risk management is the final Stage and the end-result of this self-audit. The previous five Stages have created a comprehensive body of information that ultimately informs the risk treatment and management process.

The output deliverable of the audit is the audit report, which will be printed from the interactive web version of the audit tool (when this becomes available). The audit report will be printed after the risk management exercise has been completed.

It is expected that, although the repository's risk register will be complete after this Stage, it will continue to be subject to regular review and updates

[26]ERPANET Risk Communication Tool (2003), http://www.erpanet.org/guidance/docs/ERPANETRiskTool.pdf

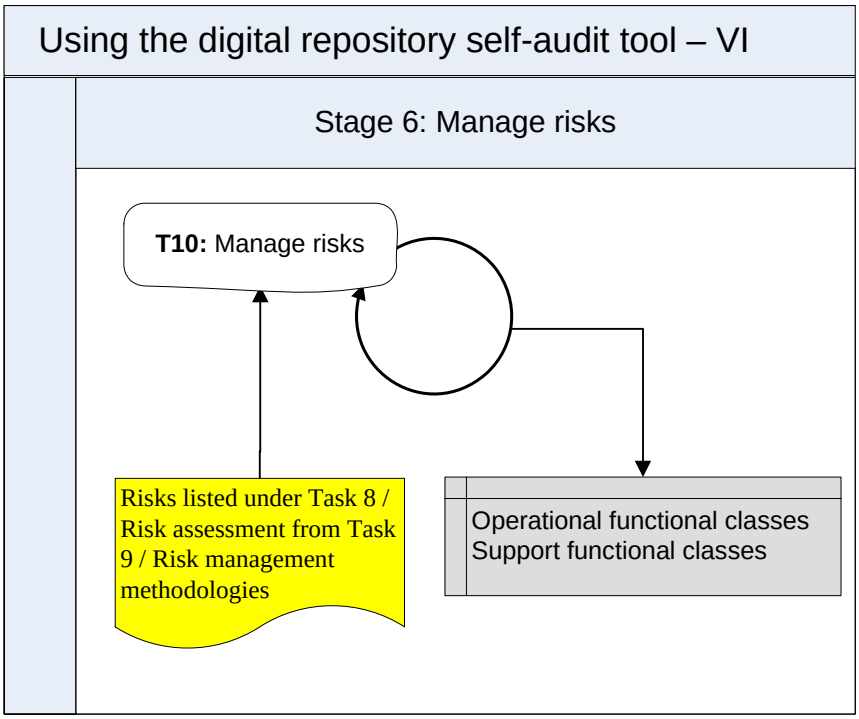
as the risk mitigation activities are completed and as the repository's operating conditions change over time.

5.12.5 What Resources are Required to Complete this Stage?

Anticipated Effort: 4 hours

Although the number of risks identified at Stage 4 will determine the number of times the risk mitigation measures have to be considered, the type, severity and ease of treatment of risks have a significant impact on how much effort has to be invested in this Stage. Ultimately, the time required to complete this Stage depends on how seriously the repository and its senior management are prepared to undertake the risk management exercise. Time spent considering, planning, and deciding how to address the identified risks can only benefit the repository and protect its business activities in the longer term.

5.12.6 Diagram Depicting this Stage



5.12.7 Instructions for Completing the Stage

5.12.7.1 T10: Manage Risks

In the table below, auditors should document preferred risk management measures, names of staff responsible for the risk management activities, and targets for each risk management measure.

The recommended steps for completing this task are as follows:

- Identify suitable responses to risk and choose a type of risk management.
- Identify a range of practical responses to each risk and describe it in terms of a risk management activity.
- Identify owner(s) for risk management activities and define targets that they should seek to achieve.
- Investigate whether the risk management activities and responses themselves pose a new threat to other areas of activity and identify these links. If necessary, return to Stages 4 and 5 and amend the documented risk relationships accordingly.
- Sort the risks into priority order.
- Update the risk register and ensure managers receive appropriate information.
- Gain approval for the plans and risk ownership allocations.
- Seek management approval for the appropriate allocation of resources to the plans and/or assigning of responsibilities for risk management activities.

T10:	**Manage Risks**	
Risk Identifier:		
Risk Name:		
Risk Description:		
Example Risk Manifestation(s):		
Date of Risk Identification:		
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	
	Operations and service delivery	
	Hardware, software or communications equipment and facilities	
Owner:		
Escalation Owner:		

Stakeholders:	
Risk Relationships:	
Risk Probability:	
Risk Potential Impact:	
Risk Severity:	
Risk Management Strategy:	
Risk Management Activity:	
Risk Management Activity Owner:	
Risk Management Activity Target:	

5.12.8 What to do in the Event of Required Information Being Unavailable

If risk management culture and principles do not yet exist in your organisation, auditors will have the opportunity to define how your organisation will respond to risks. It is recommended that auditors consult existing standards and handbooks on organisational and information security risk management and devise a risk management strategy for your repository, based on the risk register created during Stages 4 and 5.

5.12.9 What has been Provided by Other Repositories

Please refer to the section 'How to Improve: Risk Management Recommendations' below.

5.12.10 Comments

Auditors are encouraged to send comments, concerns or observations to the DCC/DPE audit and certification working group at feedback@repositoryaudit.eu.

5.13 HOW TO INTERPRET THE AUDIT RESULT

The risk-assessment based self-audit produces a composite risk score for each of the eight functional classes. This numeric result lends itself to comparisons between risk scores of functional classes and allows the identification of the areas of repository work that are most vulnerable to threats.

The online version of the self-audit toolkit (http://www.repositoryaudit.eu) will provide a mechanism for comparing the audit scores with the average risk scores obtained by other similar types of repositories that have undertaken the self-audit. Comparison of risk scores will be provided in each functional class.

The audit report that will be delivered at the end of the self-audit in the online version can be used as a risk management tool and for communication of risks to the management of the repository. A preliminary structure for the audit report is included in Appendix 4 of this document.

5.13.1 How to Improve: Risk Management Recommendations

Managing risks is a continuous exercise that should not stop with identification or assessment of vulnerabilities and threats, or with making a plan for addressing risks. The risk register resulting from this audit is an efficient tool that can be used for monitoring risk management, updating the risk mitigation, avoidance and treatment measures, and evaluating the success of the chosen measures. A repository is not for each risk restricted to recording only the information included in the example. In analysing risks auditors may well choose to enrich the risk register with further details. A sample structure of attributes in an enlarged risk register might include:

Example of Extended Risk Attribute Tags
Risk Name
Risk Type and/or Grouping
Risk Owner
Date identified
Date last updated
Description
Risk manifestation (circumstances within which risk can execute)
Cost if it materialises (monetary or otherwise)
Probability
Impact
Proximity
Avoidance strategy

Treatment strategy
Target date
Action owner/custodian
Closure date
Cross references to plans and related risks and may also include
Risk status and Risk Action Status
Date of the last assessment

Processes should be put in place to review whether risks still exist, whether new risks have arisen, whether the likelihood and impact of risks have changed, to report significant changes that alter risk priorities, and to deliver assurance on the effectiveness of control.

The risk management monitoring exercise consists of at least the following steps:

- Gaining assurance about the effectiveness of risk management strategies – are they providing the desired results?
- Checking that the risks are within the agreed risk tolerance level.
- Reassessing the exposure to risk and making amendments in the risk register accordingly.
- Re-evaluating the risk management activities and changing them where necessary.
- Identifying areas for change and improvement that need further managerial attention.
- Producing a report on risk management effectiveness and passing this to the management.

The decision regarding which risk management strategies should be applied to different risks is the key success factor in risk management. In some areas, it is easy to avoid the risks or prevent the risk situations from occurring by taking appropriate action in time. In other areas, a certain level of risk will have to be accepted and tolerated, and effective risk impact mitigation activities must be planned for. In some instances, the most vulnerable activities or assets can be transferred to another organisation with more efficient risk avoidance mechanisms, for example through a service contract.

The experience of digital repositories that have assessed their risks or undertaken this self-audit demonstrates some areas of work that are suitable for specific risk management strategies. For example:

5.13.1.1 Risk avoidance and treatment strategies

Example Risk: Legal liability for IPR infringement

Avoidance strategies:

- Assess preserved materials to determine those to which intellectual property restrictions may apply
- Seek legal advice to determine legality of activities with respect to IPR restricted content

In the event of risk's execution:

- Establish policies and procedures to follow in the event of IPR challenge

Example Risk: 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 regularly determine skill levels and training requirements

In the event of risk's execution:

- Provide training facilities to reverse obsolescence of skills

Example Risk: Finances Insufficient to Meet Organisational Objectives

Avoidance strategies:

- Develop self-sustainability with charged-for services
- Seek assurances of level of budget

In the event of risk's execution:

- Solicit additional funding to enable achievement of organisational objectives
- Revise objectives if funding stream is insufficiently flexible
- Maintain residual fund where possible to meet shortfalls

Example Risk: Loss of confidentiality of information

Avoidance strategies:

- Ensure policies and procedures are conceived with due consideration of any confidentiality requirements to which the repository is subject
- Ensure software and hardware systems and preservation strategies are capable of meeting requirements of policies

In the event of risk's execution:

- Implement policy to withdraw availability of confidential materials and invoke treatment strategies to alleviate loss of reputation

5.13.1.2 Risk transfer strategies

Example Risk: Enforced cessation of repository operations

Transfer strategy:

- Establish arrangements for succession
- Establish contingency plans or escrow agreements
- Establish exit strategy

Example Risk: Physical intrusion of hardware storage space

Transfer strategy:

- Establish service level agreement with third-party security company to provide assured physical security services

Example Risk: Hardware failure or incompatibility

Transfer strategy:

- Acquire insurance against failure of hardware systems

5.13.1.3 Risk tolerance strategies

Example Risk: Preservation strategies result in information loss

Tolerance strategy:

- Implement policy to define the parameters of acceptable loss resulting from preservation activities

Example Risk: Loss or non-suitability of backups

Tolerance strategy:

- Implement redundant backup storage

Example Risk: Loss of availability of information and/or service

Tolerance strategy:

- Define policy to commit to the delivery of minimal service levels, incorporating breathing space for tolerable downtime or information non-availability

When choosing a risk management strategy to address a particular risk, or evaluating the efficiency of a risk management measure, a number of different methods can be considered:

5.13.1.4 Operational level

Risk management at the operational level is concerned primarily with continuity of services. A repository may have partners or service providers who are carrying out risk management relating to some of the services. However, the repository must be aware that risk cannot be transferred

totally; the repository must ensure that its own risks are managed. There should be a shared understanding and agreement on the risks and their management.

5.13.1.5 Project level

Risk management at the project level focuses on keeping unwanted outcomes to the minimum. Decisions about risk management at this level form a crucial part of the business case; where providers and/or partners are involved, you must have a shared view of the risks and how they will be managed.

5.13.1.6 Strategic level

Management of risk at the strategic level is concerned with setting strategic direction and balancing potential opportunity against the costs and risks. High-level appraisals of strategic risks are a major feature of the business case when plans for change are being considered. For example, the organisation may be thinking about innovative ways of delivering business services that involve new technologies. Options for exploiting opportunities for improved performance could be assessed against the risks associated with relatively unproven technologies and/or collaboration with private sector partners.

6 PART III, CONCLUSIONS AND NEXT STEPS

6.1 CONCLUSIONS

From when we first open our eyes in the morning till when we close them at night we are all in the risk identification, mitigation and treatment business. Needless to say therefore, the ability to deal adequately with risk is an integral part of any successful business. Principles of risk management are implicit within every business decision, reflecting and influencing objectives and practically realised in business activities and assets. They assume an even more profound level of importance when dealing with digital information, such is the intrinsic uncertainty that characterises the digital domain. Repositories face a multitude of technological, organisational and methodological challenges within their activities, which if considered as treatable or avoidable risks can be more feasibly addressed and subsequently overcome.

Completion of the DRAMBORA process will yield a number of valuable results, facilitating both retrospective reflection and proactive planning for participating organisations. Firstly, organisations will have established a documented self-awareness of their fundamental objectives, and of associated activities and assets. By defining their operational contexts organisations are well positioned to determine their own assessment parameters as well as verify that their resources are optimally invested and positioned to ensure success. Secondly, organisations will have developed a documented understanding of the risks they face expressed in terms of their likelihood and potential impact. Mapped to organisational aspirations and efforts this will facilitate subsequent organisational development and resource allocation, and offer a quantifiable insight into the contemporary severity of risks faced. Finally, organisations will have defined their chosen means for risk management, determining the appropriate strategies for avoidance, treatment, transfer and tolerance as well as the mechanics of their implementation. This process, which should be repeated on a regular basis, will provide opportunities to establish and achieve quantifiable targets, facilitating the ongoing development of every aspect of organisational activity.

As well as being a tremendously valuable process in and of itself, self-assessment with DRAMBORA is expected to represent a worthwhile precursor to external audit, accreditation, and certification when these services become broadly available. The six stages of self-audit correspond closely to the preparatory work that organisations will be expected to undertake when exposed to full audit, and the aggregated documentation will be highly reusable.

6.2 ANTICIPATED NEXT STEPS

This is the first iteration of the DCC/DPE *Digital Repository Audit Method Based on Risk Assessment* Toolkit. During 2007 we will be enhancing the toolkit as we test it through repository audits the coming year. A formal testing period will follow each release, and we invite organisations to become evaluation partners in order to provide feedback and suggestions

for improvement. Feedback mechanisms will be integrated into the forthcoming online version of the tool, and an email address, feedback@repositoryaudit.eu has been established to provide a central point to direct all feedback, criticism and thoughts relating to the tool.

Within an initial testing phase, participants from the DCC aim to work with the JISC Digital Repositories Programme to evaluate the toolkit. DPE will engage with European partners to evaluate the first release, and will also use the toolkit, in combination with existing internationally defined audit criteria, as the basis for a series of formal audits. The DCC and DPE anticipate completing between seventeen and twenty further audits between 1 April 2007 and 1 December 2007, with the goal of releasing a further iteration of the toolkit on 28 February 2008.

7 APPENDICES

7.1 APPENDIX 1: ACKNOWLEDGEMENTS

The authors would like to express our gratitude to the Director of the Digital Curation Centre, Chris Rusbridge, for his encouragement, contributions and ongoing support to this endeavour. We thank David Giaretta, Associate Director of the Digital Curation Centre and Principal Investigator in CASPAR and Robin Dale, formerly of Research Libraries Group and now of OCLC for enabling the DCC Services team to participate in the work of TRAC.

We greatly appreciate the strategic guidance offered throughout this process by Bernard F Reilly, President, Center for Research Libraries (Chicago).

Ross Harvey who is normally Professor of Library and Information Management, Charles Sturt University, but who held the post of DCC Visiting Fellow and Visiting Professor in the University of Glasgow during the early months of 2007, provided valuable criticisms, asked helpful questions, and gave good guidance.

We are extremely grateful for the input, assistance, and feedback that we have received in the development of this toolkit from Stefan Strathmann and the rest of the nestor team, and in particular Dr. Astrid Schoger of the Bayerische Staatsbibliothek.

We are particularly grateful to Adam Rusbridge, DCC and LOCKSS Technical Support Officer within HATII at the University of Glasgow for his participation in the pilot audits. We also wish to thank Lorna Cullen for casting her expert eye over the document before its release.

Most importantly the preparation of this initial version of the toolkit was made possible through the generosity of the many members of the archives, library, eScience, and data curating communities who contributed time and effort. We wish to thank the following organisations and individuals for their invaluable contributions to the development of this toolkit through providing us with insights into how repositories work in different environments and the processes involved in successfully running them.

British Atmospheric Data Centre (BADC)

-Tim Folkes, Atlas Data Store Project
-Wendy Garland, Environmental Data Scientist
-Rob Harper, Storage Coordinator
-Andrew Harwood, BADC Infrastructure Manager
-Charles Kilburn, Environmental Data Scientist
-Bryan Lawrence, Head of the BADC
-Sam Pepler, Curation Manager

Beazley Archive

-Professor Donna Kurtz, Director
-Thomas Mannack, Pottery Database Administrator
-Greg Parker, Technical Director
-Claudia Wagner, Gem Database Administrator

The National Digital Archive of Datasets at ULCC

-Kevin Ashley, Head of Digital Archives
-Joanne Anthony, Archivist
-Kate Bradford, Archivist
-Mina Creathorn, Content Specialist
-Sally Hughes, Team Leader, Content Specialists
-Jim Jamieson, Team Leader, Archivists
-Jenny Leigh, Archivist
-Jo Marsh, Content Specialist
-Ed Pinsent, Archivist

National Library of New Zealand

-Mat Black, Integration Architect
-Steve Knight, NDHA Programme Architect
-Pauline LaRooy, Collections Development
-Ingrid Mason, (Former) Resource Analyst
-Ann O'Rorke, Business Change Manager
-Leigh Rosin, Digital Archivist
-Lockie Stewart, Enterprise Architect
-Ann Thompson, Collections Development

Florida Digital Archive

-James F Corey, FCLA Director
-Priscilla Caplan, Assistant Director, Digital Library Services
-Jennifer Childree, IT Entry
-Carol Chou, IT Senior
-Randy Fischer, IT Expert
-Franco Lazzarino, IT Expert
-Manny Rodriquez, IT Expert
-Chris Cuevas, IT Expert
-Daryl Marsee, Coordinator, Computer Applications
-Martin Johnson, Coordinator, Computer Applications

7.2 APPENDIX 2: SELF-AUDIT TOOLKIT TEMPLATES

T1: What is the mandate of your repository or the organisation in which it is embedded?

T2: List goals and objectives of your repository

T3: List your repository's strategic planning documents

T4: List the legal, regulatory and contractual frameworks or agreements to which your repository is subject

T5: List the voluntary codes to which your repository has agreed to adhere

T6: List any other documents and principles with which your repository complies

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

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

T9: Assess the identified risks

T10: Manage risks

Repository		Auditor		Date	
Stage	**Stage 1: Identify organisational context**	Form	**T1**	Page	

T1:	**What is the mandate of your repository or the organisation in which it is embedded?**

T2:	**List goals and objectives of your repository**
Operational functions: Acquisition & Ingest	
Operational functions: Preservation & Storage	
Operational functions: Metadata management	
Operational functions: Access & Dissemination	
Support functions: Organisation & Management	
Support functions: Staffing	
Support functions: Financial management	
Support functions: Technical infrastructure & Security	

Define your own categories or classes for listing the goals and objectives:

T2:	**List goals and objectives of your repository**

T3:	**List your repository's strategic planning documents**
Operational functions: Acquisition & Ingest	Reference
Operational functions: Preservation & Storage	Reference
Operational functions: Metadata management	Reference
Operational functions: Access & Dissemination	Reference
Support functions: Organisation & Management	Reference
Support functions: Staffing	Reference
Support functions: Financial management	Reference
Support functions: Technical infrastructure & Security	Reference

Define your own categories or classes for listing the strategic planning documents:

T3:	**List your repository's strategic planning documents**
	Reference
	Reference
	Reference
	Reference

T4:	**List the legal, regulatory and contractual frameworks or agreements to which your repository is subject**
Operational functions: Acquisition & Ingest	
Operational functions: Preservation & Storage	
Operational functions: Metadata management	
Operational functions: Access & Dissemination	
Support functions: Organisation & Management	
Support functions: Staffing	
Support functions: Financial management	
Support functions: Technical infrastructure & Security	

Define your own categories or classes for listing the legal, regulatory and contractual framework and agreements to which your repository is subject:

T4:	**List the legal, regulatory and contractual frameworks or agreements to which your repository is subject**

T5:	**List the voluntary codes to which your repository has agreed to adhere**
Operational functions: Acquisition & Ingest	Reference
Operational functions: Preservation & Storage	Reference
Operational functions: Metadata management	Reference
Operational functions: Access & Dissemination	Reference
Support functions: Organisation & Management	Reference
Support functions: Staffing	Reference
Support functions: Financial management	Reference
Support functions: Technical infrastructure & Security	Reference
Define your own category:	

Define your own categories or classes for listing the voluntary codes to which your repository has agreed to adhere:

T5:	**List the voluntary codes to which your repository has agreed to adhere**
	Reference
	Reference
	Reference
	Reference

T6:	**List any other documents and principles with which your repository complies**
Operational functions: Acquisition & Ingest	
Operational functions: Preservation & Storage	
Operational functions: Metadata management	
Operational functions: Access & Dissemination	
Support functions: Organisation & Management	
Support functions: Staffing	
Support functions: Financial management	
Support functions: Technical infrastructure & Security	

Define your own categories or classes for listing other documents and principles with which your repository complies:

T6:	**List any other documents and principles with which your repository complies**

T7:	**Identify your repository's activities, assets and their owners**	
Operational functions: Acquisition & Ingest		Owner(s)
Activity		
Asset(s)		
Activity		
Asset(s)		
Activity		
Asset(s)		
Activity		
Asset(s)		
Activity		
Asset(s)		
Activity		
Asset(s)		
Activity		
Asset(s)		
Activity		
Asset(s)		
Activity		
Asset(s)		
Activity		
Asset(s)		
Activity		
Asset(s)		
Activity		
Asset(s)		
Activity		
Asset(s)		

T7:	**Identify your repository's activities, assets and their owners**	
Operational functions: Preservation & Storage		Owner(s)
Activity		
Asset(s)		
Activity		
Asset(s)		
Activity		
Asset(s)		
Activity		
Asset(s)		
Activity		
Asset(s)		
Activity		
Asset(s)		
Activity		
Asset(s)		
Activity		
Asset(s)		
Activity		
Asset(s)		
Activity		
Asset(s)		
Activity		
Asset(s)		
Activity		
Asset(s)		
Activity		
Asset(s)		

T7:	**Identify your repository's activities, assets and their owners**	
Operational functions: Metadata management		Owner(s)
Activity		
Asset(s)		
Activity		
Asset(s)		
Activity		
Asset(s)		
Activity		
Asset(s)		
Activity		
Asset(s)		
Activity		
Asset(s)		
Activity		
Asset(s)		
Activity		
Asset(s)		
Activity		
Asset(s)		
Activity		
Asset(s)		
Activity		
Asset(s)		
Activity		
Asset(s)		
Activity		
Asset(s)		

T7:	**Identify your repository's activities, assets and their owners**	
Operational functions: Access & Dissemination		Owner(s)
Activity		
Asset(s)		
Activity		
Asset(s)		
Activity		
Asset(s)		
Activity		
Asset(s)		
Activity		
Asset(s)		
Activity		
Asset(s)		
Activity		
Asset(s)		
Activity		
Asset(s)		
Activity		
Asset(s)		
Activity		
Asset(s)		
Activity		
Asset(s)		
Activity		
Asset(s)		
Activity		
Asset(s)		

T7:	**Identify your repository's activities, assets and their owners**	
Support functions: Organisation & Management		Owner(s)
Activity		
Asset(s)		
Activity		
Asset(s)		
Activity		
Asset(s)		
Activity		
Asset(s)		
Activity		
Asset(s)		
Activity		
Asset(s)		
Activity		
Asset(s)		
Activity		
Asset(s)		
Activity		
Asset(s)		
Activity		
Asset(s)		
Activity		
Asset(s)		
Activity		
Asset(s)		
Activity		
Asset(s)		

T7:	**Identify your repository's activities, assets and their owners**	
Support functions: Staffing		Owner(s)
Activity		
Asset(s)		
Activity		
Asset(s)		
Activity		
Asset(s)		
Activity		
Asset(s)		
Activity		
Asset(s)		
Activity		
Asset(s)		
Activity		
Asset(s)		
Activity		
Asset(s)		
Activity		
Asset(s)		
Activity		
Asset(s)		
Activity		
Asset(s)		
Activity		
Asset(s)		
Activity		
Asset(s)		

T7:	**Identify your repository's activities, assets and their owners**	
Support functions: Financial management		Owner(s)
Activity		
Asset(s)		
Activity		
Asset(s)		
Activity		
Asset(s)		
Activity		
Asset(s)		
Activity		
Asset(s)		
Activity		
Asset(s)		
Activity		
Asset(s)		
Activity		
Asset(s)		
Activity		
Asset(s)		
Activity		
Asset(s)		
Activity		
Asset(s)		
Activity		
Asset(s)		
Activity		
Asset(s)		

T7:	**Identify your repository's activities, assets and their owners**	
Support functions: Technical infrastructure & Security		Owner(s)
Activity		
Asset(s)		
Activity		
Asset(s)		
Activity		
Asset(s)		
Activity		
Asset(s)		
Activity		
Asset(s)		
Activity		
Asset(s)		
Activity		
Asset(s)		
Activity		
Asset(s)		
Activity		
Asset(s)		
Activity		
Asset(s)		
Activity		
Asset(s)		
Activity		
Asset(s)		
Activity		
Asset(s)		

T7:	**Identify your repository's activities, assets and their owners**	
Operational functions: Acquisition & Ingest		Owner(s)
Activity		
Asset(s)		
Activity		
Asset(s)		
Activity		
Asset(s)		
Activity		
Asset(s)		
Activity		
Asset(s)		
Activity		
Asset(s)		
Activity		
Asset(s)		
Activity		
Asset(s)		
Activity		
Asset(s)		
Activity		
Asset(s)		
Activity		
Asset(s)		
Activity		
Asset(s)		
Activity		
Asset(s)		

Repository		Auditor		Date	
Stage	**Stage 3: Identify activities, assets and their owners**	Form	**T7**	Page	

Define your own categories or classes for identifying the activities, assets and their owners:

T7:	**Identify your repository's activities, assets and their owners**	
		Owner(s)
Activity		
Asset(s)		
Activity		
Asset(s)		
Activity		
Asset(s)		
Activity		
Asset(s)		
Activity		
Asset(s)		
Activity		
Asset(s)		
Activity		
Asset(s)		
Activity		
Asset(s)		
Activity		
Asset(s)		

T8:	**Identify risks associated with activities and assets of your repository**	
Risk Identifier:		
Risk Name:		
Risk Description:		
Example Risk Manifestation(s):		
Date of risk identification:		
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	
	Operations and service delivery	
	Hardware, software or communications equipment and facilities	
Owner:		
Escalation Owner:		
Stakeholders:		
Risk Relationships:		

T9:	**Assess the identified risks**	
Risk Identifier:		
Risk Name:		
Risk Description:		
Example Risk Manifestation(s):		
Date of risk identification:		
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	
	Operations and service delivery	
	Hardware, software or communications equipment and facilities	
Owner:		
Escalation Owner:		
Stakeholders:		
Risk Relationships:		
Risk Probability:		
Risk Potential Impact:		
Risk Severity:	… x … = …	

T10:	**Manage risks**	
Risk Identifier:		
Risk Name:		
Risk Description:		
Example Risk Manifestation(s):		
Date of risk identification:		
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	
	Operations and service delivery	
	Hardware, software or communications equipment and facilities	
Owner:		
Escalation Owner:		
Stakeholders:		
Risk Relationships:		
Risk Probability:		
Risk Potential Impact:		
Risk Severity:	… x … = …	
Risk Management Strategy(ies):		
Risk Management Activity(ies):		
Risk Management Activity Owner:		
Risk Management Activity Target:		

7.3 APPENDIX 3: EXAMPLE DIGITAL REPOSITORY RISKS WITH DESCRIPTIONS

Please note that the following tables contain example risks that auditors may wish to incorporate within their own risk register. However, the fields included below are not comprehensive; they omit certain highly repository-specific fields which if included would be immediately redundant. Auditors should refer to the table in section 'Risk Assessment Principles' above for a complete list of required fields that must be included within their risk register.

7.3.1 Organisation Management

Risk Identifier:	R01	
Risk Name:	Management failure	
Risk Description:	One or more aspect of organisational management is unsuccessful, resulting in a failure to deliver an anticipated or required business outcome.	
Is this Risk Relevant?:	• Is organisation subject to central management control?	
Example Risk Manifestation(s):	• Repository management fails to allocate sufficient resources to complete one or more business activities • Management's adopted preservation strategies result in information loss	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	X
	Operations and service delivery	
	Hardware, software or communications equipment and facilities	
Owner:	Management	
Escalation Owner:	Management	
Stakeholders:	Management	
Mitigation strategy(ies):	Avoidance strategies: • Conceive comprehensive management policies and procedures and establish mechanisms for their regular review • Establish benchmarks to determine effectiveness of management policies and procedures In the event of risk's execution: • Establish continuity or recovery mechanisms to recover from effects	
Risk Relationships:	←→R02 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R02	
Risk Name:	Loss of trust or reputation	
Risk Description:	One or more stakeholder communities have doubts about the repository's ability to achieve its business objectives.	
Is this Risk Relevant?:	• Does the organisation rely upon its reputation as a business asset? • Does the organisation rely upon its trustworthiness as a business asset? • Has the organisation identified a correlation between its business effectiveness and the reputation and level of trust it enjoys?	
Example Risk Manifestation(s):	• An irrecoverable loss of digital objects provokes community concerns about the repository's competence • A public statement announcing a cut in funding raises concerns that the repository will have insufficient resources to operate effectively	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	X
	Operations and service delivery	X
	Hardware, software or communications equipment and facilities	
Owner:	Management	
Escalation Owner:	Management	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Seek all available and relevant certifications to publicly demonstrate the repository's operational effectiveness • Promote organisational transparency to reveal suitability and extent of coverage of policies and procedures • Aim for excellence in pursuit of organisational objectives • Establish outreach mechanisms to reflect where possible expectations of user communities	
Risk Relationships:	←→R01 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R03	
Risk Name:	Activity is overlooked or allocated insufficient resources	
Risk Description:	An integral business activity is mismanaged leading to its non-completion.	
Is this Risk Relevant?:	• Is repository responsible for budgetary development and allocation of resources?	
Example Risk Manifestation(s):	• Repository budgeting does not include a financial allocation for system security maintenance • A 0.5 FTE has sole responsibility to ingest 100 objects per day, although it takes on average 30 minutes for an individual to ingest a single object	
Nature of Risk:	Physical environment	X
	Personnel, management and administration procedures	X
	Operations and service delivery	X
	Hardware, software or communications equipment and facilities	X
Owner:	Management	
Escalation Owner:	Management	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Derive activities, policies and procedures from fundamental repository objectives • Allocate resources to correspond with identified activities • Establish mechanisms to review and adjust resource allocations In the event of risk's execution: • Maintain residual fund to facilitate subsequent resourcing of originally overlooked activity	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R* [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R04	
Risk Name:	Business objectives not met	
Risk Description:	One or more integral business outcomes are not achieved, or are achieved inadequately.	
Is this Risk Relevant?:	• Does repository make a commitment to its stakeholder groups to achieve one or more stated objectives?	
Example Risk Manifestation(s):	• Business commits to delivering object *x* within 5 minutes of its request but on average delivery takes 15 minutes • Repository fails to adequately preserve identified significant properties of ingested materials	
Nature of Risk:	Physical environment	X
	Personnel, management and administration procedures	X
	Operations and service delivery	X
	Hardware, software or communications equipment and facilities	X
Owner:	Management	
Escalation Owner:	Management	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Define activities, policies and procedures with strict reference to corresponding fundamental objectives • Secure and allocate resources based on business priorities • Establish mechanisms to regularly review and, if necessary, adjust policies and procedures in order to ensure objectives are realised In the event of risk's execution: • Undertake appropriate internal enquiries to determine the shortcomings that led to failure and update policies accordingly	
Risk Relationships:	→R01 [contagious] →R02 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R05	
Risk Name:	Repository loses mandate	
Risk Description:	Basis for repository's existence is withdrawn or substantially altered, rendering it incompatible with business activities.	
Is this Risk Relevant?:	• Is repository's mandate subject to ongoing review? • Is primary repository service contract subject to renewal or renegotiation?	
Example Risk Manifestation(s):	• Scope of repository responsibility is changed by legislative amendment • Repository obligations are altered within contract renegotiations	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	X
	Operations and service delivery	
	Hardware, software or communications equipment and facilities	
Owner:	Management	
Escalation Owner:	Management	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Seek all available and relevant certifications to publicly demonstrate the repository's operational effectiveness • Promote organisational transparency to reveal suitability and extent of coverage of policies and procedures • Aim for excellence in pursuit of organisational objectives In the event of risk's execution: • Establish arrangements for succession • Establish contingency plans or escrow agreements • Establish exit strategy	
Risk Relationships:	→R08 [contagious] →R01 [contagious] →R02 [contagious] →R* [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R06	
Risk Name:	Community requirements change substantially	
Risk Description:	Community expectations or requirements are substantially altered, and no longer correspond to business activities.	
Is this Risk Relevant?:	• Have user requirements been subject to change in the past? • Has the repository or have other external, comparable repositories experienced a change or evolution in the communities using or depositing content?	
Example Risk Manifestation(s):	• User community adopts new software systems which provide no support for legacy data formats that were previously dominant • Community becomes increasingly unfamiliar with the semantics of a previously well-known and widely employed scientific markup language	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	
	Operations and service delivery	X
	Hardware, software or communications equipment and facilities	
Owner:	Management	
Escalation Owner:	Management	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Monitor requirements, expectations and knowledge base of user community • Document and review organisational definition of understandability for each distinct user community In the event of risk's execution: • Maintain flexible approach to operational objectives to react to emerging community requirements	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R11 [contagious] →R67 [contagious] →R74 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R07	
Risk Name:	Community requirements misunderstood or miscommunicated	
Risk Description:	Repository is incapable of determining the expectations of its stakeholder communities and therefore unable to tailor business activities appropriately.	
Is this Risk Relevant?:	• Does the repository have mechanisms established to monitor the community's knowledge base, requirements or expectations? • Are community members consulted about the adequacy of available service levels?	
Example Risk Manifestation(s):	• Repository fails to identify that its user communities require data to be delivered encoded as *.abc* files in order for them to be usable	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	
	Operations and service delivery	X
	Hardware, software or communications equipment and facilities	
Owner:	Management	
Escalation Owner:	Management	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Establish appropriate technical mechanisms to facilitate monitoring of requirements, expectations and knowledge base of user community In the event of risk's execution: • Maintain dialogue with community to ensure the continued correctness of understandability definition • Maintain flexibility within operational objectives to react to misunderstanding of requirements	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R11 [contagious] →R67 [contagious] →R74 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R08	
Risk Name:	Enforced cessation of repository operations	
Risk Description:	Repository is forced to cease its business activities.	
Is this Risk Relevant?:	• Does the mechanism responsible for the repository's establishment include a stated and finite period for its existence before renewal measures must be undertaken? • Are mechanisms available to counterbalance periods of financial loss or constraint? • Are significant aspects of business activities susceptible to legal challenge? • Is there evidence to suggest that the scale of the repository's user community is diminishing over time?	
Example Risk Manifestation(s):	• Repository's responsibilities are withdrawn by legislative amendment • Repository fails secure renewal of its preservation contract with its primary client and/or funder • Repository goes bankrupt or is no longer financially sustainable • Repository loses its place in a competitive marketplace	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	
	Operations and service delivery	X
	Hardware, software or communications equipment and facilities	
Owner:	Management	
Escalation Owner:	Management	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Seek all available and relevant certifications to demonstrate publicly the repository's operational effectiveness • Promote organisational transparency to reveal suitability and extent of coverage of policies and procedures • Aim for excellence in pursuit of organisational objectives In the event of risk's execution: • Establish arrangements for succession • Establish contingency plans or escrow agreements • Establish exit strategy	
Risk Relationships:	→R01 [contagious] →R02 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R09	
Risk Name:	Community feedback not received	
Risk Description:	Repository fails to solicit responses from the community regarding its level of service, or fails to provide mechanisms for this.	
Is this Risk Relevant?:	• Does repository have mechanisms available to solicit feedback from community members? • Is a proportion of staff time allocated to the gathering or receipt of community feedback? • Are feedback mechanisms regularly tested to ensure they are functioning correctly?	
Example Risk Manifestation(s):	• Repository fails to identify that its user communities are increasingly incapable of using data encoded within the repository's chosen formats with the software that they principally employ	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	
	Operations and service delivery	X
	Hardware, software or communications equipment and facilities	X
Owner:	Management	
Escalation Owner:	Management	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Maintain appropriate mechanisms for community to provide feedback, such as email, web-forms, telephone helpdesk and mail address • Actively solicit feedback, allocating a proportion of staff time to community engagement In the event of risk's execution: • Identify reasons for communication failure and update policies and procedures accordingly	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R10 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R10	
Risk Name:	Community feedback not acted upon	
Risk Description:	Although feedback is received, it has no influence over repository's business activities.	
Is this Risk Relevant?:	• Is a proportion of staff time allocated to responding to community feedback, or reflecting it in changes to operational objectives? • Are policies and procedures in place to enable the repository to react within an appropriately timely fashion to the receipt of community feedback? • Are operational objectives adaptable to react to community feedback?	
Example Risk Manifestation(s):	• Repository fails to react to the fact that its user communities are increasingly incapable of using data encoded within the repository's chosen formats with the software that they principally employ	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	
	Operations and service delivery	X
	Hardware, software or communications equipment and facilities	
Owner:	Management	
Escalation Owner:	Management	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Establish policies to acknowledge and react to community feedback In the event of risk's execution: • Acknowledge failure to act with community and retrospectively react to received feedback	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R11 [contagious] →R67 [contagious] →R74 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R11	
Risk Name:	Business fails to preserve essential characteristics of digital information	
Risk Description:	Repository's preservation activities are insufficient to maintain the properties of its digital holdings that are of greatest significance to its user communities	
Is this Risk Relevant?:	• Are significant properties defined and documented for each class of object preserved within the repository? • Are members of the community consulted throughout the process of defining significant properties? • Are preservation policies and procedures sufficient to maintain defined properties?	
Example Risk Manifestation(s):	• Repository preserves transcribed text from digitised manuscripts within *.txt* files, although user communities are interested in looking at the original illuminations in subsequent research • Repository aims to preserve images of manuscript illuminations but chosen resolution is insufficient to display the level of detail required by user community	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	
	Operations and service delivery	X
	Hardware, software or communications equipment and facilities	
Owner:	Management	
Escalation Owner:	Management	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Document significant properties of digital objects that will be maintained, based on community expectations and requirements In the event of risk's execution: • Acknowledge organisational shortcoming and revise policies and significant properties definition accordingly	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R04 [contagious] →R67 [contagious] →R74 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R12	
Risk Name:	Business policies and procedures are unknown	
Risk Description:	Fundamentals of why and how repository's business activities are conducted are undocumented and unknown, or known only by specific individuals.	
Is this Risk Relevant?:	• Are policies and procedures comprehensively documented? • Is documentation widely accessible and understandable throughout the organisation? • Is the location of policy and procedure documentation recorded and well known?	
Example Risk Manifestation(s):	• Policies and procedures associated with each organisational facet are known only to the individuals responsible • Policies are documented in Microsoft Word files but stored only on an unshared partition of a workstation hard-disk	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	
	Operations and service delivery	X
	Hardware, software or communications equipment and facilities	
Owner:	Management	
Escalation Owner:	Management	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Conceive and document comprehensive policies and procedures • Circulate documentation among repository staff and create multiple copies in alternative locations • Circulate details of documentation locations	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R04 [contagious] →R19 [contagious] →R* [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R13	
Risk Name:	Business policies and procedures are inefficient	
Risk Description:	Rationale and/or practical approach adopted for business fail to demonstrate optimal efficiency.	
Is this Risk Relevant?:	• Do measurable aspects of performance compare favourably with those of similar organisations? • How does the repository's current operational efficiency compare with its peak level?	
Example Risk Manifestation(s):	• Repository makes objects available one hour after a dissemination request, but comparable organisations providing similar content are capable of doing so in just 30 minutes • Revised policies are demonstrably less efficient than those that preceded	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	
	Operations and service delivery	X
	Hardware, software or communications equipment and facilities	
Owner:	Management	
Escalation Owner:	Management	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Expose policies and procedures to regular review to determine their efficiency and appropriateness with respect to organisational goals • Seek external validation of policies and procedures (e.g. accredited auditors or user communities) In the event of risk's execution: • Identify those policies that are inefficient and revise them accordingly	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R* [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R14	
Risk Name:	Business policies and procedures are inconsistent or contradictory	
Risk Description:	Rationale and/or practical approach adopted for particular business objectives introduce obstacles to the successful completion of other business activities.	
Is this Risk Relevant?:	• Are business policies and procedures conceived with consideration of the operations of the repository as a whole? • Are mechanisms in place to resolve conflicting policies and/or procedures?	
Example Risk Manifestation(s):	• Repository requires staff to undertake quality assurance procedures for each object ingested, which takes on average 10 minutes, although an additional policy states that ingest should be completed in 10 minutes	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	
	Operations and service delivery	X
	Hardware, software or communications equipment and facilities	
Owner:	Management	
Escalation Owner:	Management	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Expose policies and procedures to regular review to determine their consistency with respect to organisational goals • Seek external validation of policies and procedures (e.g. accredited auditors or user communities) In the event of risk's execution: • Identify those policies that are inconsistent and revise them accordingly	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R* [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R15	
Risk Name:	Legal liability for IPR infringement	
Risk Description:	Repository is legally accountable for a breach of copyright, patent infringement or other IPR-related misdemeanour as a direct result of its business activities.	
Is this Risk Relevant?:	• Does the repository deal with content with specific associated intellectual property rights? • Does the repository consult with legal experts when determining the legality of their activities with respect to IPR restricted content? • Is there evidence of a high degree of litigiousness within the domain or jurisdiction within which the repository operates?	
Example Risk Manifestation(s):	• As part of its preservation activities, the repository reverse engineers a software application, and in doing so contravenes a condition of its end user license agreement • An institutional repository disseminates e-journal content, and in doing so is guilty of copyright breach	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	X
	Operations and service delivery	
	Hardware, software or communications equipment and facilities	
Owner:	Legal	
Escalation Owner:	Legal	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Assess preserved materials to determine those to which intellectual property restrictions may apply • Seek legal advice to determine legality of activities with respect to IPR restricted content In the event of risk's execution: • Establish policies and procedures to follow in the event of IPR challenge	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R04 [contagious] →R14 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R16	
Risk Name:	Legal liability for breach of contractual responsibilities	
Risk Description:	Repository is legally accountable for either failing to fulfil responsibilities or acting beyond the scope of what is permissible, as detailed in stakeholder contracts.	
Is this Risk Relevant?:	• Does the repository engage in contractual relationships? • Does the repository consult with legal experts when determining the legality of their activities with respect to enforceable contracts that they are party to? • Is there evidence of a high degree of litigiousness within the domain or jurisdiction within which the repository operates?	
Example Risk Manifestation(s):	• Repository disseminates preserved content over the public Internet without restriction, although the corresponding deposit agreement stated that only a limited community should have access	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	X
	Operations and service delivery	
	Hardware, software or communications equipment and facilities	
Owner:	Legal	
Escalation Owner:	Legal	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Monitor contracts and ensure that implemented policies correspond to their terms • Seek legal advice to determine legality of activities with respect to IPR restricted content In the event of risk's execution: • Establish policies and procedures to follow in the event of contractual challenge	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R04 [contagious] →R14 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R17	
Risk Name:	Legal liability for breach of legislative requirements	
Risk Description:	Repository is legally accountable for either failing to fulfil responsibilities or acting beyond the scope of what is permissible, as detailed in legislative instruments.	
Is this Risk Relevant?:	• Is the repository established within legislation? • Do any other legislative acts or statutory instruments establish restrictions or obligations related to repository activities? • Does the repository consult with legal experts when determining the legality of their activities with respect to relevant legislation? • Is there evidence of a high degree of litigiousness within the domain or jurisdiction within which the repository operates?	
Example Risk Manifestation(s):	• Repository fails to accept deposited materials in contravention of legal deposit laws established in local legislation	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	X
	Operations and service delivery	
	Hardware, software or communications equipment and facilities	
Owner:	Legal	
Escalation Owner:	Legal	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Monitor legislation in order to ensure that policies and procedures correspond to intrinsic requirements and prohibitions • Seek legal advice to determine legality of activities with respect to legislation In the event of risk's execution: • Establish policies and procedures to follow in the event of legislative challenge	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R04 [contagious] →R14 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R18	
Risk Name:	Liability for regulatory non-compliance	
Risk Description:	Repository is liable for failure to conduct its activities in accordance with industrial, business oriented or global regulation.	
Is this Risk Relevant?:	• Do any regulations establish restrictions or obligations related to repository activities? • Does the repository consult with legal experts when determining the legality of their activities with respect to relevant regulations? • Is there evidence of a high degree of litigiousness within the domain or jurisdiction within which the repository operates?	
Example Risk Manifestation(s):	• Repository fails to conform to appropriate jurisdictional health and safety regulations for employees	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	
	Operations and service delivery	X
	Hardware, software or communications equipment and facilities	
Owner:	Legal	
Escalation Owner:	Legal	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Monitor regulatory framework and ensure policies and procedures correspond to their requirements and prohibitions • Seek legal advice to determine legality of activities with respect to regulatory framework In the event of risk's execution: • Establish policies and procedures to follow in the event of IPR challenge	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R04 [contagious] →R14 [contagious]]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R19	
Risk Name:	Inability to evaluate repository's successfulness	
Risk Description:	Repository is incapable of effectively determining the extent to which it has successfully achieved its business objectives.	
Is this Risk Relevant?:	• Does the repository maintain policies and procedures to verify and record the integrity, authenticity, provenance and understandability of archived information? • Does the repository maintain policies and procedures to evaluate and record the execution of repository processes and to check that their outputs are complete and correct? • Does the repository engage with user communities to determine their overall level of satisfaction? • Are mechanisms to determine the effectiveness of repository operations exploited on a regular basis?	
Example Risk Manifestation(s):	• Repository has no way of demonstrating that the integrity and authenticity of its archived materials have been maintained • Repository cannot demonstrate that submitted information has been ingested correctly and transformed into a corresponding complete and correct archival package	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	X
	Operations and service delivery	
	Hardware, software or communications equipment and facilities	
Owner:	Management	
Escalation Owner:	Management	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Establish internal means of assessment including risk management • Seek relevant external certification in order to demonstrate competence	
Risk Relationships:	→R01 [contagious] →R02 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R20	
Risk Name:	False perception of the extent of repository's success	
Risk Description:	Repository's assessments of success are flawed and indicate a level of performance inconsistent with reality.	
Is this Risk Relevant?:	• Do the repository's various efforts to determine effectiveness result in inconsistent results? • Do repository's evaluation mechanisms offer comprehensive and reliable coverage?	
Example Risk Manifestation(s):	• Based on flawed end-user survey evidence solicited from just a small subsection of its user community, the repository is satisfied that its efforts are successful, although mechanisms in place are actually insufficient to maintain the understandability, integrity and authenticity of archived information	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	X
	Operations and service delivery	
	Hardware, software or communications equipment and facilities	
Owner:	Management	
Escalation Owner:	Management	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Establish internal means of assessment including risk management • Seek relevant external certification in order to demonstrate competence	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R19 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

7.3.2 Staffing

Risk Identifier:	R21	
Risk Name:	Loss of key member(s) of staff	
Risk Description:	Individuals with roles, responsibilities or aptitudes vital to the achievement of business objectives part company with the repository, rendering the achievement of those objectives less straightforward.	
Is this Risk Relevant?:	• Has the repository experienced significant staff turnover? • Is the status, expertise or knowledge of any individual staff member such that their loss would be of considerable detriment to the organisation's business objectives?	
Example Risk Manifestation(s):	• Repository's head systems' administrator, the sole individual with knowledge of the system's root password, leaves the organisation to work within an alternative industry	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	X
	Operations and service delivery	
	Hardware, software or communications equipment and facilities	
Owner:	Personnel	
Escalation Owner:	Personnel	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Offer favourable terms and conditions for staff In the event of risk's execution: • Promote sharing of organisational responsibilities and duplication of skills in order to limit the impact of losing individual members of staff • Ensure policies and procedures are widely circulated and not known only to selected individuals	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R12 [contagious] →R* [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R22	
Risk Name:	Staff suffer deterioration of skills	
Risk Description:	Staff members demonstrate a diminishing level of skills over time.	
Is this Risk Relevant?:	• Are staff members required to possess skills that are practically employed only on an infrequent basis? • Are skills refreshment opportunities available to staff?	
Example Risk Manifestation(s):	• Repository technical staff are rarely required to recover content from backups, and consequently suffer a deterioration of the appropriate skills to use backup retrieval mechanism	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	X
	Operations and service delivery	
	Hardware, software or communications equipment and facilities	
Owner:	Personnel	
Escalation Owner:	Personnel	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Establish means for staff skills refreshment, and for staff to employ skills of limited frequent value in test environment • Implement staff performance reviews to regularly determine skill levels and training requirements In the event of risk's execution: • Provide training facilities to reverse skills haemorrhage	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R* [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R23	
Risk Name:	Staff skills become obsolete	
Risk Description:	Staff members' skills stagnate and are no longer current.	
Is this Risk Relevant?:	• Does the repository's natural development presuppose that staff will develop new skills and abilities over time? • Are training and professional development opportunities made available to staff? • Are staff members required to identify and pursue appropriate training activities?	
Example Risk Manifestation(s):	• Staff are only capable of employing dated preservation strategies and are not trained in or exposed to emerging techniques or technologies	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	X
	Operations and service delivery	
	Hardware, software or communications equipment and facilities	
Owner:	Personnel	
Escalation Owner:	Personnel	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	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 regularly determine skill levels and training requirements In the event of risk's execution: • Provide training facilities to reverse obsolescence of skills	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R* [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R24	
Risk Name:	Inability to evaluate staff effectiveness or suitability	
Risk Description:	Repository is incapable of effectively determining the extent to which staff are capable of achieving business objectives.	
Is this Risk Relevant?:	• Does the repository maintain policies and procedures to review staff performance?	
Example Risk Manifestation(s):	• Repository has no record of performance levels of individuals within its staff or means to effectively identify training requirements	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	X
	Operations and service delivery	
	Hardware, software or communications equipment and facilities	
Owner:	Management	
Escalation Owner:	Management	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • 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:	→R01 [contagious] →R02 [contagious] →R19 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

7.3.3 Financial Management

Risk Identifier:	R25	
Risk Name:	Finances insufficient to meet repository commitments	
Risk Description:	Finances are insufficient to adequately resource each of the business's integral activities.	
Is this Risk Relevant?:	• Does the repository undertake budgetary management? • Is financial investment necessary to achieve repository objectives? • Within its current business model, is the repository capable of self-sustainable income generation?	
Example Risk Manifestation(s):	• Repository operating on an annual loss • Insufficient resource to facilitate every intrinsic activity	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	X
	Operations and service delivery	
	Hardware, software or communications equipment and facilities	
Owner:	Budgeting	
Escalation Owner:	Budgeting	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Develop self-sustainability with charged-for services • Seek assurances of level of budget In the event of risk's execution: • Solicit additional funding to enable achievement of organisational objectives • Revise objectives if funding stream is insufficiently flexible • Maintain contingency fund where possible to meet shortfalls	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R* [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R26	
Risk Name:	Misallocation of finances	
Risk Description:	Repository allocates resources ill-advisedly, representing a poor investment, with benefits not proportional to expenditure.	
Is this Risk Relevant?:	• Is budgetary management and expenditure within the responsibilities of the repository?	
Example Risk Manifestation(s):	• Management invest heavily in software that offers functionality far in excess of operational requirements, when cheaper alternatives with limited, but adequate features are available	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	X
	Operations and service delivery	
	Hardware, software or communications equipment and facilities	
Owner:	Budgeting	
Escalation Owner:	Budgeting	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Establish policies and budgetary authorisation infrastructure to ensure appropriate use of repository funding In the event of risk's execution: • Revise policies to limit likelihood of subsequent misallocation	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R25 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R27	
Risk Name:	Liability for non-adherence to financial law or regulations	
Risk Description:	Repository is liable for failing to fulfil its responsibilities with respect to jurisdictional financial responsibilities.	
Is this Risk Relevant?:	• Is the repository subject to regulation that compels it to manage financial records in a particular fashion? • Does the repository solicit the advice of appropriate experts in order to fulfil its financial and accounting responsibilities?	
Example Risk Manifestation(s):	• Failure to address taxation requirements • Failure to conduct compulsory financial auditing	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	X
	Operations and service delivery	
	Hardware, software or communications equipment and facilities	
Owner:	Budgeting	
Escalation Owner:	Budgeting	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Monitor financial legislation and regulations in order to ensure that policies and procedures correspond to intrinsic requirements and prohibitions • Seek legal and professional financial advice to ensure adequate fulfilment of responsibilities In the event of risk's execution: • Establish policies and procedures to follow in the event of legislative challenge	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R04 [contagious] →R14 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R28	
Risk Name:	Financial shortfalls or income restrictions	
Risk Description:	Atypical operational circumstances result in budgetary shortfall or gap.	
Is this Risk Relevant?:	• To what extent is the repository's annual budgetary allocation assured? • Is the repository required to make any capital investments on a less than annual basis? • Is there a possibility of expenditure commitments arising without warning and with a requirement for immediate investment?	
Example Risk Manifestation(s):	• Unanticipated enforced expenditure, such as replacement of non-functioning technological assets • Expenditure on new server systems every four years, rendering investment during those budgeting periods far in excess of the other three-quarters of the time	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	X
	Operations and service delivery	
	Hardware, software or communications equipment and facilities	
Owner:	Budgeting	
Escalation Owner:	Budgeting	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Manage budgetary allocations, bearing in mind commitments that are less than annual • Calculate replacement timescale for repository resources and aim to pre-empt hardware failure by reinvesting regularly In the event of risk's execution: • Maintain residual emergency fund	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R25 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R29	
Risk Name:	Budgetary reduction	
Risk Description:	Repository's operational budget is reduced.	
Is this Risk Relevant?:	• To what extent are the repository's funding streams assured? • What proportion of budget is controlled and allocated externally as opposed to self-generated?	
Example Risk Manifestation(s):	• Local recession provokes budgetary reduction of government financed repository	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	X
	Operations and service delivery	
	Hardware, software or communications equipment and facilities	
Owner:	Budgeting	
Escalation Owner:	Budgeting	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Develop self-sustainability with charged-for services • Seek assurances of level of budget In the event of risk's execution: • Solicit additional funding to enable achievement of organisational objectives • Revise objectives if funding stream is insufficiently flexible • Maintain residual fund where possible to meet shortfalls	
Risk Relationships:	→R02 [contagious] →R25 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

7.3.4 Technical Infrastructure and Security

Risk Identifier:	R30	
Risk Name:	Hardware failure or incompatibility	
Risk Description:	System hardware is rendered incapable of facilitating current business objectives.	
Is this Risk Relevant?:	• Are policies and procedures in place to monitor the adequacy of hardware technologies amid changing community requirements and external influences? • What service level guarantees are offered from third-party hardware service providers? • Is a proportion of staff time allocated to determining the ongoing suitability and operational functionality of hardware?	
Example Risk Manifestation(s):	• Server's power supply burns out, rendering hardware unusable	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	
	Operations and service delivery	
	Hardware, software or communications equipment and facilities	X
Owner:	Technical	
Escalation Owner:	Technical	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Allocate a proportion of staff time to monitoring the ongoing suitability of repository hardware and assessing the potential value of emerging technologies • Evaluate effects of system changes prior to their implementation • Pre-empt hardware failure with anticipatory investment In the event of risk's execution: • Seek formal assurances or SLAs from hardware suppliers or providers of third-party hardware services	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R32 [contagious] →R35 [contagious] →R52 – 79 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R31	
Risk Name:	Software failure or incompatibility	
Risk Description:	System software is rendered incapable of facilitating current business objectives.	
Is this Risk Relevant?:	• Are policies and procedures in place to monitor the adequacy of software technologies amid changing community requirements and external influences? • What service level guarantees are offered from third-party software service providers? • Is a proportion of staff time allocated to determining the ongoing suitability and operational functionality of software?	
Example Risk Manifestation(s):	• Software update breaks dependencies of other core software services	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	
	Operations and service delivery	
	Hardware, software or communications equipment and facilities	X
Owner:	Technical	
Escalation Owner:	Technical	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Allocate a proportion of staff time to monitoring the ongoing suitability of repository software and assessing the potential value of emerging technologies • Evaluate effects of system changes prior to their implementation • Pre-empt software obsolescence with anticipatory investment In the event of risk's execution: • Seek formal assurances or SLAs from software suppliers or providers of third-party software services	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R32 [contagious] →R35 [contagious] →R52 – 79 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R32	
Risk Name:	Hardware or software incapable of supporting emerging repository aims	
Risk Description:	Technical infrastructure, while adequate for meeting current aims, is incapable of meeting new requirements resulting from organisation's natural evolution.	
Is this Risk Relevant?:	• Are additional technical facilities required to facilitate the repository's anticipated development? • To what extent is the repository's current service level likely to increase over time?	
Example Risk Manifestation(s):	• Technical infrastructure is insufficiently scalable to handle an anticipated escalation in number of objects or requests • Hardware is incompatible with emerging operation systems	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	
	Operations and service delivery	
	Hardware, software or communications equipment and facilities	X
Owner:	Technical	
Escalation Owner:	Technical	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Allocate a proportion of staff time to monitoring the scalability and compatibility of repository technologies with respect to emerging organisational aims	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R52 – 79 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R33	
Risk Name:	Obsolescence of hardware or software	
Risk Description:	Core technology is no longer current or is incongruent with that of most comparable organisations.	
Is this Risk Relevant?:	• Do vendors of currently employed hardware and software technologies offer a guaranteed period of support? • Are hardware and software technologies employed widely within contemporary and comparable organisations? • What is the mean-time-between-failure associated with the repository's chosen technologies?	
Example Risk Manifestation(s):	• Operating systems no longer supported by vendor, and therefore security updates are no longer being made available.	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	
	Operations and service delivery	
	Hardware, software or communications equipment and facilities	X
Owner:	Technical	
Escalation Owner:	Technical	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Allocate a proportion of staff time to monitoring the ongoing suitability of repository technologies and assessing the potential value of emerging technologies • Pre-empt technological obsolescence with anticipatory investment	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R52 – 79 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R34	
Risk Name:	Media degradation or obsolescence	
Risk Description:	Storage media deteriorates, limiting the extent to which it can be written to and read from.	
Is this Risk Relevant?:	• Does the repository preserve digital content on removable media such as tapes, optical disks and flash devices? • Are employed storage media formats used widely within contemporary and comparable organisations? • Is the mean lifetime of relied upon media technologies understood and documented?	
Example Risk Manifestation(s):	• Tape-stored content is inaccessible or corrupted due to physical deterioration of magnetic tape • Contemporary tape drives are incapable of reading dated storage media which is prolific throughout archive	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	
	Operations and service delivery	
	Hardware, software or communications equipment and facilities	X
Owner:	Technical	
Escalation Owner:	Technical	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Allocate a proportion of staff time to monitoring the expected lifetime of storage media and assessing the potential value of emerging technologies • Pre-empt media obsolescence with anticipatory investment In the event of risk's execution: • Maintain redundant copies of information objects • Establish policies and procedures to extract archived materials from degraded media	
Risk Relationships:	→R02 [contagious] →R52 – 79 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R35	
Risk Name:	Exploitation of security vulnerability	
Risk Description:	Shortcoming in repository's security provisions is identified and used to gain unauthorised access.	
Is this Risk Relevant?:	• Are vulnerabilities conceivably evident within repository's physical and system security? • Is it possible that individuals internal or external to the repository might be motivated to compromise system security to acquire or vandalise materials? • Are archived materials stored on network accessible computers?	
Example Risk Manifestation(s):	• Unpatched software security loophole hack • Intruder gains physical access to repository through a security door that is wedged open	
Nature of Risk:	Physical environment	X
	Personnel, management and administration procedures	
	Operations and service delivery	
	Hardware, software or communications equipment and facilities	X
Owner:	Technical	
Escalation Owner:	Technical	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Establish and regularly evaluate policies and procedures for physical and software security in accordance with relevant standards • Limit execution of non-essential services • Update software with latest security patches • Allocate staff time to analyse attempted security compromises and monitor security sources for details of known vulnerabilities • Compel users to change passwords frequently In the event of risk's execution: • Rebuild system to ensure there are no residual effects of system compromise	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R36 [contagious] →R37 [contagious] →R38 [contagious] →R42 [contagious] →R46 [contagious →R52 – 79 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R36	
Risk Name:	Unidentified security compromise, vulnerability or information degradation	
Risk Description:	Security exploitation or vulnerability occurs and is not monitored or identified by repository staff.	
Is this Risk Relevant?:	• Are mechanisms in place to identify all system access attempts? • Are mechanisms in place to determine when and how changes to stored content have taken place? • Are system logs regularly analysed to seek evidence of security breaches or attempted breaches?	
Example Risk Manifestation(s):	• System is hacked and key logger installed without knowledge of systems staff	
Nature of Risk:	Physical environment	X
	Personnel, management and administration procedures	
	Operations and service delivery	
	Hardware, software or communications equipment and facilities	X
Owner:	Technical	
Escalation Owner:	Technical	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Undertake appropriate measures to limit likelihood of system compromises, and implement monitoring to detect where attempts have taken place in accordance with relevant standards In the event of risk's execution: • Allocate staff time to analyse system logs for details of security compromises • Rebuild system to ensure there are no residual effects	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R42 [contagious] →R46 [contagious →R52 – 79 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R37	
Risk Name:	Physical intrusion of hardware storage space	
Risk Description:	Intruder gains access to area within which repository technical hardware is physically located.	
Is this Risk Relevant?:	• Are vulnerabilities conceivably evident within repository's physical security? • Is it possible that individuals internal or external to the repository might be motivated to compromise system security to acquire or vandalise materials?	
Example Risk Manifestation(s):	• Intruder breaks into repository, bypassing security measures	
Nature of Risk:	Physical environment	X
	Personnel, management and administration procedures	
	Operations and service delivery	
	Hardware, software or communications equipment and facilities	
Owner:	Technical	
Escalation Owner:	Technical	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Establish, test and regularly evaluate policies and procedures for physical security in accordance with relevant standards	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R42 [contagious] →R46 [contagious →R52 – 79 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R38	
Risk Name:	Remote or local software intrusion	
Risk Description:	Repository suffers software intrusion conducted either from onsite or from a remote location, by bypassing network security provisions.	
Is this Risk Relevant?:	• Are vulnerabilities conceivably evident within repository's system security? • Is it possible that individuals internal or external to the repository might be motivated to compromise system security to acquire or vandalise materials? • Are archived materials stored on network accessible computers?	
Example Risk Manifestation(s):	• Hacker remotely exploits server software security via secure shell tunnelling, executing malicious code on the server	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	
	Operations and service delivery	
	Hardware, software or communications equipment and facilities	X
Owner:	Technical	
Escalation Owner:	Technical	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	• Establish and regularly evaluate policies and procedures for software security in accordance with relevant standards • Limit execution of non-essential services • Update software with latest security patches • Allocate staff time to analyse attempted security compromises and monitor security sources for details of known vulnerabilities • Compel users to change passwords frequently In the event of risk's execution: • Rebuild system to ensure there are no residual effects of system compromise	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R42 [contagious] →R46 [contagious →R52 – 79 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R39	
Risk Name:	Local destructive or disruptive environmental phenomenon	
Risk Description:	Repository business activities are affected by circumstances that originate externally to the repository, with localised consequences.	
Is this Risk Relevant?:	• Is the repository likely to be exposed to adverse or extreme weather conditions? • Is the repository under threat from geological or man-made dangers (such as earthquakes, volcanoes, mining-related subsidence or coastal erosion)?	
Example Risk Manifestation(s):	• Hurricane, tornado or typhoon in nearby vicinity • Earthquake	
Nature of Risk:	Physical environment	X
	Personnel, management and administration procedures	
	Operations and service delivery	
	Hardware, software or communications equipment and facilities	
Owner:	Technical	
Escalation Owner:	Technical	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Monitor for likelihood of applicable environmental concerns • Take physical precautions against the most locally profound threats, such as installing hurricane-proof windows In the event of risk's execution: • Establish redundant storage facilities at remote location	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R42 [contagious] →R46 [contagious] →R52 – 79 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R40	
Risk Name:	Accidental system disruption	
Risk Description:	Business activities are adversely affected by non-deliberate intervention, or intervention that was not intended to result in these outcomes.	
Is this Risk Relevant?:	• Do repository systems permit members of staff to perform interactions that are contrary to agreed policies or procedures? • Are interactions reversible?	
Example Risk Manifestation(s):	• Staff member accidentally stops integral repository software services • Content is inadvertently deleted during its ingest	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	
	Operations and service delivery	X
	Hardware, software or communications equipment and facilities	X
Owner:	Technical	
Escalation Owner:	Technical	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Develop systems to limit extent to which non-valid interactions, or those that contradict policy can physically occur • Ensure staff are well trained in use of systems and informed of the importance of checking their interactions prior to execution In the event of risk's execution: • Identify reason for accidental action and introduce measures to disallow or dissuade users from repeating the error	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R52 – 79 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R41	
Risk Name:	Deliberate system sabotage	
Risk Description:	Business activities are adversely affected by measures intended to have these effects.	
Is this Risk Relevant?:	• Is it conceivable that individuals may seek to maliciously damage repository content or systems? • To what extent are system interactions, or those undertaken by circumventing the system, reversible? • Are members of staff that leave the organisation accompanied off-site and stripped of system access and authorisations?	
Example Risk Manifestation(s):	• e-Terrorism or physical (conventional) terrorism • Disaffected staff members maliciously vandalise systems	
Nature of Risk:	Physical environment	X
	Personnel, management and administration procedures	X
	Operations and service delivery	X
	Hardware, software or communications equipment and facilities	X
Owner:	Technical	
Escalation Owner:	Technical	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Maintain, test and revise physical and software security in accordance with relevant standards • Monitor for suspicious network activity or physical activity that appears unusual • Remove staff members or ex-staff members that are likely to be disaffected and immediately revoke system privileges In the event of risk's execution: • Ensure as far as possible that all system interactions are reversible • Ensure availability of redundant copies of system state and archived information at remote geographical location	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R42 [contagious] →R46 [contagious] →R52 – 79 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R42	
Risk Name:	Destruction or non-availability of repository site	
Risk Description:	Repository's physical premises are destroyed or rendered permanently or temporarily unusable.	
Is this Risk Relevant?:	• Are the repository's operational activities undertaken within a single physical building or group of buildings within a small geographical area? • Are redundant system and storage facilities established?	
Example Risk Manifestation(s):	• Fire damage • Asbestos found within building	
Nature of Risk:	Physical environment	X
	Personnel, management and administration procedures	
	Operations and service delivery	
	Hardware, software or communications equipment and facilities	
Owner:	Technical	
Escalation Owner:	Technical	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Maintain, test and revise physical and software system security policies in accordance with relevant standards In the event of risk's execution: • Establish redundant storage facilities capable of becoming operational base	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R52 – 79 [contagious] →R52 – 79 [explosive]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R43	
Risk Name:	Non-availability of core utilities	
Risk Description:	Key third-party, externally originating services suffer from temporary disruption, and are not available.	
Is this Risk Relevant?:	• Does repository rely upon availability of externally provided utilities such as gas, electricity, network services or water?	
Example Risk Manifestation(s):	• Temporary disruption to repository's electrical supplies	
Nature of Risk:	Physical environment	X
	Personnel, management and administration procedures	
	Operations and service delivery	
	Hardware, software or communications equipment and facilities	
Owner:	Management	
Escalation Owner:	Management	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Establish service level agreements or service commitments with utility provider In the event of risk's execution: • Establish internal means to nullify disruption wherever possible, such as installing a petrol electricity generator and UPS systems	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R42 [contagious] →R52 – 79 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R44	
Risk Name:	Loss of other third-party services	
Risk Description:	Other third-party services that the repository relies upon suffer disruption.	
Is this Risk Relevant?:	• Does the repository sub-contract any of its repository activities? • Does the repository rely upon any other third-party services such as cleaning or catering?	
Example Risk Manifestation(s):	• The web hosting company serving the repository's information dissemination systems goes out of business • Repository's catering company takes industrial action and staff are unable to receive meals	
Nature of Risk:	Physical environment	X
	Personnel, management and administration procedures	
	Operations and service delivery	X
	Hardware, software or communications equipment and facilities	X
Owner:	Management	
Escalation Owner:	Management	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Establish service level agreements or service commitments with third-party provider In the event of risk's execution: • Establish internal means to nullify disruption wherever possible	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R42 [contagious] →R52 – 79 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R45	
Risk Name:	Change of terms within third-party service contracts	
Risk Description:	Conditions with which third-party services are delivered change substantially.	
Is this Risk Relevant?:	• Are third-party service or utilities contracts subject to renewal or due to be renegotiated?	
Example Risk Manifestation(s):	• Electricity prices escalate • Web hosting service provider withdraws a relied-upon technology from its servers	
Nature of Risk:	Physical environment	X
	Personnel, management and administration procedures	X
	Operations and service delivery	X
	Hardware, software or communications equipment and facilities	X
Owner:	Management	
Escalation Owner:	Management	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Establish lasting service level agreements with third-party provider with minimal scope for their subsequent renegotiation In the event of risk's execution: • Implement policy to seek alternative service providers capable of offering more favourable terms	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R42 [contagious] →R52 – 79 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R46	
Risk Name:	Destruction of primary documentation	
Risk Description:	Repository documentation is partially or completed destroyed.	
Is this Risk Relevant?:	• Is repository documentation maintained and stored within the principal repository site? • Are multiple copies of documentation maintained and stored?	
Example Risk Manifestation(s):	• Fire damage within repository's administrative offices destroys contracts and policy documentation	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	X
	Operations and service delivery	X
	Hardware, software or communications equipment and facilities	X
Owner:	Management	
Escalation Owner:	Management	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Maintain multiple electronic and hard copies of documentation stored in multiple locations	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R12 [contagious] →R52 – 79 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R47	
Risk Name:	Inability to evaluate effectiveness of technical infrastructure and security	
Risk Description:	Repository is incapable of effectively determining the extent to which its technical infrastructure and security provisions are capable of facilitating business objectives.	
Is this Risk Relevant?:	• Does the repository maintain policies and procedures to verify and record attempted security compromises? • Does the repository maintain policies and procedures to identify non-authorised or inappropriate system interactions? • Does the repository maintain policies and procedures to ensure the ongoing suitability and functionality of hardware and software technologies and storage media? • Are mechanisms to determine the effectiveness of technical and security provisions exploited on a regular basis?	
Example Risk Manifestation(s):	• Repository has no mechanisms to test security provisions or to evaluate the effectiveness of technological infrastructure	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	X
	Operations and service delivery	
	Hardware, software or communications equipment and facilities	X
Owner:	Management	
Escalation Owner:	Management	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Establish internal means of assessment including risk management • Seek relevant external certification in order to demonstrate competence	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R19 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

7.3.5 Acquisition and Ingest

Risk Identifier:	R48	
Risk Name:	Structural non-validity or malformedness of received packages	
Risk Description:	Received packages fail to correspond to what repository expects or is capable of preserving.	
Is this Risk Relevant?:	• Does repository define the structure that should be conformed to by submitted content? • Does repository stipulate acceptable formats?	
Example Risk Manifestation(s):	• Deposited content is encoded in a format that is unsupported by the repository • Deposited XML-encoded content does not validate against the schema provided by the repository	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	
	Operations and service delivery	X
	Hardware, software or communications equipment and facilities	
Owner:	Ingest	
Escalation Owner:	Ingest	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Develop definition for submission package structure • Establish list of acceptable formats for submission • Communicate definition to depositors and producers In the event of risk's execution: • Maintain policy and procedure to determine whether package is disposed of, returned or ingested	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R49 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R49	
Risk Name:	Incompleteness of submitted packages	
Risk Description:	Received packages do not contain information that is necessary to facilitate their preservation.	
Is this Risk Relevant?:	• Does repository define the structure that should be conformed to by submitted content? • Does repository stipulate metadata requirements for submitted content?	
Example Risk Manifestation(s):	• Submitted package lacks metadata information that, in accordance with contracts, must accompany all deposited content	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	
	Operations and service delivery	X
	Hardware, software or communications equipment and facilities	X
Owner:	Ingest	
Escalation Owner:	Ingest	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Develop definition for submission package structure • Establish list of acceptable formats for submission • Communicate definition to depositors and producers In the event of risk's execution: • Maintain policy and procedure to determine whether package is disposed of, returned or ingested	
Risk Relationships:	→R01 [contagious] →R02 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R50	
Risk Name:	Externally motivated changes or maintenance to information during ingest	
Risk Description:	Between the points of receipt and the creation of an archivable object the received package is subjected to changes that are not sanctioned or implemented by the repository.	
Is this Risk Relevant?:	• Does repository obtain full physical and intellectual control of submitted content?	
Example Risk Manifestation(s):	• An intrinsic part of a submitted object is not included within the deposited package and instead is remotely referenced. During the process of ingest this remote object is subject to alteration by external actors	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	
	Operations and service delivery	X
	Hardware, software or communications equipment and facilities	
Owner:	Ingest	
Escalation Owner:	Ingest	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Ensure that sole, complete physical and intellectual control is obtained over received object In the event of risk's execution: • Maintain policy and procedure to determine whether package is disposed of, returned or ingested	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R52 – 79 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R51	
Risk Name:	Archival information cannot be traced to a received package	
Risk Description:	An archival object cannot be traced to a corresponding received package or selection of packages.	
Is this Risk Relevant?:	• Are policies and procedures in place to validate that archived content corresponds with what was originally submitted? • Is ingested content subject to transformation to an archival package?	
Example Risk Manifestation(s):	• Repository cannot identify the origins of an archived package in order to ensure that its integrity has been adequately preserved	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	
	Operations and service delivery	X
	Hardware, software or communications equipment and facilities	
Owner:	Ingest	
Escalation Owner:	Ingest	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Record appropriate provenance information, detailing interactions undertaken during receipt and ingest process In the event of risk's execution: • Maintain policy and procedure to determine whether package is disposed of, returned or retained	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R55 [contagious] →R60 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

7.3.6 Preservation and Storage

Risk Identifier:	R52	
Risk Name:	Loss of confidentiality of information	
Risk Description:	Information protected by confidentiality agreements is made available to communities, in contravention of those agreements.	
Is this Risk Relevant?:	• Is repository bound by requirements to maintain information confidentiality?	
Example Risk Manifestation(s):	• Repository authorisation subsystems fail and commercially sensitive information is exposed to a community that is considerably wider than that to whom, according to the relevant deposit agreement, access may be legitimately afforded	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	
	Operations and service delivery	X
	Hardware, software or communications equipment and facilities	
Owner:	Preservation	
Escalation Owner:	Preservation	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Ensure policies and procedures are conceived with due consideration of any confidentiality requirements that the repository is subject to • Ensure software and hardware systems and preservation strategies are capable of meeting requirements of policies In the event of risk's execution: • Implement policy to withdraw availability of confidential materials and invoke treatment strategies to alleviate loss of reputation	
Risk Relationships:	→R01 [contagious] →R02 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R53	
Risk Name:	Loss of availability of information and/or service	
Risk Description:	Repository is unable to provide a comprehensive range of services or access to all of its information holdings for which access ought to be available.	
Is this Risk Relevant?:	• Does repository commit to defined service levels? • Does repository provide assurances of information availability?	
Example Risk Manifestation(s):	• Repository's servers fail, rendering a proportion of its collections inaccessible, although contracts stipulate that access should be afforded	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	
	Operations and service delivery	X
	Hardware, software or communications equipment and facilities	
Owner:	Preservation	
Escalation Owner:	Preservation	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Ensure policies and procedures are conceived with due consideration of any service levels that the repository has committed to • Ensure software and hardware systems and preservation strategies are capable of meeting service levels In the event of risk's execution: • Invoke treatment strategies to alleviate loss of reputation or trust	
Risk Relationships:	→R01 [contagious] →R02 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R54	
Risk Name:	Loss of authenticity of information	
Risk Description:	Repository is incapable of demonstrating that information objects are what they purport to be.	
Is this Risk Relevant?:	• Does repository commit to the preservation of information authenticity?	
Example Risk Manifestation(s):	• Repository is unable to demonstrate the authenticity of preserved records that purport to describe government departmental expenditure	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	
	Operations and service delivery	X
	Hardware, software or communications equipment and facilities	
Owner:	Preservation	
Escalation Owner:	Preservation	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Ensure policies and procedures are conceived with due consideration of authenticity requirements • Maintain and review policies and procedures to ensure adequate recording of provenance information to demonstrate that archived material represents authentic representation of what was initially deposited or received • Ensure software and hardware systems and preservation strategies are capable of preserving authenticity In the event of risk's execution: • Invoke treatment strategies to alleviate loss of reputation or trust	
Risk Relationships:	→R01 [contagious] →R02 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R55	
Risk Name:	Loss of integrity of information	
Risk Description:	Repository is incapable of demonstrating that the integrity of information has been maintained since its receipt, and that what is stored corresponds exactly with what was originally received.	
Is this Risk Relevant?:	• Does repository commit to preservation of information integrity?	
Example Risk Manifestation(s):	• Records documenting government expenditure have been subjected to unauthorised or unanticipated changes, rendering them no longer representative of originally deposited content	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	
	Operations and service delivery	X
	Hardware, software or communications equipment and facilities	
Owner:	Preservation	
Escalation Owner:	Preservation	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Ensure policies and procedures are conceived with due consideration of integrity requirements • Maintain and review policies and procedures to ensure adequate recording and comparison of checksums to demonstrate that archived information has suffered no loss of integrity since its deposit or receipt • Ensure software and hardware systems and preservation strategies are capable of preserving information integrity In the event of risk's execution: • Invoke treatment strategies to alleviate loss of reputation or trust	
Risk Relationships:	→R01 [contagious] →R02 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R56	
Risk Name:	Unidentified information change	
Risk Description:	Repository is incapable of tracking or monitoring where one or more changes to archived information has taken place.	
Is this Risk Relevant?:	• Are repository mechanisms available to identify where preserved information has been subject to interactions or change?	
Example Risk Manifestation(s):	• Repository has failed to record or maintain adequate checksum information to detect where changes have been made to archived information	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	X
	Operations and service delivery	X
	Hardware, software or communications equipment and facilities	X
Owner:	Preservation	
Escalation Owner:	Preservation	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Implement policies and procedures to record, calculate and compare checksum values for archived information on a regular basis In the event of risk's execution: • Implement policies and procedures to record, calculate and compare checksum values for archived information on a regular basis • Invoke treatment strategies to alleviate loss of reputation or trust	
Risk Relationships:	→R01 [contagious] →R02 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R57	
Risk Name:	Loss of non-repudiation of commitments	
Risk Description:	Repository is incapable of ensuring that commitments cannot later be denied by either of the parties involved.	
Is this Risk Relevant?:	• Does repository engage in agreements where obligations are assumed by contracting parties?	
Example Risk Manifestation(s):	• Repository fails to record details of transactions with contractor who later denies that they have agreed to the information exchanged, and its implied obligations	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	X
	Operations and service delivery	X
	Hardware, software or communications equipment and facilities	
Owner:	Preservation	
Escalation Owner:	Preservation	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Maintain and review policies and procedures to ensure contractual commitments are communicated, understood, recorded and agreed upon by both parties. In the event of risk's execution: • Implement policy to define appropriate procedural response, such as seeking legal advice to pursue enforcement of contract	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R16 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R58	
Risk Name:	Loss of information reliability	
Risk Description:	Repository is incapable of demonstrating the reliability of its information holdings.	
Is this Risk Relevant?:	• Does repository commit to preserve reliability of information?	
Example Risk Manifestation(s):	• Archived information within a meteorological data centre is regarded as being insufficiently reliable to form the basis for scientific research • A court of law refuses to admit archived information as evidence on the grounds that it is unreliable	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	
	Operations and service delivery	X
	Hardware, software or communications equipment and facilities	
Owner:	Preservation	
Escalation Owner:	Preservation	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Ensure policies and procedures are conceived with due consideration of reliability requirements • Maintain and review policies and procedures to ensure adequate recording and comparison of checksums to demonstrate that archived information has suffered no loss of integrity since its deposit or receipt • Maintain and review policies and procedures to ensure adequate recording of provenance information to demonstrate that archived material represents authentic representation of what was initially deposited or received • Ensure software and hardware systems and preservation strategies are capable of preserving information reliability In the event of risk's execution: • Invoke treatment strategies to alleviate loss of reputation or trust	
Risk Relationships:	→R01 [contagious] →R02 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R59	
Risk Name:	Loss of information provenance	
Risk Description:	Repository is incapable of demonstrating the provenance of its information holdings, and their traceability from receipt and through each interaction that they have been subject to.	
Is this Risk Relevant?:	• Are mechanisms in place to record the origins and lifecycle of an archived package and any transactions or interactions that it has been subject to?	
Example Risk Manifestation(s):	• Repository fails to document the preservation processes undertaken to convert a received Microsoft Word file into a plain text preservation master	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	
	Operations and service delivery	X
	Hardware, software or communications equipment and facilities	
Owner:	Preservation	
Escalation Owner:	Preservation	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Ensure policies and procedures are conceived with due consideration of provenance requirements • Maintain and review policies and procedures to record the origins and lifecycle of archived packages and any transactions or interactions that they have been subject to • Ensure software and hardware systems and preservation strategies are capable of maintaining and recording provenance information In the event of risk's execution: • Invoke treatment strategies to alleviate loss of reputation or trust	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R51 [contagious] →R69 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R60	
Risk Name:	Loss or non-suitability of backups	
Risk Description:	Repository is unable to retrieve content or system state information from backup mechanism.	
Is this Risk Relevant?:	• Does repository rely upon backups of its system or content to react to the loss or non-availability of primary digital resources? • Are backup systems built upon well-established and widely used technologies? • In the event of destruction or damage to the primary repository site, is the safety of backed-up materials also threatened?	
Example Risk Manifestation(s):	• Faced with the loss of primary archival information, the repository discovers that it is unable to restore content because backup tapes are irreparably corrupted	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	
	Operations and service delivery	X
	Hardware, software or communications equipment and facilities	X
Owner:	Technical	
Escalation Owner:	Technical	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Maintain multiple copies of backups • Store backed-up content in remote locations • Undertake regular 'fire-drill' tests to determine whether systems and data can be restored from backup In the event of risk's execution: • Recover as much content as possible, exploiting techniques such as digital archaeology and digital forensics • Invoke treatment strategies to alleviate loss of reputation	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R52-69 [explosive]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R61	
Risk Name:	Inconsistency between redundant copies	
Risk Description:	Where repository maintains multiple copies of archived information, one or more differs from peers.	
Is this Risk Relevant?:	• Does repository maintain multiple redundant copies of archived content? • Does repository employ mechanisms to check for inconsistencies between multiple copies? • Are policies and procedures in place to react to the discovery of such inconsistencies?	
Example Risk Manifestation(s):	• Repository maintains three redundant copies of archived information, but random checksum comparisons reveal that one is different from its peers	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	
	Operations and service delivery	X
	Hardware, software or communications equipment and facilities	X
Owner:	Preservation	
Escalation Owner:	Preservation	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Record and compare checksum information corresponding to redundant packages on a regular basis • Maintain system technologies and security to limit likelihood of data corruption or malfeasance In the event of risk's execution: • Conceive policies and procedures to react to the discovery of such inconsistencies – for instance, use an election system where the checksum values in the majority are assumed to be correct and the minority is/are disposed of and replaced	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R12 [explosive]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R62	
Risk Name:	Extent of what is within the archival object is unclear	
Risk Description:	Repository is incapable of determining the parts of the archival object that will be subject to ongoing preservation.	
Is this Risk Relevant?:	• Does repository define the scope and extent of its archival package format(s)? • Do policies and procedures exist to validate archival packages for completeness and correctness?	
Example Risk Manifestation(s):	• Repository fails to adequately define its archival package format	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	
	Operations and service delivery	X
	Hardware, software or communications equipment and facilities	
Owner:	Preservation	
Escalation Owner:	Preservation	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Conceive definition for archival package In the event of risk's execution: • Conceive policy to react to ambiguity surrounding archival object	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R12 [explosive]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R63	
Risk Name:	Inability to validate effectiveness of ingest process	
Risk Description:	Repository is incapable of asserting that integrity and authenticity were maintained during the process of ingesting digital information.	
Is this Risk Relevant?:	• Does the repository maintain policies and procedures to record and compare checksum values? • Does the repository maintain policies and procedures to evaluate and record the execution of repository processes and to check that their outputs are complete and correct? • Are mechanisms to determine the effectiveness of ingest procedures exploited on a regular basis?	
Example Risk Manifestation(s):	• Repository is unable to demonstrate that ingest procedures have resulted successfully in complete and correct archival packages	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	X
	Operations and service delivery	X
	Hardware, software or communications equipment and facilities	
Owner:	Preservation	
Escalation Owner:	Preservation	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Establish internal means of assessment including risk management • Seek relevant external certification in order to demonstrate effectiveness of ingest process	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R19 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R64	
Risk Name:	Identifier to information referential integrity is compromised	
Risk Description:	Where identifiers are applied to information, the repository is incapable of locating the archival package that corresponds to a given ID.	
Is this Risk Relevant?:	• Does repository apply or maintain existing persistent identifiers for information packages? • Is identifier potentially distinguishable from related information?	
Example Risk Manifestation(s):	• Repository maintains the use of the file path from the digital object's original environment as the identifier for the archived object, resulting in two distinct objects that originated from different locations sharing the duplicate identifer "C:\Documents and Settings\John Smith\Document.pdf" • Identifiers generated at ingest consist of the timestamp at the point of ingest, but two ingest systems operate simultaneously and duplicate identifiers are consequently applied	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	
	Operations and service delivery	X
	Hardware, software or communications equipment and facilities	
Owner:	Preservation	
Escalation Owner:	Preservation	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Define, document and review policies and procedures describing the means by which identifiers are associated with corresponding information packages and communicate this information widely within the organisation • Define and review policies and procedures describing the creation of identifiers to ensure their uniqueness, or mandating the adoption of third-party identifier technologies such as Handles, DOIs or PURLs In the event of risk's execution: • Define policy to respond to fracturing of relationship between identifiers and information • Invoke treatment strategies to alleviate loss of reputation	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R12 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R65	
Risk Name:	Preservation plans cannot be implemented	
Risk Description:	Repository is incapable of executing in practice the preservation planning it has undertaken.	
Is this Risk Relevant?:	• Is preservation planning undertaken within the repository with the anticipation that it will subsequently be implemented? • Does preservation planning reflect the extent of technological, financial and human resources available within the repository as well as its organisational objectives?	
Example Risk Manifestation(s):	• Repository's planned emulation strategy requires technological expertise to implement that is unavailable within the staff, and insufficient resource exists to contract with third-party developers to undertake the work	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	
	Operations and service delivery	X
	Hardware, software or communications equipment and facilities	
Owner:	Preservation	
Escalation Owner:	Preservation	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Aim to reflect the extent of technological, financial and human resources available within the repository as well as its organisational objectives when conceiving preservation plans • Seek additional resources to facilitate original plans In the event of risk's execution: • Implement policy to refine preservation plans to correspond more closely to that which is feasible within the organisation	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R67 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R66	
Risk Name:	Preservation strategies result in information loss	
Risk Description:	Exposure of an archived object to preservation plans results in loss or damage to one or more of its significant characteristics.	
Is this Risk Relevant?:	• Does repository offer a definition of acceptable loss that may result from preservation activities?	
Example Risk Manifestation(s):	• Repository's proposed migration strategy results in loss of 'look and feel' of archived documents, regarded as essential properties by user community	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	
	Operations and service delivery	X
	Hardware, software or communications equipment and facilities	
Owner:	Preservation	
Escalation Owner:	Preservation	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Evaluate preservation strategies in testbed environment prior to execution • Ensure procedures are reversible in the event of unexpected or inappropriate results In the event of risk's execution: • Define policies to describe the acceptable levels of loss tolerated by the repository	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R52-R69 [contagious] →R61 [explosive]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R67	
Risk Name:	Inability to validate effectiveness of preservation	
Risk Description:	Repository is incapable of effectively determining the extent to which its preservation activities are successful in terms of its business objectives.	
Is this Risk Relevant?:	• Does repository maintain policies and procedures to verify the preservation of information understandability, authenticity and integrity?	
Example Risk Manifestation(s):	• Repository lacks means to demonstrate continued preservation, including understandability to the appropriate user communities, of its holdings over a number of years, given the age of the repository and its holdings	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	
	Operations and service delivery	X
	Hardware, software or communications equipment and facilities	
Owner:	Preservation	
Escalation Owner:	Preservation	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Establish internal means of assessment including risk management • Seek relevant external certification in order to demonstrate competence	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R19 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R68	
Risk Name:	Non-traceability of received, archived or disseminated package	
Risk Description:	Packages cannot be traced to corresponding packages or groups of packages from an earlier point within the repository's information lifecycle.	
Is this Risk Relevant?:	• Are mechanisms in place to record the origins and lifecycle of information packages and any transactions or interactions that they have been subject to?	
Example Risk Manifestation(s):	• Repository fails to maintain appropriate documentation describing the origins and lifecycle of an archived package and any transactions or interactions to which it has been subject	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	X
	Operations and service delivery	X
	Hardware, software or communications equipment and facilities	
Owner:	Management	
Escalation Owner:	Management	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Record appropriate provenance information, detailing interactions undertaken during receipt, ingest, preservation and dissemination processes In the event of risk's execution: • Define policy and procedures to determine whether package should be disposed of, returned or retained	
Risk Relationships:	→R01 [contagious] →R02 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

7.3.7 Metadata Management

Risk Identifier:	R69	
Risk Name:	Metadata to information referential integrity is compromised	
Risk Description:	Associations between information packages and corresponding metadata are broken, and can no longer be traversed.	
Is this Risk Relevant?:	• Does repository maintain metadata records associated with archived information? • Is it conceivable that metadata records might become divorced from corresponding archived information? • How are associations defined and described?	
Example Risk Manifestation(s):	• Documentation describing the repository's directory structure, which represents relationships between metadata and corresponding objects, is irretrievably lost	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	X
	Operations and service delivery	X
	Hardware, software or communications equipment and facilities	
Owner:	Documentation	
Escalation Owner:	Documentation	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Define, document and review policies and procedures describing the means by which metadata are associated with corresponding information packages and communicate this information widely within the organisation • Define and review policies and procedures describing the metadata schema that will be used within the repository's activities In the event of risk's execution: • Define policy to respond to fracturing of relationship between metadata and information • Invoke treatment strategies to alleviate loss of reputation	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R52 - 69[contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R70	
Risk Name:	Documented change history incomplete or incorrect	
Risk Description:	Metadata recording interactions, implemented preservation strategies or procedures undertaken with respect to information packages are undocumented, or only partially documented.	
Is this Risk Relevant?:	• Are mechanisms in place to record the origins and lifecycle of an information package and any transactions or interactions that it has been subject to?	
Example Risk Manifestation(s):	• Repository fails to maintain appropriate documentation describing the origins and lifecycle of an archived package and any transactions or interactions that it has been subject to	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	X
	Operations and service delivery	X
	Hardware, software or communications equipment and facilities	
Owner:	Documentation	
Escalation Owner:	Documentation	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Ensure policies and procedures are conceived with due consideration of provenance requirements • Maintain and review policies and procedures to record the origins and lifecycle of archived packages and any transactions or interactions that it has been subject to • Ensure software and hardware systems and preservation strategies are capable of maintaining and recording provenance information In the event of risk's execution: • Invoke treatment strategies to alleviate loss of reputation or trust	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R60 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R71	
Risk Name:	Non-discoverability of information objects	
Risk Description:	Metadata supporting information package discovery are insufficient.	
Is this Risk Relevant?:	• Does repository make discovery metadata available to a user community, however small that community may be? • What degree of flexibility is offered to the user with respect to discovering archived content? • What systems are integral to the discovery of information objects?	
Example Risk Manifestation(s):	• A geophysical data centre records discovery metadata to facilitate searching only by name of data set, but researchers within the community wish to search based on the physical location where the data was acquired and the name of the instrument used	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	
	Operations and service delivery	X
	Hardware, software or communications equipment and facilities	X
Owner:	Documentation	
Escalation Owner:	Documentation	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Determine extent of discovery mechanisms and searchable fields in consultation with designated community • Communicate full range of available information discovery mechanisms to community In the event of risk's execution: • Introduce alternative means for information discovery based on perceived shortcomings	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R75 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R72	
Risk Name:	Ambiguity of understandability definition	
Risk Description:	Repository is unable to describe what understandability means with reference to their stakeholder communities' expectations or requirements.	
Is this Risk Relevant?:	• Does the repository define understandability with respect to its user communities' expectations and requirements?	
Example Risk Manifestation(s):	• Repository preserves information and associated metadata based on a perception of what is required by user communities that is not necessarily representative	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	X
	Operations and service delivery	X
	Hardware, software or communications equipment and facilities	
Owner:	Documentation	
Escalation Owner:	Documentation	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Define and regularly review the concept of understandability with respect to community's expectations, requirements and knowledge base • Make understandability definition available to community and solicit their feedback In the event of risk's execution: • Retrospectively introduce policy detailing understandability definition	
Risk Relationships:	→R01 [contagious] →R02 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R73	
Risk Name:	Shortcomings in semantic or technical understandability of information	
Risk Description:	Repository fails to maintain appropriately complete representation information to facilitate information understandability.	
Is this Risk Relevant?:	• Does repository record or refer to adequate representation information such as file format information? • Are understandability requirements referenced when determining minimal essential semantic or technical metadata?	
Example Risk Manifestation(s):	• Repository preserving social science data documents information about the *SPSS* format within which much of its content is encoded but fails to record the meaning of the acronyms used as field headings throughout these files	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	
	Operations and service delivery	X
	Hardware, software or communications equipment and facilities	
Owner:	Documentation	
Escalation Owner:	Documentation	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Record or refer to appropriate representation information such as file format information, taking into account community understandability requirements • Solicit community feedback as to the extent to which preserved information remains understandable	
Risk Relationships:	→R01 [contagious] →R02 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

7.3.8 Access and Dissemination

Risk Identifier:	R74	
Risk Name:	Non-availability of information delivery services	
Risk Description:	Repository is unable to provide access to information packages.	
Is this Risk Relevant?:	• What systems are required to provide dissemination services? • Does the repository offer a variety of alternative delivery services? • Do policies and procedures exist to describe the means by which information is disseminated?	
Example Risk Manifestation(s):	• Web server relied upon for dissemination of materials is off-line due to network services failure	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	
	Operations and service delivery	X
	Hardware, software or communications equipment and facilities	X
Owner:	Dissemination	
Escalation Owner:	Dissemination	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Define policies describing available information delivery services and communicate these to the user community • Implement appropriate systems to meet delivery policy requirements • Establish sufficiently robust technical infrastructure to satisfy demands of proposed delivery services	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R79 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R75	
Risk Name:	Authentication subsystem fails	
Risk Description:	Systems for limiting accessibility of information are insufficient, resulting in inappropriate accesses or failures to access.	
Is this Risk Relevant?:	• Is repository compelled by contracts or mandate to establish and maintain a means of limiting end-user access to archived information? • What systems are necessary to maintain the operation of the repository's authentication controls?	
Example Risk Manifestation(s):	• Individuals who are not entitled to have access to the content can access it. Repository system relies upon IP-based authentication, but since all users within University *x* access the web via a web proxy the application perceives any access from that campus as coming from a single IP, and every resident user gains access.	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	
	Operations and service delivery	X
	Hardware, software or communications equipment and facilities	X
Owner:	Dissemination	
Escalation Owner:	Dissemination	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Define policies describing authentication requirements to correspond with conditions expressed in deposit agreements and other regulatory, legislative or contextual provisions • Implement appropriate systems to meet authentication policy requirements • Establish sufficiently robust technical infrastructure to satisfy demands of proposed authentication services In the event of risk's execution: • Determine the shortcoming that led to authentication failure and subsequently remedy it • If system is self-aware of its failure, implement a policy to describe the appropriate reaction; for instance, upon failure refuse all access attempts	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R79 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R76	
Risk Name:	Authorisation subsystem fails	
Risk Description:	Systems to ensure appropriate allocation of system privileges are insufficient, resulting in incorrect rights allocations to users.	
Is this Risk Relevant?:	• Is the repository compelled by contracts or mandate to define and control multiple levels of end-user access? • What systems are necessary to maintain the operation of the repository's authorisation controls?	
Example Risk Manifestation(s):	• Authorisation system which allocates privileges based on database username look-ups fails because two distinct users are permitted to share the same username string	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	
	Operations and service delivery	X
	Hardware, software or communications equipment and facilities	X
Owner:	Dissemination	
Escalation Owner:	Dissemination	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Define policies describing authorisation requirements to correspond with conditions expressed in deposit agreements and other regulatory, legislative or contextual provisions • Implement appropriate systems to meet authorisation policy requirements • Establish sufficiently robust technical infrastructure to satisfy demands of proposed authorisation services In the event of risk's execution: • Determine the shortcoming that led to authorisation failure and subsequently remedy it • If system is self-aware of its failure, implement a policy to describe the appropriate reaction; e.g., upon failure restrict all user privileges	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R79 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R77	
Risk Name:	Inability to validate effectiveness of dissemination mechanism	
Risk Description:	Repository is incapable of effectively determining the extent to which its dissemination mechanisms are successful in terms of its overall business objectives.	
Is this Risk Relevant?:	• Does the repository maintain policies and procedures to verify and record the integrity, authenticity, provenance and understandability of disseminated information? • Does the repository maintain policies and procedures to determine usage rights and limit inappropriate access? • Are mechanisms to determine the effectiveness of delivery operations exploited on a regular basis?	
Example Risk Manifestation(s):	• Repository end-user feedback questionnaires provide a non-exhaustive set of multi-choice responses that restrict the extent to which responses reflect the success of the dissemination	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	X
	Operations and service delivery	X
	Hardware, software or communications equipment and facilities	X
Owner:	Dissemination	
Escalation Owner:	Dissemination	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Establish internal means of assessment including risk management • Seek relevant external certification in order to demonstrate effectiveness of dissemination	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R19 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R78	
Risk Name:	Loss of performance or service level	
Risk Description:	Repository is incapable of meeting service level goals in accordance with its business objectives.	
Is this Risk Relevant?:	• Does repository make a commitment to its stakeholder groups to offer a minimal level of service or performance?	
Example Risk Manifestation(s):	• Repository aims to deliver each object in less than 5 minutes after the request but it consistently takes 10 minutes per object	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	X
	Operations and service delivery	X
	Hardware, software or communications equipment and facilities	
Owner:	Dissemination	
Escalation Owner:	Dissemination	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Define realistic service levels and implement policies and procedures for their review and adjustment • Secure and allocate resources based on business priorities • Establish mechanisms to regularly review and if necessary adjust policies and procedures in order to ensure objectives are realised In the event of risk's execution: • Undertake appropriate internal enquiries to determine the shortcomings that led to failure and update policies accordingly	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R04 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

7.4 APPENDIX 4: PRELIMINARY STRUCTURE FOR THE AUDIT REPORT

As noted above it is our intention that this is the first iteration of this toolkit. We intend in due course to release a second version DRAMBORA as an online tool, with subsequent versions both as paper-based toolkits and online tools as we refine the tool in response to user comments and the audits that DCC and DPE are planning to execute as part of this process.

The final report that can be automatically produced at the end of the on-line version of the self-audit will include most of the information as entered by the auditor, and be enhanced with analytical material that would help the repository's senior management to initiate effective action on the identified risks.

An automatically generated report will require further formatting and editing in terms of language, layout and organisational details. It will be produced in a format that allows for some customisation, for example inclusion or exclusion of some sections of the report, and editing of textual information, but the risk scores will be locked for editing. The final output will be in the PDF format.

The sections of the automatically generated self-audit report will include:

1) Title page

2) Brief description of the repository

3) Mission and mandate of the repository

4) Stated objectives and goals of the repository

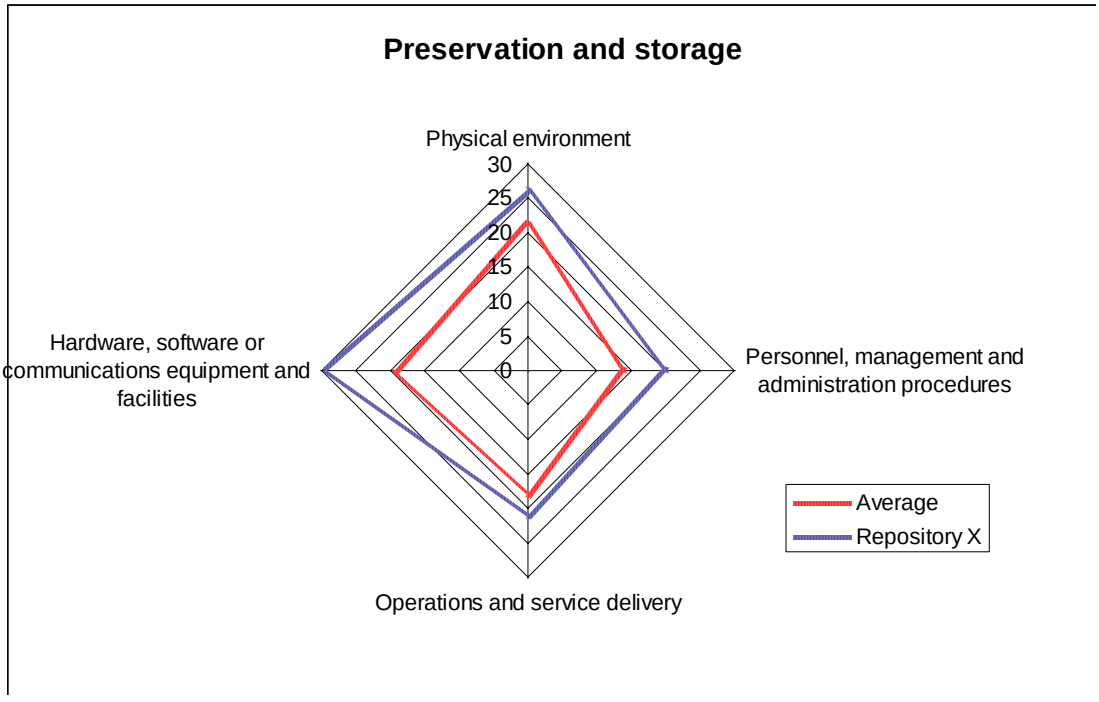
5) Activities of the repository
   Activities that were listed to achieve the stated goals. Ideally, these would be sorted either by functional group, or according to some other parameter that the auditor has chosen.

6) Risk register of the repository
   The risk register will be ordered according to parameters chosen by the auditor.

7) Comparison of the risk scores with average risk scores of similar repositories that have taken the self-audit

The results will be presented as a table and diagrams, much like the following:

Functional Class	Average	[Repository name]
Operational functions		
Acquisition & Ingest	12	11
Preservation & Storage	18	24
Metadata management	8	14
Access & dissemination	15	17
Support functions		
Organisation & management	9	6
Staffing	20	18
Financial management	26	24
Technical infrastructure and security	24	22



8) Risk management tasks

A list of risks and measures that have been identified to avoid, mitigate, transfer or accept them.

9) Recommendations

For continuing the risk management exercise, monitoring risks and the interval it is recommended to repeat the self-audit.

7.5 APPENDIX 5: ACRONYMS AND ABBREVIATIONS

AZ/NZS 4360	Australian and New Zealand standard for Risk Management
BASCS	Business Activity Structure Classification System
CASPAR	Cultural, Artistic and Scientific knowledge for Preservation, Access and Retrieval
CCLRC	Council of the Central Laboratory of the Research Councils
CCSDS	The Consultative Committee for Space Data Systems
CRL	Centre for Research Libraries
DCC	Digital Curation Centre
DIRKS	Design and Implementation of Recordkeeping Systems
DPE	DigitalPreservationEurope
DRAMBORA	Digital Repository Audit Method Based on Risk Assessment
ERPANET	Electronic Resource Preservation and Access Network
HATII	Humanities Advanced Technology and Information Institute
InterPARES	The International Research on Permanent Authentic Records in Electronic Systems
ISO 19011	*Guidelines for quality and/or environmental management systems auditing*
ISO 27001	*Information technology – Security techniques – Information security management systems - Requirements*
JISC	Joint Information Systems Committee
LOCKSS	Lots of Copies Keeps Stuff Safe
NARA	National Archives and Records Administration (USA)
nestor	Network of Expertise in long-term STOrage of digital Resources
OAIS	Open Archival Information System
OCLC	Online Computer Library Centre
RLG	Research Libraries Group
TRAC	Transparent Approach to Costing
UKOLN	UK Office for Library Networking
VRC	Virtual Remote Control

7.6 BIOGRAPHICAL SKETCHS OF THE AUTHORS

Andrew McHugh, advisory services manager for the DCC since 2004, leads a world-class team of digital curation practitioners in offering leading-edge expertise and insight in a range of issues. His most recent work at the DCC has involved leading its work in trusted repository Audit and Certification. McHugh also lectures on multimedia systems and design on the MSc in Information Technology run by the Computing Science Department at Glasgow.

Raivo Ruusalepp is currently involved in the audit and certification of digital repositories work of the EU DigitalPreservationEurope (DPE) project. He is employed at the National Archives of Netherlands and the Estonian Business Archives. Ruusalepp has an MA in computing applications for history from University of London and has worked with digital archives and electronic records management for more than ten years.

Seamus Ross, professor of Humanities Informatics and Digital Curation and director of Humanities Computing and Information Management at the University of Glasgow, runs HATII (Humanities Advanced Technology and Information Institute, of which he is the founding director. He is an associate director of the DCC, a member of the Scientific Board of the DELOS Digital Libraries Network of Excellence and Leader of its Digital Preservation Cluster, and principal director of DigitalPreservationEurope (DPE). He was Principal Director of ERPANET which was the precursor to DPE.

Hans Hofman is senior advisor on digital longevity at the Nationaal Archief of the Netherlands. He has acted as co-director of ERPANET. He is involved in several committees at government and municipal level with respect to metadata, digital preservation and open standards. On the international scene he is, co-investigator and representative of the Nationaal Archief in the Inter Pares 2 research project (http://www.interpares.org), since 2000 representing the Netherlands in the ISO TC46/SC11 on Records Management, in which committee he is chair of the Working Group on RM metadata, and he represents the Nationaal Archief in recent European projects such as the preservation cluster of the DELOS NOE, PLANETS and DigitalPreservationEurope.

7.7 APPENDIX 6: REFERENCES (INCLUDING RELATED STANDARDS)

7.7.1 Audit and Certification of Digital Repositories

Robin Dale, *Making Certification Real: Developing Methodology for Evaluating Repository Trustworthiness. RLG DigiNews*, Issue index: October 15, 2005, http://www.rlg.org/en/page.php?Page_ID=20793#article2

Deutsche Initiative für Netzwerkinformation E.V., Electronic Publishing Working Group, *DINI-Certificate Document and Publication Services. Draft Version*. (2007), http://www.dini.de/documents/DINI_certificate_eng_2006-10-12_draft.pdf

Susanne Dobratz, Astrid Schoger, *Digital Repository Certification: A Report from Germany*. *RLG DigiNews*, Issue index: October 15, 2005, http://www.rlg.org/en/page.php?Page_ID=20793#article3

ERPANET, *Workshop on Audit and Certification in Digital Preservation* (2004), http://www.erpanet.org/events/2004/antwerpen/index.php

nestor Working Group on Trusted Repositories Certification, *The Catalogue of Criteria for Trusted Digital Repositories*. *Version 1*. nestor Studies, no. 8 (2006), http://edoc.hu-berlin.de/series/nestor-materialien/8en/PDF/8en.pdf

RLG/NARA Task Force, *An Audit Checklist for the Certification of Trusted Digital Repositories* (2005), http://www.rlg.org/en/pdfs/rlgnara-repositorieschecklist.pdf

RLG/OCLC Task Force, *Trusted Digital Repositories: Attributes and Responsibilities* (2002), http://www.rlg.org/legacy/longterm/repositories.pdf

Seamus Ross, Andrew McHugh, *Audit and Certification of Digital Repositories: Creating a Mandate for the Digital Curation Centre (DCC)*. *RLG DigiNews*, Issue index: October 15, 2005, http://www.rlg.org/en/page.php?Page_ID=20793#article1

Seamus Ross, Andrew McHugh, *The Role of Evidence in Establishing Trust in Repositories*. *D-Lib Magazine*, July/August, vol. 12, nos 7/8 (Also published in *Archivi e Computer*, August 2006), http://www.dlib.org/dlib/july06/ross/07ross.html

Seamus Ross, Andrew McHugh, *The Digital Curation Centre Repository Pilot Audits: Results and Lessons*, (forthcoming a).

Seamus Ross, Andrew McHugh, *Preservation Pressure Points: Evaluating Diverse Evidence for Risk Management*, (forthcoming b).

World Bank, *Assessment of Organisational Capacity to Manage Records: A Top Level Checklist* (2004),
http://web.worldbank.org/WBSITE/EXTERNAL/EXTABOUTUS/EXTARCHIVES/0,,contentMDK:20035550~pagePK:36726~piPK:437378~theSitePK:29506,00.html

7.7.2 Digital Repositories

Rachel Heery, Sheila Anderson, *Digital Repositories Review* (2005),
http://www.jisc.ac.uk/uploaded_documents/digital-repositories-review-2005.pdf

Hans Hofman, Babak Hamidzadeh, Ken Hawkins, Bill Underwood, *Business-driven recordkeeping model. Version 5.0* (February 2007) (forthcoming by InterPARES-2)

National Council on Archives, *Your Data At Risk. Why you should be worried about preserving electronic records* (2005),
http://www.ncaonline.org.uk/materials/yourdataatrisk.pdf

7.7.3 Risk Management in Digital Preservation

Cornell University Library Virtual Remote Control (VRC) tool,
http://irisresearch.library.cornell.edu/VRC/methods.html

ERPANET *Risk Communication Tool* (2003),
http://www.erpanet.org/guidance/docs/ERPANETRiskTool.pdf

JISC, *Managing Risk: a Model Business Preservation Strategy for Corporate Digital Assets* (2005),
http://www.jisc.ac.uk/whatwedo/programmes/programme_preservation/programme_404/project_managingrisk.aspx

Gregory Lawrence, William Kehoe, Oya Rieger, William Walters, Anne Kenney, *Risk Management of Digital Information: A File Format Investigation*. CLIR Report no. 93 (2000),
http://www.clir.org/pubs/reports/pub93/pub93.pdf

Victoria Lemieux, *Managing Risks for Records and Information.* ARMA International (2004).

Nancy McGovern, Anne Kenney, Richard Entlich, William Kehoe, Ellie Buckley, *Virtual Remote Control. Building a Preservation Risk Management Toolbox for Web Resources. D-Lib Magazine*, vol. 10, no. 4, April 2004,
http://www.dlib.org/dlib/april04/mcgovern/04mcgovern.html

Seamus Ross, *Uncertainty, Risk, Trust, and Digital Persistency*, 2006 NHPRC Electronic Records Research Fellowships' Symposium Lecture, University of North Carolina at Chapel Hill, 6 October 2006 [a pre-print of the lecture is available form the erpaeprints server].

7.7.4 Risk Assessment and Management Literature

Institute of Risk Management, Association of Insurance and Risk Managers, ALARM (The National Forum for Risk Management in the Public Sector), *A Risk Management Standard* (2002),
http://www.theirm.org/publications/documents/Risk_Management_Standard_030820.pdf

Institute of Internal Auditors, *Code of Ethics*,
http://www.iia.org.uk/cms/IIA/uploads/2c9103-ea9f7e9fbe--7f73/2002CodeofEthics2.pdf

Treasury Board of Canada, Integrated Risk Management Framework (2001),
http://www.tbs-sct.gc.ca/pubs_pol/dcgpubs/RiskManagement/rmf-cgr_e.asp

UK Office of Government Commerce, *Successful Delivery Toolkit. Risk Management* (2005).

UK Treasury, *Orange Book. Management of Risk – Principles and Concepts* (2004),
http://www.hm-treasury.gov.uk/media/FE6/60/FE66035B-BCDC-D4B3-11057A7707D2521F.pdf

7.7.5 Operational Context Analysis Methodology

National Archives of Australia, *The DIRKS Manual: A Strategic Approach to Managing Business Information* (2003),
http://www.naa.gov.au/recordkeeping/dirks/dirksman/dirks.html

Collections Canada, *Business Activity Structure Classification System (BASCS) Guidance*,
http://www.collectionscanada.ca/information-management/002/007002-2089-e.html

7.7.6 Standards

AS/NZS 4360:2004 *Risk Management*,
HB 436:2004 *Risk Management Guidelines – Companion to AS/NZS 4360:2004*.
Cf. http://www.riskmanagement.com.au/

BS 7799-3:2006 *Information security management systems – Part 3: Guidelines for information security risk management.*

BS 25999-1:2006 *Business continuity management – Part 1: Code of practice.*

ISO/IEC Guide 73:2002 *Risk management – Vocabulary – Guidelines for use in standards*

ISO/IEC 13335-1:2004 *Information technology – Security techniques – Management of information and communications technology security – Part 1: Concepts and models for information and communications technology security management*

ISO 9001:2000 *Quality management systems – Requirements.*

ISO 14721:2003 *Space data and information transfer systems -- Open archival information system -- Reference model*

ISO 15489:2001 *Information and Documentation – Records Management. Part 1 & 2.*

ISO 17799:2005 *Information technology – Security techniques – Code of practice for information security management.*

ISO 19011:2002 *Guidelines for quality and/or environmental management systems auditing.*

ISO 27001:2005 *Information technology – Security techniques – Information security management systems – Requirements.*

7.7.7 Relevant Projects

Certification of Digital Archives Project, Center for Research Libraries (CRL) http://www.crl.edu and http://www.crl.edu/content.asp?l1=13&l2=58&l3=142

Digital Curation Centre (DCC), http://www.dcc.ac.uk/

DigitalPreservationEurope (DPE), http://www.digitalpreservationeurope.eu/

Digital Repository Infrastructure Vision for European Research (DRIVER), http://www.driver-repository.eu/

nestor Working Group on Trusted Repositories Certification, http://nestor.cms.hu-berlin.de/tiki/tiki-index.php?page=wg-repositories

RLG, Digital Repository Certification, http://www.rlg.org/en/page.php?Page_ID=580&projGo.x=33&projGo.y=12