A Risk Register for Digital Curation aligned with the OAIS reference model

Ana Raquel Correia Bairrão
raquel.bairrao@tecnico.ulisboa.pt

Instituto Superior Técnico, Lisboa, Portugal

June 2015

Abstract

A risk register can act as a knowledge base and guidance for analysing relevant risks affecting an organization. It represents a thorough research and understanding of the organization context to all levels of operation. Since the probability of emerging risks to occur rises overtime, it has become a necessity to adopt measures regarding assessment, mitigation, treatment and control of these risks, for long term data preservation. Data is an important asset nowadays. Having access to detailed information of data gives people the freedom to prevent or risk within the support of data assessment, representing business opportunities. The development of a Risk Management Plan in the design of Digital Curation solutions regarding the domain of an organization should be a common practice in organizations nowadays. Therefore, it is important that the organization follows the principles and guidelines of Risk Management, such as the ones given by the ISO 31000. By doing so, Digital Curation workflow of preserving, maintaining and adding value to data, would have a way to support the overall data life-cycle management. Although its not easy to implement a Risk Management Process in an organization, the purpose of this thesis is to bring enlightenment on where to start. This action will enable the identification of risks which can be misperceived within the organization. We propose a Risk Register, that is aligned with the business of Digital Curation, as well as the known standards like OAIS and TRAC for digital repositories trustworthiness and long-time preservation.

Keywords: Risk Management, Risk Register, Digital Curation, OAIS

1. Introduction

Risk identification is the first step of executing a risk assessment, during the Risk Management Process. [14] A risk register can act as a knowledge base [10] and guidance for analysing relevant risks affecting an organization. It represents a thorough research and understanding of the organization context to all levels of operation. [14]

To understand the usefulness of producing a risk register, one can start by analysing the graph in figure 1. The conclusion relies on the fact that, organizations, nowadays, face the challenge of executing a proper Risk Management due to a lack of sufficient data to support it.

![Risk Identification Breakdown](image-url)

Figure 1: Survey conducted by The Intelligence Unit of The Economic Times (EIU) of 208 risk management and regulatory compliance executives at retail, commercial, and investment banks equally balanced from North America, Europe, Asia-Pacific and the rest of the world (June 2014).
Risk Management [15] practice has been developed through time in order to meet the various needs and goals of an organization. Furthermore, the consistent adoption of a comprehensive framework in the definition of an organization processes helps to ensure that risk is managed effectively, efficiently and coherently across all areas of the organization. [5, 14] Although risk is an effect of uncertainty [15], the concern of understanding what might be a risk for a particular context of business is crucial for the development of business strategies.

Digital Curation is an ongoing process, alongside with the process of long-term digital preservation. [22] To maintain, preserve and add value to digital data throughout the data preservation lifecycle [8], a necessity raised for making an efficient digital data management [13], by identifying possible threats and mitigate identified risks. [22] Moreover, since digital data is shared among the research community, it is of relevance to have curated data in trusted digital repositories. [9] For curation to enhance the long-term value of digital data [8], Risk Management can act as a positive support to sustain the overall digital curation process. In hope it will bring sustainability for the lifetime activity of repositories, this strategy helps managing digital data assets such as business records, research data, cultural heritage collections, personal archives and other assets that represent value to repositories. [1, 22]

The outlook of the risk register is to allow for potential risks to be identified and analysed. This action relies on providing solid ground for risk evaluation and implementation of mitigation measures, designated as controls. [14, 22] The risk register aims to acknowledge digital repositories community of a baseline of risks which entail to support future decisions, related to the long-term lifetime of digital repositories business. [22] To summarize, this measure is intended to add value to data while executing the process of Digital Curation.

2. Problem and Motivation


Starting from this premise, we concluded that there isn’t a knowledge base [10] of identified risks for Digital Curation. Therefore, the problem we aim to address is how to start developing a knowledge base of risks for Digital Curation, having as guidelines the ISO 31000 Risk Management process [14] and the OAIS reference model for digital repositories. [10]

Moreover, figure 2 shows the results of a conducted survey on Digital Information Risks by Archives New Zealand. [2] One can underline important risk acknowledgments on which organizations:

- don’t have the means to understand the value of their assets;
- lack resources to manage information efficiently;
- are not aware of the existence of some information assets.

One can perceive the opportunity and need on which organizations should implement Risk Management as a practice, on the overall levels of operation. Furthermore, considering the value of digital information should be a priority to an organization. By using this measure, the business continuity of organizations would be re-evaluated from time to time, preventing possible losses and assuring digital data preservation for the long-term of its lifecycle.


ISO 31000 [14] standard pursues the goal to give organizations a generic guideline regarding the matter of design and implementation of a risk management plan. This standard provides a form to harmonize the existing management processes in an organization since it takes into account the various needs of the organization and can be applied throughout the life cycle of an organization, including its business strategies, operations, processes, activities, services and assets. [14] Within the Risk Management scope, it is important to notice the difference regarding the terms risk management and management of the risk. While the first one refers to the architecture principles, frameworks and processes for managing
risks effectively, the second one refers to the application of that architecture to specific risks that were identified. [16] Having understood the difference between these terms, it is next presented a conceptual map that addresses the principles for Risk Management, accordingly to the standard ISO 31000. [14]

The conceptual map for risk management principles illustrates the global context for this matter, explained in the next paragraph.

First, the organization should have a committed risk attitude towards the integration of risk management within their overall processes. Therefore, dialog with the stakeholders and management resources should be engaged to acquire knowledge of the business strategy and goals the organization intends to achieve. Having this into account, it is then possible to define the specific context of the organization. After collecting information from the internal and external factors outlined for the organization, it is possible to design a risk framework consistent with the risk criteria defined within the established context. Alongside with this, rises the identification of threats, vulnerabilities and risks based on the events that may affect the achievement of goals identified at the beginning of the risk management process.

Risk assessment is then applied within the risk profile identification, analysis and evaluation, in order to decide which are the appropriate techniques and controls to treat them. Risk management aims to create value for the organization, as it explicitly addresses uncertainty and takes in consideration the best available information to help the decision-making of stakeholders. Risk management is dynamic, iterative and responsive to change process, as well as transparent and aligned with the overall organization processes. The management of risk enables the continual improvement and enhancement of the organization.

4. Digital Curation

The general definition of Digital Curation, as defined by DCC 1, is:

"Digital curation involves maintaining, preserving and adding value to digital content throughout its entire lifecycle. The active management of digital material reduces threats to its long-term value and mitigates the risk of digital obsolescence. As well as reducing duplication of effort in digital object creation, curation enhances the long-term value of existing content by making it available for further use in a wide variety of contexts.” [18]

The lifecycle of digital curation involves the following steps, as it is defined by DCC 2:

Conceptualise: idealize a plan for the creation of digital objects, as well as ingestion methods and storage;
Create: generate digital objects and designate them accordingly to its metadata: descriptive, structural, technical, and administrative;

---

1As defined by the Digital Curation Centrehttp://www.dcc.ac.uk/digital-curation/what-digital-curation
2DCC - http://www.dcc.ac.uk/digital-curation/what-digital-curation
Access and use: make sure digital objects are accessible to its community, accounting for different user profiles regarding data privacy;

Appraise and select: evaluate and verify which digital objects need long-term data preservation. Document this information in form of guides, policies or legal requirements;

Dispose: not selected digital objects are disposed. Document this information in form of guides, policies or legal requirements;

Ingest: transfer digital objects to an archive, trusted digital repository or data centre. Document this information in form of guides, policies or legal requirements;

Preservation action: plan ahead digital preservation actions, to assure the integrity and authenticity of digital objects throughout its lifetime;

Reappraise: digital objects that fail validation measures are returned to "Appraise and select" step;

Store: take measures to safely storage digital objects, recurring to standards as a reference;

Access and reuse: data should be accessible to the community, taking into account different users profile and data privacy policies;

Transform: use digital preservation techniques to create new digital objects formats.

Figure 4 displays the Digital Curation lifecycle model, defined by Digital Curation Centre (DCC). 3

5. Reference Standards

Digital Repository Audit Method Based on Risk Assessment (DRAMBORA)

An important initiative of addressing Digital Curation through Risk Management was Digital Repository Audit Method Based on Risk Assessment [20]. This method used self-assessment repository audit, encouraging organizations to define their objectives, activities and assets before applying risk assessment to the identified risks within their organization. However, DRAMBORA risk assessment audit method relies on traditional preservation systems, being currently, an obsolete audit method. [5]

Open Archival Information System (OAIS)

The Open Archival Information System (OAIS) [10] reference model was published by the Consultative Committee for Space Data Systems. The goal of OAIS reference model is to offer the community a conceptual model of an archival system, alongside with a common language to address the repository business. [5] Figure 5 presents over view of the OAIS reference model.

Audit and Certification of Trustworthy Digital Repositories (TRAC)

---

3http://www.dcc.ac.uk/resources/curation-lifecycle-model
The Trustworthy Repositories Audit & Certification: Criteria and Checklist [9] idea is to provide a document describing the metrics of an OAIS compliant digital repository. It deals with organizational and technical infrastructure for secured repositories and embraces capabilities of certification for organizations to assume long-term preservation responsibilities. [5]

6. Proposed Solution
A risk register is a record of information about identified risks. [15] This solution follows the principles and guidelines, techniques and concepts provided by the ISO 31000 family standards. [14, 16, 15] To provide background on the terms used, a description is presented next, accordingly to ISO-Guide73 Risk Management - Vocabulary. [15]

**Assets** - anything that has value for an organization.

**Vulnerabilities** - properties of an asset that can be exploited, leading to an event with a consequence. This defines the level of exposure of an event.

**Events** - the occurrence or change of a particular set of circumstances. This defines the level of likelihood of a change happening;

**Consequences** - the outcome of an event, which affects organization goals. This defines the level of impact of the occurrence of an event.

**Risk** - effect of uncertainty on objectives. An effect can be positive or negative. Objectives are aspects such as financial, environment, applied to strategic or organization-wide levels. It is characterized by the relationship between potential events and consequences. The outcome is the combination of the consequences of an event and the associated likelihood. This defines the level of risk or severity;
Controls - implemented mitigation measures.

The proposed solution is as follows (see figure 6):

1. **Establishing the context for risk identification in Digital curation** - this was achieved by gathering information regarding the overall digital repositories structure: infrastructure, resources, activities, services and operations;

2. **Align this information with the concepts of the OAIS and TRAC reference models for digital repositories** - traceability of the concepts between OAIS [10], DRAMBORA [20] and TRAC [9] was produced;

3. **Identification of the assets, vulnerabilities, events, consequences, risks and possible controls** - using a set of questions;

4. **Insert the collected information in a risk assessment tool** - HoliRisk;

5. **Communicate the results** - to my team at INESC-ID and risk consultants;

6. **Use checklists, brainstorming and interviews techniques** - to validate the achieved results;

7. **Re-analyse the identified risks** - accordingly to the feedback provided by step 5;

8. **Re-do this iteration from step 2 to 7** - the number of times needed until finding a list of risks suitable for Digital Curation context.

On the ongoing process of retrieving information regarding step 2 of the proposed solution, the questions asked while conducting risk identification were:

1. What assets are of value for digital curation?
2. What are the main activities of digital repositories/preservation/curation?
3. How are the assets related to digital repositories activities?
4. To which vulnerabilities are these assets exposed to?
5. What is the level of exposure of the assets to vulnerabilities?
6. What events can incur from the exploitation of my assets vulnerabilities?
7. What is the likelihood for those events to occur?
8. What is the level of likelihood for these events to occur?
9. How can the occurrence of these events impact my assets?
10. How can this impact lead to a consequence?
11. How can these consequences affect digital repositories goals?
12. How does the likelihood of these events to occur and consequences impact derive possible risks?
13. What is the level of risk associated by the combination of the likelihood of these events to occur and consequences impact?
14. Are there any mitigation measures implemented?
7. A Risk Register for Digital Curation

While conducting this research work, it was possible to observe that TRAC follows the similar concepts used by the OAIS model, since they were produced by the same organization. In the case of DRAMBORA, it doesn’t consider an explanation regarding these concepts, although it uses them in the description of the identified assets and activities presented in this document. Therefore, after analysing DRAMBORA, was possible to achieve a traceability of the terms used and the concepts stated in the OAIS reference standard for Digital Curation.

Starting from this premise, suggested assets for Digital Curation, organized by their type, are: (i) Activities; (ii) Information Package; (iii) Digital Object; (iv) Metadata; (v) Infrastructure.

Next, the identification of suggested vulnerabilities, events, consequences, risks and controls was conducted, providing acknowledgement on which:

(i) identified assets present an answer to the questions 1, 2, and 3; (ii) identified vulnerabilities present an answer to the questions 4, and 5; (iii) identified events present an answer to the questions 6, 7, and 8; (iv) identified consequences represents an answer to the questions 9, 10, and 11; (v) identified risks represents an answer to the questions 12 and 13; (vi) identified controls represents an answer to the questions 14.

Figure 7: Workflow for the step two of the proposed solution

Figure 7 displays a visual workflow of steps regarding the second step of the proposed solution. The
intention is for the reader to have a view of the executed procedures in order to create a risk register. These automated procedures were possible due to the use of HoliRisk - a risk assessment tool, developed by our team at INESC-ID. [3] The remaining steps of the proposed solution worked as evaluation of the under development work. A practical application of the proposed solution was validated using two digital repositories case studies- LNEC and PWA.

8. Results
We were able to demonstrate that it is possible to put in practice the proposed solution, assuring that our understanding of the needed steps to follow when creating a risk register were accurate, namely:

(i) it is possible to use the concepts of the reference model OAIS to create a knowledge base for Digital Curation; (ii) it is possible to use these concepts to retrieve a list of risks for Digital Curation; (iii) it is possible to create a risk register for Digital Curation, applying the concepts of ISO 31000 [14] aligned with the concepts of the OAIS [10] model.

The results obtained reassured that the creation of a risk register represents a knowledge base for Digital Curation. The only adjustments that were taken in consideration were adding specifications of LNEC/PWA business. As an example, (i) as LNEC is a public institution, the vulnerability "V1 - Governamental funding" was added; (ii) as PWA is a web archive, the event "E1 - External attack (ex: bot's and webcrawlers)" was added.

The creation of a risk register helps on the storage of risks information overtime, enabling risk analysis, evaluation and treatment. The outcome of this data is what supports organizations decision-making towards new opportunities or prevents it of major losses.

The work reported herein was published as result of project deliverables for the European Comission project 4C [6, 23]. In addition, the papers [4, 22] were accepted and presented at Encontro Interccional de Arquivos [4](EIA2014) and Internacional Conference on Enterprise Information Systems [5] (ICEIS2015) conferences. A poster [21] was accepted and presented at International Digital Curation Conference (IDCC2015).

9. Conclusions and Future work
This work presented an approach to Risk Management applied to Digital Curation, acting as a guideline of thoughts on understanding the outlook of risks identification, supported by the creation of a risk register. It became clear while drawing the solution that, a profound understanding of the overall context of Digital Curation is a key point to identify the associations between assets, activities, vulnerabilities, events and consequences. This action enables a thorough risk identification and provides feedback for possible controls to be implemented.

The proposed solution provided a set of steps on how to create a risk register for Digital Curation. This solution is aligned with the reference standards ISO 31000 [14] for Risk Management, and OAIS [10] for digital repositories.

We were able to demonstrate that it is possible to put in practice the proposed solution, assuring that our understanding of the needed steps to follow when creating a risk register were accurate.

To summarize, the risk register is important as a support for risk assessment. This work describes how an organization can start to create their own risk register, following the guidelines of the proposed solution, and using a risk assessment tool such as HoliRisk.

As future work, I suggest the validation of the risk register to a broaden audience, on the context of Digital Curation. By doing this, the idea of conducting a Delphi technique [19, 12] for identification of risks seems suitable to act as a knowledge base of common risks for Digital Curation. This technique is suggested as another option to support risk identification while executing risk assessment of the Risk Management process, in the ISO 31010 document. [16]

Acknowledgements
This work was supported by national funds through Fundao para a Cincia e a Tecnologia (FCT) with reference UID/CEC/50021/2013, and by the project 4C, co-funded by the European Commission under the 7th Framework Programme for research, technological development and demonstration activities, (FP7/2007-2013) under grant agreement no. 600471.

4http://eiarquivos2014.weebly.com/
5http://www.iceis.org/
References


