2022

Designated Community: Uncertainty and Risk

Rebecca D. Frank
University of Tennessee, Knoxville, rfrank7@utk.edu

Laura Rothfritz
Humboldt-University Berlin, laura.rothfritz@hu-berlin.de

Designated Community: Uncertainty and Risk

Rebecca D. Frank & Laura Rothfritz

Note: This paper was published in the Journal of Documentation. Please cite the published version.

DOI: https://doi.org/10.1108/JD-07-2022-0161

Designated Community: Uncertainty and Risk

Rebecca D. Frank

School of Information Sciences, The University of Tennessee, Knoxville, Knoxville, Tennessee, USA and Einstein Center Digital Future, Berlin, Germany

Laura Rothfritz

Berlin School of Library and Information Science, Humboldt-Universität zu Berlin, Berlin, Germany

Abstract

Purpose: This article explores the tension between the concept of a Designated Community as a foundational element in Trustworthy Digital Repository certification and curators' uncertainty about how to interpret and apply this concept in practice.

Design/methodology/approach: This research employs a qualitative research design involving in-depth semi-structured interviews with stakeholders in the Trustworthy Digital Repository Audit and Certification process.

Findings: Our findings indicate that stakeholders in the audit and certification process viewed their uncertainty about how to apply the concept of a Designated Community in the context of an audit as a source of risk for digital repositories and their collections.

Originality: This article brings new insights to digital preservation by applying social theories of risk to trustworthy digital repository audit and certification processes, with an emphasis on the concept of Designated Community.

Keywords: Designated Community, Digital Preservation, Trustworthy Digital Repository, ISO 16363, OAIS, risk, uncertainty

Paper Type: Article (Research Paper)

1 Introduction

Digital repositories are places where the important work of preserving digital content takes place. There are many decisions that people who do this work have to make, but one of the most important is deciding who should be able to access, understand, and use the information that they are preserving. This decision drives many other choices and as such can have an outsized influence on preservation processes and can determine the success of digital preservation efforts.

A basic definition of Designated Community (DC) is: the group or groups of consumers for whom a digital repository is preserving information. A key reason for defining a DC is to set parameters for repository staff as they make preservation decisions. This concept was introduced in the Open Archival Information System (OAIS) model (Consultative Committee for Space Data Systems, 2012), and is foundational to several systems for trustworthy digital repository (TDR) audit and certification, including Trustworthy Digital Repository Audit and Certification (TRAC), ISO 16363, CoreTrustSeal, and nestor (Consultative Committee for Space Data Systems, 2011, 2012; CoreTrustSeal Standards and Certification Board, 2019; nestor Working Group Trusted Repositories - Certification, 2009; RLG-NARA Digital Repository Certification Task Force, 2007). In each of these systems, a repository is expected to clearly define the group of future consumers who should be able to access and understand the repository's preserved digital content. Other repository policies and practices are evaluated in terms of how well they meet the needs of the DC.

Despite the centrality of this concept for repository certification, the DC is poorly understood. We argue that uncertainty about the DC in the context of a repository audit influences the ways in which stakeholders construct their understanding of risk, focusing on TRAC certification.

In this article we explore the tension between the centrality of DCs in the TRAC certification process on one hand, and the uncertainty about how to apply this concept in practice on the other. We ask:

1. How do stakeholders in TDR certification understand the concept of the DC?
2. How do those stakeholders construct their understanding of risk with regard to DCs?

Our findings indicate that: (1) standard developers and auditors viewed the DC as a foundational element of the TRAC certification process, (2) standard developers, auditors, and repository staff members who discussed DCs expressed uncertainty about the concept, including how to interpret this requirement for repositories in the context of certification, and (3) uncertainty about the DC concept was described as a source of risk for digital repositories.

2 Background/Literature Review

2.1 Designated Communities

The concept of a DC was introduced in the OAIS model (i.e., ISO 14721), which outlines requirements for digital repositories that engage in long-term preservation (Consultative Committee for Space Data Systems, 2012). The OAIS model forms the basis for several TDR certification processes, which all take different approaches to evaluating how well a given repository conforms to the OAIS model. In this article we focus on the role that the DC plays in TRAC certification, a process discussed in greater detail below.

The OAIS model defines DC as:

> "An identified group of potential Consumers who should be able to understand a particular set of information. The Designated Community may be composed of multiple user communities. A Designated Community is defined by the Archive and this definition may change over time." (Consultative Committee for Space Data Systems, 2012, pp. 1–11)

There are two key elements to this definition that we would like to emphasize: first, the DC refers to *potential* consumers, which means that members of the DC do not necessarily act as immediate consumers of the information but rather are people or systems who should be able to access and use this information at some point in the future, because "the primary goal of an OAIS is to preserve information for a Designated Community over an indefinite period of time" (Consultative Committee for Space Data Systems, 2012, pp. 4–20). Second, the DC should not be seen as one static group of future consumers but may consist of multiple communities or systems that "share an identifiable set of characteristics which can be used as a reference when executing curation or preservation actions" (Moles, 2019, p. 24). This means that the DC can include current users – people or systems – but there is an emphasis on potential rather than current use for decision making.

The DC forms the basis for preservation decisions. Choices about, for example, which representation information to capture, which modes of access to support, and which file formats to use, depend on what will best meet the needs and expectations of the DC. As such, having a well-defined DC, that repository stakeholders understand, is important for a repository whose staff want to demonstrate compliance with the OAIS model through TDR certification.

The set of characteristics that a DC shares is referred to as the Knowledge Base (KB). A KB is “a set of information, incorporated by a person or system, that allows that person or system to understand received information” (Consultative Committee for Space Data Systems, 2012, pp. 1–12). The OAIS model recommends that repository staff regularly review the DC, in part because they may wish to redefine their repository’s DC, and in part because the KB of a DC can change over time (e.g., Donaldson *et al.*, 2020).

Changes to the DC and/or the KB can necessitate changes or additions to the representation information (e.g., metadata) in order to ensure that the DC will be able to understand the repository’s information in the future (e.g., Parsons and Duerr, 2006). The *Monitor Designated Community* function of the OAIS model emphasizes that repository staff should focus on changes in technology uses and requirements, and that they can gather this information through the use of surveys, workshops or other forms of interaction with the user base (Consultative Committee for Space Data Systems, 2012, pp. 4–14). While this does provide some information about how digital repository staff could track changes in the KB of their DC over time, it has been criticized as vague (e.g., Donaldson *et al.*, 2020).

Information about how to implement the DC in practice is sparse. The lack of information about how to apply this concept has been noted by several studies (e.g., Bettivia, 2016; Donaldson *et al.*, 2020; Kärberg, 2014; Locher, 2017; Moles, 2022; Parsons and Duerr, 2006). Scholarship that emphasizes the importance of the DC for long-term preservation largely aligns with the definitions in the OAIS model, but does not address arguments about the impracticality of implementing the DC (e.g., Bountouri *et al.*, 2018; Clarke and Shiue, 2020; Giaretta, 2011). Some have described implementations of the DC that are overly broad or that conflate the DC with a repository’s current users (e.g., Baker *et al.*, 2015).

In the absence of clear guidance about how to identify and define the DC, several scholars have attempted to create frameworks to help repository staff identify and define the DC for their own organizations (e.g., Donaldson *et al.*, 2020; Kärberg, 2014; Kim, 2015; Parsons and Duerr, 2006). Locher (2017) and Kärberg (2014) both argue that repositories should systematically study current repository users in order to establish a definition of their DC. Donaldson et al., (2020) argue that a key responsibility of a repository or archive is to preserve information for its DC, and provide an example of a repository whose DC changed over time.

Several scholars have identified the exclusionary nature of DC as problematic for memory institutions that serve broad publics (e.g., Bettivia, 2016; Bishop and Hank, 2016; Moles, 2019). From this perspective, repositories that explicitly seek to meet the needs of only some users or consumers necessarily privilege groups that they already understand while excluding groups with whom they are less familiar. This is closely linked to the notion that digital preservation is the act of making digital information usable for *someone*. As Bettivia argues, the OAIS model is one in which “Designated Communities are bound together with the assumption of preservation for someone rather than preservation of something” (Bettivia, 2016, p. 3). This emphasis on making sure that members of a specific community can use and understand digital information in the future has the potential to reinforce the perspectives of repository staff who must decide for whom they are preserving this information, rather than making the information in repositories accessible to groups who have traditionally not been served by memory institutions.

The overall picture is that DC is a term with a broad definition, that is foundational for repositories wishing to implement and demonstrate compliance with the OAIS model. Scholarship about DC consistently identifies the problem of being encouraged to define the DC broadly, while also being asked to maintain highly detailed information about the DC, their KB, and information needs (e.g., Parsons and Duerr, 2006). It is impractical for repository staff. It encourages repositories to define their DC narrowly, in line with what they can reasonably define and describe. This, in turn, leads to DCs that are exclusionary and in conflict with the mission of cultural heritage institutions that serve broad publics (Bettivia, 2016; Moles, 2022; Parsons and Duerr, 2006). All of this creates uncertainty for repositories seeking to follow the OAIS model.

2.2 Risk in Trustworthy Digital Repository Audit and Certification

There are several avenues for digital repositories to pursue certification as trustworthy. Processes such as CoreTrustSeal, nestor, and TRAC rely on similar criteria, which are intended to assess trustworthiness for long-term preservation by evaluating whether a repository's policies and practices align with the OAIS model through the use of a requirements checklist (Consultative Committee for Space Data Systems, 2011, 2012; CoreTrustSeal Standards and Certification Board, 2019; nestor Certification Working Group, 2013). This paper focuses on the TRAC certification system, as administered by the Center for Research Libraries (CRL).

TRAC was a joint effort by CRL, the Research Libraries Group (RLG), the National Archives and Records administration (NARA), and Consultative Committee for Space Data Standards (CCSDS) (Yakel, 2007). The Trustworthy Repositories Audit and Certification (TRAC): Criteria Checklist was created in 2007 (RLG-NARA Digital Repository Certification Task Force, 2007), and the ISO 16363 standard was approved in 2012 and confirmed in 2017 (Consultative Committee for Space Data Systems, 2011). CRL conducted audits to assess the trustworthiness of digital repositories using the TRAC checklist from 2010-2014, and continued to maintain those certifications over time until at least 2018 (e.g., Center for Research Libraries, 2018).

Through TRAC certification, repositories demonstrate their trustworthiness regarding the long-term preservation of digital information. In order to do so, they show documentary evidence of risk assessment and mitigation efforts, which is reviewed by external auditors (Frank, 2022). The ISO 16363 standard states:

> "A trustworthy digital repository will understand threats to and risks within its systems. Constant monitoring, planning, and maintenance, as well as conscious actions and strategy implementation will be required of repositories to carry out their mission of digital preservation." (Consultative Committee for Space Data Systems, 2011, pp. 2–11)

Despite the centrality of risk for repository certification, research has focused on concepts such as trustworthiness rather than risk (e.g., Bak, 2016; Dryden, 2011; Faundeen, 2017).

Some research about TDR certification processes such as TRAC has been optimistic, arguing that certification ensures that the institutions tasked with caring for valuable data and information are suited to the task (e.g., Giaretta *et al.*, 2011; Husen *et al.*, 2017; Reilly, Jr. and Waltz, 2013). Organizations publish reports of their efforts to achieve certification or to otherwise demonstrate compliance with the TRAC/ISO 16363 standard outside of formal certification (e.g., Phillips *et al.*, 2015). And repositories that have successfully achieved TRAC certification published accounts of their experience (e.g., CLOCKSS, 2014; Kirchhoff *et al.*, 2010).

Despite these positive views, scholars in recent years have begun to question the value proposition of repository certification (Bak, 2016) and whether certification processes sufficiently consider all relevant criteria (Abrams, 2021). In 2020 Donaldson observed:

> "In reality, we do not know if audit and certification of TDRs actually matters. For example, we do not know if digital repositories are actually better at preserving

> digital information after certification than they were before. Additionally, we do not know if TDRs preserve digital information better than their counterparts, although TDR standards definitely promulgate this assumption." (Donaldson, 2020, p. 12)

In summary, risk is central to TDR certification but has not received as much critical attention as other concepts such as trust, and the overall value proposition of TDR certification remains an open question.

2.3 Risk and Uncertainty

Risk is foundational to TRAC certification (Frank, 2022; McHugh, 2012). In many cases, and particularly in digital preservation, discourse about risk relies on a deterministic view which assumes risks are knowable and calculable. A classical understanding of risk holds that it is a combination of the probability and consequences of an event (e.g., International Organization for Standardization Technical Committee, 2018; Leveson *et al.*, 2009; Royal Society (Great Britain) and Study Group on Risk, 1983).

Scholarship in digital preservation has tended to focus on this view of risk as calculable and knowable (e.g., Barateiro *et al.*, 2010; Saffady, 2020; Vermaaten *et al.*, 2012). Yet, research across a broad spectrum of disciplines has argued that risk is socially constructed (e.g., Burgess, 2015; Hilgartner, 1992), that social factors influence how people construct their understanding of risk (e.g., Bankoff and Hilhorst, 2009; Nelkin, 1989; Perrow, 1999; Slovic, 1987; Vaughan, 1996), and that the social construction of risk is relevant for digital preservation (Frank, 2020).

Uncertainty has been shown to influence perceptions of risk (Tversky and Kahneman, 1982). Scholars have argued that risk calculations which take place under conditions of speculation and/or ignorance represent uncertainty about the probability or consequences of a threat (van Est *et al.*, 2012; Starr, 2003). Silver defines uncertainty as "risk that is hard to measure" (Silver, 2012, p. 29). More recently, scholars have argued that it is more productive to discuss risks themselves as uncertain because the dichotomy between probability and consequences is flawed: "current risk assessment is mostly future-oriented. The basis for risk assessment, therefore, has shifted from probability, based on experience in the past, to possibility, based on expectations about the future" (van Est *et al.*, 2012, p. 1077). In this view, probability and magnitude cannot be separated when considering uncertainty for risk. Rather, these elements combine to make risks themselves uncertain.

In the context of assessments of technical systems, "uncertainties compound the difficulties of risk evaluation and leave considerable leeway for subjective factors to enter both scientific interpretations and public perceptions" (Nelkin, 1989, p. 97). Nelkin also argues that fundamental uncertainties in technology "defy systematic analysis" and that the "effort to quantify risks and benefits masks real technical uncertainties" (Nelkin, 1989, p. 100). For TRAC certification, this means that (1) uncertainties about how to assess and mitigate risks create space for the requirements to be interpreted differently by different actors, and (2) efforts to quantify risks will obscure existing uncertainties.

This is particularly relevant with regard to the requirement that repositories understand their DC. Given how central the understanding of a repository's DC is for the TRAC requirements, and the necessity of understanding the DC for the risk assessment activities that the checklist represents, it follows that uncertainty about the DC will influence how stakeholders in this process will construct their understanding of risk.

3 Research Methods

This qualitative study is part of a larger research project whose goal is to understand how stakeholders in the TRAC repository certification process construct their understanding of risk for long-term digital preservation. This project involves 44 interviews with standard developers, auditors, and repository staff members. In this paper we report on results 19 of those interviews, focusing on those individuals who discussed the concept of the DC in their interview. This study was reviewed and deemed "not regulated" by the Institutional Review Board at the first author's university.

3.1 Sites and Participants

At the time of data collection for the study in 2016, there were six TRAC certified repositories. Of those, four were certified for their entire repository: Canadiana.org, Chronopolis, HathiTrust, and Portico (Center for Research Libraries, 2010, 2011, 2012, 2015). Two were certified for only their e-journal content: Scholars Portal and CLOCKSS (Center for Research Libraries, 2013, 2014, 2018). These repositories and their certification processes formed the sites for this study.

The participants for this research came from three groups consisting of (1) developers of the ISO 16363 standard, (2) auditors, and (3) three to five staff members from each TRAC certified repository. Standard developers as a group consists of people who participated in the development and maintenance of the ISO 16363 standard. These individuals held a range of professional roles and affiliations. The group of auditors consists of people who were staff members at CRL as well as people from CRL member organizations who were invited to participate in the audit process. The group of repository staff members consists of people who worked at the six repositories listed above and were involved in their repository's TRAC audit process in some way.

Table I below shows a breakdown of the interviewees included in this study.

Table I. Interviewees by category and role (N = 19).

	Roles			Total
	Repository Administration	Digital Preservation	IT	
Standard Developers	0	7	3	10
Auditors	1	4	0	5
Repository Staff	1	2	1	4
Total	2	13	4	19

3.2 Data Collection

Interviews lasting one to two hours were conducted with all participants. Each interview consisted of two sections. First, participants were presented with a brief vignette which was sent ahead of the interview (Frank, 2018). The vignette consisted of a sample repository description, which was generated based on the text of the ISO 16363 standard as well as the six TRAC-certified repositories. Interviewees were asked to discuss the repository described in the vignette, and to identify potential sources of risk based on the information presented. The vignette allowed for common ground across the interviewees, and is a useful interview strategy when working with research participants who are highly visible or identifiable within their communities – as these interviewees were likely to be (Gubrium and Holstein, 2001).

The second half of the interviews consisted of questions about each participant's own experience with TDR certification. Participants were asked questions about the audit and certification process and were also asked to identify and discuss potential sources of risk for TDRs.

All interviews were audio recorded and transcribed for analysis.

3.3 Data Analysis

Interview transcripts were coded in NVivo, a qualitative data analysis package. We employed an open coding approach consisting of descriptive, thematic, and analytic codes. In first round analysis interview transcripts were coded in two groups: standard developers and auditors, and repository staff members. For each, two coders worked together to achieve an acceptable interrater reliability score. We reached a Scott's pi of 0.719 for the standard developers and auditors and 0.711 for the repository staff members (Craig, 1981; Scott, 1955). The code set for this analysis consisted of codes relating to potential sources of risk, factors that influence risk perception, digital preservation, and the TRAC audit process.

After this initial round of analysis, we examined the data further, focusing on the topics of DC, risk, and uncertainty. A single team member conducted the secondary analysis.

3.4 Limitations

Participants in this research experienced some problems with memory and recall (Sudman *et al.*, 1996). In order to address these issues, we sent interviewees copies of their audit reports, and suggested that they review their own documentation and calendars before, during, and after each interview. Social desirability and expectancy effects likely occurred, given the small size of the total population for this research (Bernard, 2013). Deference effects and inaccuracy in self reporting were most likely also present (Bernard, 2013). The vignette portion of the interviews was included in part to offset some of these limitations.

4 Findings

We organize our findings into three themes based on our analysis: (1) the foundational role of the DC in TRAC certification, (2) uncertainty about the concept of the DC, and (3) the DC as a potential source of risk.

Findings from this research demonstrate that while the concept of the DC is considered foundational for TRAC certification among interviewees who discussed it, it is also a source of uncertainty for auditors and repository staff in the context of an audit. Uncertainty about how repositories should identify their DCs influences how stakeholders in this process construct their understanding of risk in the context of TRAC certification.

4.1 Designated Community: A Keystone for Trustworthy Digital Repositories

DCs were widely described by interviewees as foundational for TDRs, which aligns with the expectations set by the OAIS model and the TRAC/ISO 16363 standard as described above.

While interview questions did not specifically ask about DCs, 10 of the 11 standard developers, 5 of the 10 auditors, and 4 of the 22 repository staff members discussed this concept in their interviews, which were focused on discussing risk for digital repositories. In other words, nearly all of the standard developers and half of the auditors brought up the concept of the DC when they were asked to identify and discuss potential sources of risk for digital repositories in the context of TRAC certification, but only a small number of the repository staff members mentioned it.

Standard developers and auditors discussed the DC in ways that emphasized its' centrality, which reflected the view of the DC that the standard developers advance in the TRAC documentation. Among standard developers, a common theme that arose during interviews was the idea that the DC must be well-understood by repository management, and that having a well-defined DC would help a repository to mitigate potential risks:

> "The Designated Community has to be visible to the management of the repository and has to be available, essentially, for assurance that the repository's strategies are in keeping with the Designated Community's desires … if you've got a Designated Community and they're keeping you honest, then many of the other problems are fairly easy to deal with." (Standard Developer 01)

Similarly, standard developers explained that it was important for an audit team to include someone who is familiar with and understands the repository's DC: "It would be nice to have, as part of that team, one or more of the team members be familiar with the Designated Community for those archives and have an understanding of those areas" (Standard Developer 08).

Another perspective from standard developers that emphasized the importance of the DC came from Standard Developer 03, whose primary role was focused on digital preservation. This interviewee explained that in order to improve their documentation to become TRAC certified, the repository described in the vignette would need to clearly identify and describe not just the membership of the DC but also their KB, and then take the extra step of confirming that information with members of the DC:

> "Well the first one they'd need to have a clear statement of what their mission is and what they are and aren't going to take in. And who their Designated Community is, what the Knowledge Base of that Designated Community is, and ensure - get some feedback from the members of the group that they think make up their Designated Community to see if they're right." (Standard Developer 03)

These perspectives demonstrate that for standard developers in the TRAC certification system, it is crucial for repositories to know and understand their DC, and to be in contact with representatives from that DC in order to understand whether their policies and practices meet the needs of that DC.

Auditors shared a similar perspective. During their interviews both Auditors 04 and 09 explained that they came to understand the importance of the DC for TRAC certification through their experience as auditors, interpreting and applying the TRAC standard as written by the standard developers. For example, "the more I worked on the CRL audits the more important that notion of a Designated Community became in my mind" (Auditor 04).

This shows that the importance of the DC was something auditors learned in the review process. Repository staff members also found that auditors were very focused on the DC, "I think that the auditors are very attuned to the Designated Community" (Repository Staff 06).

In addition to explicitly describing a well-defined DC as important, interviewees framed their belief about the importance of the DC in terms of problems that could arise when this information is missing. Standard Developers 03, 05, 06, 07, 09, 11; Auditors 02, 04, 05, 10; and Repository Staff 07, 17, and 18 all expressed a belief that a lack of understanding about a repository's DC would be an impediment for certification for the repository described in the vignette. Standard Developer 05 explained that a clear explanation of the DC is a prerequisite for understanding a repository's digital object management:

> "I think that the first thing, with reference to the Digital Object Management, should be what is your Designated Community? You must know exactly why you preserve what, for whom? This must be well defined." (Standard Developer 05)

Auditor 03 stated that they would need to have a clear picture of the DC in order to understand the repository. In other words, the ability to understand a repository well enough to assess it for trustworthiness would depend ultimately on how well the DC was defined:

> "I think in order to really understand what the repository is, what they are, who they serve, I really would need to understand a little bit more about who they're preserving for." (Auditor 03)

For both Standard Developer 05 and Auditor 03, it was not possible to understand whether the repository in the vignette had appropriate processes for managing digital information, that would address potential risks, without knowing who the repository was preserving that information for. Although interviewees focused more on the DC as consisting of people than systems or non-human actors this largely aligns with the definition of the DC discussed previously, as the consumers who should be able to understand the information being preserved by the repository. In light of this alignment, it makes sense that it would be necessary to understand that DC in order to know whether the policies and practices will be appropriate for them.

4.2 Uncertainty

Despite the importance of the DC for TDRs, interviewees expressed a substantial amount of uncertainty about this concept. While the importance of the DC was primarily discussed by standard developers and auditors, interviewees across all three groups (i.e., standard developers, auditors, and repository staff members) agreed that the DC is a source of uncertainty in the TRAC audit process.

Standard developers noted that repositories in their test audits tended to have trouble defining a DC. Standard Developer 01 explained that uncertainty about the DC was a common theme across all the repositories they reviewed, and that uncertainty about how repositories should go about defining their DC is a weakness of the OAIS model:

> "Probably the most frequent was that they didn't have a good description of their Designated Community, and none of them would admit to ever having a meeting of representatives of the Designated Community … The idea that the Designated Community is the basis for all the actions that all the preservation has done, that idea didn't really have currency then, and I'm not sure that it does yet. If there's a real weakness in the OAIS model, it's that we don't have a good handle on how to, how we can advise repositories to produce or create a usable Designated Community or form an organization to represent a Designated Community. We don't discuss that at all, we just assume that they should know that already." (Standard Developer 01)

Indeed, uncertainty about the DC was a common theme across interviews. We organize these uncertainties into two categories: uncertainty about how to define and understand DCs, and uncertainty about how to monitor the KB of the DC over time.

4.2.1 Defining and Understanding Designated Communities

Several standard developers discussed the difficulty that repositories had in establishing a clear picture of their DC that they could communicate to auditors. When discussing the test audits that they conducted while developing the TRAC standard, standard developers found that the repositories were lacking clear explanations of their DCs. Standard developers 06 and 09 both said that repositories they reviewed had failed to differentiate the DC from their current users:

> "You could tell it was not really fully addressing the preservation concerns that it should be addressing. Again, it was focused on current use and meeting current user demands. Well, your Designated Community has to include users who haven't even been born yet. You have to have a way in which you can ensure, guarantee, that you can preserve that information a half century, a full century, four centuries into the future." (Standard Developer 06)

In failing to frame this as the DC and instead talking about their current users, the staff of the repositories in these test audits demonstrated that they did not understand how important the concept of the DC was for certification.

Repository staff members discussed challenges that they encountered in clearly defining their repository's DC. Repository Staff 07 explained that the audit process pushed the repository to more fully document policies that they had taken for granted, "we sort of assumed we had them we just didn't have them written down." The DC was one of those policies: "we hadn't even realized that those were areas where we hadn't put any thought into it" (Repository Staff 07). Once it became clear that the repository needed a clear definition of their DC, they realized that they also needed a much more specific definition:

> "We spent a lot of time defining our Designated Community because we've always done it very broadly and when you start actually looking at certifying a repository you start to realize well you actually you have to be a lot more specific, and I think, constrained about what that is." (Repository Staff 07)

In addition to defining the DC, another area of uncertainty for interviewees was how repositories should go about understanding and meeting the needs of their DCs. Repository staff members explained that their organizations experienced difficulties articulating the link between repository policies and practices and the DC. For Repository Staff 18, bringing repository governance into alignment with the expectations of a diverse DC was difficult: "It's complicated, the governance and managing expectation of a diverse Designated Community is complicated in a certain way."

Auditors recognized that the lack of clear definition of the DC led to uncertainty about other policies and practices. Uncertainty about the DC led to problems in other repository policies, such as the scope of the collection and policies governing decisions about what to accept and ingest to the repository:

> "I would say the biggest issue was the [repository] audit was the role of that organization and its Designated Community … We needed some clarity around what that Designated Community looked like. And it was a little bit unclear, too, what their mandate was in terms of the breadth of the types of material that they would seek to ingest." (Auditor 08)

For standard developers, auditors, and repository staff members, the concept of the DC was met with uncertainty. In the context of a TRAC audit, members from all three groups described instances in which staff members of digital repositories were uncertain about how to apply the concept of the DC to their repository and/or about how to define their own DC. Auditors and repository staff members also described instances in which a lack of understanding about the DC led to uncertainty in other areas of repository management such as governance and collection management decisions.

4.2.2 The Knowledge Base of the Designated Community

In addition to defining the DC and developing an understanding of their needs, repositories that seek TRAC certification must also monitor the KB of their DCs in order to ensure that they are preserving information in a way that will be understandable over time.

Monitoring the KB of the DC was described as both a source and result of uncertainty. For repository staff members, uncertainty about how to define their DC could lead to problems in understanding the KB of that DC. Alternately, changes in the KB of the DC over time were also described as something that could create uncertainty for digital repositories.

Discussions about monitoring the KB of the DC over time demonstrated uncertainty among interviewees about the concept of the DC. For example, Standard Developer 09 explained that although understanding the DC and making preservation decisions that align with the KB of that DC is crucial for TRAC certification, it is difficult to do in practice and in his opinion it would be fine for repositories to instead set policies based on the needs of their current users:

> "[A] Designated Community is a fundamental idea, but it's very difficult to do in practice. Repositories often think in terms of their current user base, which is fine as long as they also have in mind that the future users, the Designated Community, may have a different Knowledge Base." (Standard Developer 09)

This highlights the importance of understanding a DC as separate and distinct from a repository's current users in order to make preservation decisions that take the KB of the DC into account. This perspective was particularly salient for standard developers, who emphasized the difference between the DC and a repository's current users in the OAIS model and TRAC checklist.

4.3 Risk

Lack of clarity about a concept that was understood as foundational for the TRAC audit process was described as a source of risk for digital repositories. Interviewees discussed this uncertainty as a risk to the repositories and the digital information that they sought to preserve.

A lack of understanding about the DC for a repository was viewed as a problem because it was an indication of potentially inconsistent policies and practices. For example, Standard Developer 03 and Repository Staff 18 explained that a lack of clarity about the DC could ultimately result in a repository that was not meeting the needs of users and could therefore threaten funding, "the foundational risk is that they haven't identified what exactly they're going to keep and how long they're going to keep it and who they're going to keep it for. And so over the long term that can have an impact on your funding and the viability of the repository … there's an existential risk to the repository" (Standard Developer 03).

Interviewees also discussed the concept of the DC as malleable. For several interviewees, successful TRAC certification was a result of carefully defining a repository's DC in a way that would justify current policies and practices, even when they ran counter to the recommendations in the TRAC standard. Standard Developer 01 and Repository Staff 18 both described situations in which repositories justified preservation policies regarding data backups that failed to conform to best practices as set by the TRAC standard by arguing that they met the expectations of their DCs. The repositories that they were describing both achieved TRAC certification.

4.3.1 Designated Community Composition, Expectations, and Knowledge Base

As discussed above, the DC is foundational for TRAC certification. Interviewees described the DC as the basis for repository policies and practices, and said that repositories wishing to become TRAC certified would be evaluated in terms of how well their policies and practices met the needs and expectations of their DCs. A well-defined DC was described as "the starting point of any OAIS-based repository" (Standard Developer 01).

In light of the substantial role that the DC plays in repository certification, uncertainty about the membership of a repository's DC and/or about the needs and expectations of the DC was viewed as a source of risk for the long-term preservation of digital content. Standard developers 01, 03, 05, and 09, and Auditor 02 all identified the lack of a clearly defined as a potential source of risk for the repository in the vignette: "There's no information about who the community is and what they would expect, and I think that's a flag" (Auditor 02).

Standard Developer 05 explained that many elements of digital preservation are put at risk when the DC is not clearly articulated:

> "If you don't know exactly the reason and the focus, you are not able to define the level of granularity of your description. Of your data management. You are not able to define what has to be received when you have this and what has to be added and which kind of documentation, and information, you have to put on when you give access in the future, also immediately, to the users. Which kind of users? How to create this chain if you don't have clear ideas what you're doing for whom?" (Standard Developer 05)

When discussing the vignette, Standard Developer 09 found inconsistencies in the preferred format policy and thought this was evidence that the DC was not well-understood. According to this interviewee, uncertainty about file formats was a potential source of risk for the repository because it demonstrated a lack of understanding about the expectations of the DC:

> "The risk here is that the expectations of users do not match what the repository is providing in terms of support for preferred versus non-preferred formats … So for me, that's a risk. It suggests that the Designated Community is not really understood." (Standard Developer 09)

The above statement demonstrates the expectation of standard developers that the DC forms the basis of policy decisions within repositories. Repository policies and practices that were not internally consistent, or that seemed to conflict with one another were indicators of risk for this interviewee.

Communication about repository policies was described as an important way to manage expectations with a repository's membership, in part by explaining the DC, to contextualize policies and practices. Auditor 08 explained that repositories could offset some problems by minimizing uncertainty through good communication practices:

> "It's really important to communicate, in this case, this is the Designated Community.

The organization has to really have a good foundation in communicating with that Designated Community and making sure that there's consensus that those changes and those clarifications are good and supported and solid." (Auditor 08)

Lack of clarity about the DC was described as a threat not just to the digital content in a repository, but to the repository itself. Auditor 08 and Repository Staff 18 explained that a repository that lacked a clear picture of their DC was at risk of losing the support of their user community:

> "[T]he foundational risk is that they haven't identified what exactly they're going to keep and how long they're going to keep it and who they're going to keep it for. And so over the long term that can have an impact on your funding and the viability of the repository. Because if you're not meeting the needs of your customers, your funding - the membership dues - will decrease, grant funding will go away. So there's an existential risk to the repository." (Standard Developer 03)

Repository Staff 18 explained further, that in addition to needing to know if they were meeting the needs of the DC, it was also important to know how the repository was viewed, and what expectations the DC would have about a repository's infrastructure and services. Understanding how a repository can remain relevant to the DC was crucial:

> "From my perspective the most significant risk is just the lack of clarity around the mandate. Because basically the whole rest of everything kind of falls out of that. Needing to know what, how the members of the Designated Community view the repository. Is it a core piece of their operating infrastructure? Is it something they're just throwing money at in order to say, 'yeah, we're dealing with preservation, it's this thing over here?' We'd need to know that because it's that, that all the other pieces that are risky are going to hang off of." (Repository Staff 18)

In addition to the composition and expectations of a DC, interviewees discussed uncertainty about changes to the KB over time as a potential source of risk. When asked about sources of uncertainty for digital repositories, Standard Developer 09 discussed monitoring the KB in order to be aware of changes over time: "Future technology, I guess. And I guess, changes in the community that you're trying to support" (Standard Developer 09).

For TRAC certification, interviewees identified risk in the ways that repositories did, or did not, understand, define, and monitor the needs of their DCs. Interviewees across tall three groups (i.e., standard developers, auditors, and repository staff members) argued that a lack of clarity about DC would be a risk to the long-term preservation of digital content, and to the financial sustainability of a repository.

4.3.2 Using the Designated Community to Justify Sub-Optimal Policies and Practices

The lack of clarity about how to identify and describe a DC was also a source of risk for repositories because it created opportunities for stakeholders in the TRAC process to justify sub-optimal preservation policies and practices.

Several interviewees expressed a strong belief that a repository could justify any kind of policies or practices, even if those policies were in direct contrast to the OAIS model and TRAC requirements, if they could claim that it met the expectations of their DC. For example, Repository Staff 18 described a situation in which a repository received certification despite failing to meet data backup requirements because they argued that their DC was ok with what they were doing:

> "On some level, there were some conversations that we had where they were really pushing for a technical, the example I would give is: our off-site back-ups. We have backups and we have off-site backups. Our off-site back-ups were not what they deemed to be sufficiently far away … And through quite a lot of research and hand wringing and the like, we sort of came around to the idea that there aren't really well-established standards for this. It's sort of based on risk management and risk mitigation and so I think they were lobbying fairly hard for a solution that was a given distance away. And I think there was some question as to whether or not they're the ones to dictate that to us ... I actually don't think that's the role of the auditor. I think that's the role of the Designated Community. If they have concerns that it's not enough then I think it's their role to ask the Designated Community if they think it's enough." (Repository Staff 18).

Standard Developer 01 said that the backup strategy of the repository in the vignette was not sufficient, but also if it met the expectations of the DC then it would be fine. This attitude is a paradox in repository certification. The goal of certification is to assess repositories and provide an assessment by experts in order to help data depositors, repository users, and funders to know whether the repositories are trustworthy because regular users don't have specialist knowledge about how repositories should preserve content. But the certification process has a clause that allows auditors and repository staff to do anything as long as they claim that it is expected by the DC – a group of people who may not understand enough about preservation to know if the services provided are sufficient and trustworthy, "I guess, again, it's a matter of what the Designated Community wants us to do, but active mirror backup sites are not in and of themselves ... They're not sufficient" (Standard Developer 01).

Auditor 04 was even more explicit, and said that he learned through the audit process that repositories which fell short of meeting the best practices described in the TRAC standard could still become TRAC certified if they argued that the repository was meeting the expectations of the DC: "As long as your policies adhere to what your Designated Community expects, then it's basically cool" (Auditor 04).

Repository Staff 06 and 07 both identified the bit-level preservation described in the vignette as a potential source of risk, but argued that this would still be acceptable as long as the repository did not promise more: "Yeah, if all you promise is bit-level of preservation, for anything you want to put in there and it's encrypted and whatever, then good enough" (Repository Staff 06).

Repository Staff 07 went on to explain that this approach – to manage expectations in order to justify particular approaches to digital preservation – was still potentially problematic, because it would be difficult to fully explain the implications of bit-level preservation to people without expertise in digital preservation:

> "I think the more low-level and basic what you're proposing to do is, the more careful you have to actually be about managing expectations and understandings of what it is that you're actually promising. There's nothing wrong with bit level preservation but making your depositors and your Designated Communities actually understand what the implications of bit level preservation could be, I think may be potentially more

> challenging." (Repository Staff 07)

So far we have discussed how interviewees use the DC to justify preservation policies and practices that may be risky with regard to long-term preservation. Interviewees also described situations in which a repository could meet the requirements for certification by changing the definition of their DC rather than changing policies to meet the needs and expectations of their stated DC: "that's easy to fix because all you have to do is to be more precise about his Designated Community" (Standard Developer 07).

Standard Developer 07 went on to explain that broadening the scope of the DC could be a way for a repository to acquire support and resources, suggesting a strategic, extractive view of the DC:

> "If you can increase the value, broaden the community of users, so not the Designated Community, but the community of users who can clearly use the data, then eventually you might broaden your Designated Community … Then you can start building business cases and justify the resources that go into preservation." (Standard Developer 07)

A repository whose policies and documentation do not align with their DC was described as a red flag in an audit, and a signal of risk for the long-term preservation of content and to the repository itself. However, in many cases interviewees described ways that repositories could subvert the TRAC requirements by arguing that their DCs either expected or were willing to accept policies and practices that fell short of the requirements, or by redefining the DC to fit what the repository was doing, rather than working to meet the needs and expectations of the DC.

5 Discussion

The DC is a foundational element of the OAIS model and the TRAC certification requirements (Consultative Committee for Space Data Systems, 2011, 2012). Despite the importance of the DC, it is a poorly understood concept that repository staff members have difficulty implementing in the context of their own repository (e.g., Bettivia, 2016; Boutard, 2020; Moles, 2022; Parsons and Duerr, 2006). This study expanded the discussion to include an examination of the role that the DC played in the certification process for all six of the TRAC certified repositories.

We already know that both scholars and practitioners find the DC to be a problematic concept for digital repositories. This article contributes to the discussion about DCs by interrogating the relationship between DCs, repository certification, and risk.

As early as 2006, scholars such as Parsons and Duerr criticized the concept of the DC as too narrow (Parsons and Duerr, 2006). Since that time, others have noted that the concept is difficult to implement (e.g., Donaldson, 2020), and that it forces institutions that serve broad publics to instead narrow their focus to a specific set of potential consumers (e.g., Bettivia, 2016). Scholars have also argued that by focusing on a narrowly-defined DC, repositories risk failing to provide meaningful access to digital information for more broadly conceptualized user communities (Boutard, 2020; Moles, 2022).

Scholars, such as Moles (2022) and Bettivia (2016), have argued that repositories seeking to strictly implement the requirement for a clearly defined DC which guides preservation strategy can lead repositories to implement exclusionary practices that conflict with their professional ethics. While this study finds that the concept of the DC was viewed by some TRAC certification stakeholders in this way – as a tool to narrow the focus of preservation strategies to meet the needs of a particular group of people – we found that others viewed the concept of a DC as a malleable and changeable way to justify a range of preservation strategies.

Our findings that interviewees justify policies and practices that conflict with the TRAC requirements by appealing to their DC begs the question of whether members of a repository's DC possess sufficient expertise in long-term digital preservation to disregard widely accepted best practices. One of the purposes of TRAC certification is to demonstrate to repository stakeholders that the organization is trustworthy for long-term preservation by having experts examine the repository, so that current and future repository users can understand whether a repository is trustworthy without having to become experts in digital preservation. Circumventing the requirements of the TRAC standard by explaining that non-experts are willing to accept sub-par preservation practices, without demonstrating that those people understand best practices, introduces risk to the long-term preservation of digital information as well as to the sustainability of the repository itself.

Choices about preservation strategies such as file formats, metadata, and contextual information should understandably be guided by the DC. However, we argue here that preservation strategies, such as data backup policies, should also be guided by expertise and best practices in digital preservation. Implementing strategies that conflict with accepted best practices in digital preservation, based on the expectations of a DC lacking in expertise about this topic, introduces uncertainty and risk to both the digital content and the repository itself. Likewise, it brings into question the value of TRAC certification if repositories with strategies that fail to meet the requirements described in the standard can still achieve certification.

6 Conclusion

Risk is a foundational but poorly defined concept for TRAC certification. The DC is also a foundational but poorly defined concept for TRAC certification. We have argued here that uncertainty about the DC in the context of a repository audit influences the ways in which stakeholders in the process construct their understanding of risk. Our findings indicate that: (1) standard developers and auditors viewed the DC as a foundational element of the TRAC certification process, (2) stakeholders from all three groups of interviewees who discussed DCs expressed uncertainty about the concept, including how to interpret this requirement for repositories in the context of certification, and (3) uncertainty about the DC concept was described as a source of risk for digital repositories.

While previous research has focused on the ways in which the concept of a DC can lead to exclusionary policies and practices by focusing on some subset of potential future users, we argue here that uncertainty about concept of a DC is a potential source of risk to the sustainability of repositories and the long-term preservation of digital content. TDR certification processes that rely on the DC, including TRAC, ISO 16363, CoreTrustSeal, and nestor, would be strengthened by a clearer description of the concept, as well as stronger norms about how auditors and/or reviewers should assess repositories with regard to this concept.

7 Acknowledgements

The authors would like to thank Dr. Elizabeth Yakel, Ph.D., Dr. Paul Conway, Ph.D., Dr. Paul Courant, Ph.D. and Dr. Shobita Parthasarathy, Ph.D. for the feedback and guidance at various stages of this project. The authors would also like to thank Megh Marathe and Carl Haynes for the assistance with data analysis. Funding: This research was funded in part by a University of Michigan Rackham Graduate Student Research Grant. This research was also partly funded by the Einstein Center Digital Future.

8 References

Abrams, S. (2021), "Tacit attitudinal principles for evaluating digital preservation success", *Archival Science*, Vol. 21 No. 3, pp. 295–315.

Bak, G. (2016), "Trusted by Whom? TDRs, Standards Culture and the Nature of Trust", *Archival Science*, Vol. 16 No. 4, pp. 373–402.

Baker, K.S., Duerr, R.E. and Parsons, M.A. (2015), "Scientific Knowledge Mobilization: Co-evolution of Data Products and Designated Communities", *International Journal of Digital Curation*, Vol. 10 No. 2, pp. 110–135.

Bankoff, G. and Hilhorst, D. (2009), "The politics of risk in the Philippines: comparing state and NGO perceptions of disaster management", *Disasters*, Vol. 33 No. 4, pp. 686–704.

Barateiro, J., Antunes, G., Freitas, F. and Borbinha, J. (2010), "Designing Digital Preservation Solutions: A Risk Management-Based Approach", *International Journal of Digital Curation*, Vol. 5 No. 1, pp. 4–17.

Bernard, H.R. (2013), *Social Research Methods: Qualitative and Quantitative Approaches*, 2nd ed., SAGE Publications, Los Angeles.

Bettivia, R.S. (2016), "The Power of Imaginary Users: Designated Communities in the OAIS Reference Model", *Proceedings of the Association for Information Science and Technology*, Vol. 53 No. 1, pp. 1–9.

Bishop, B.W. and Hank, C. (2016), "Data Curation Profiling of Biocollections", *Proceedings of the Association for Information Science and Technology*, Vol. 53, presented at the The 79th ASIS&T Annual Meeting: Creating Knowledge, Enhancing Lives Through Information & Technology, John Wiley & Sons, Ltd, Copenhagen, Denmark, pp. 1–9.

Bountouri, L., Gratz, P. and Sanmartin, F. (2018), "Digital Preservation: How to Be Trustworthy", in Ioannides, M. (Ed.), *Digital Cultural Heritage*, Vol. 10605, Springer, Cham, pp. 364–374.

Boutard, G. (2020), "Alter-Value in Data Reuse: Non-Designated Communities and Creative Processes", *Data Science Journal*, Ubiquity Press, Vol. 19 No. 1, p. 23.

Burgess, A. (2015), "Social Construction of Risk", in Cho, H., Reimer, T. and McComas, K. (Eds.), *The Sage Handbook of Risk Communication*, SAGE Publications, Thousand Oaks, CA, pp. 56–68.

Center for Research Libraries. (2010), *CRL Certification Report on Portico Audit Findings*, Center for Research Libraries, Chicago, IL, available at: https://www.crl.edu/sites/default/files/reports/CRL%20Report%20on%20Portico%20Audit%202010.pdf.

Center for Research Libraries. (2011), *CRL Certification Report on the HathiTrust Digital Repository*, Center for Research Libraries, Chicago, IL, available at: https://www.crl.edu/sites/default/files/reports/CRL%20HathiTrust%202011.pdf.

Center for Research Libraries. (2012), *CRL Certification Report on Chronopolis Audit Findings*, Center for Research Libraries, Chicago, IL, available at: https://www.crl.edu/sites/default/files/reports/Chron_Report_2012_final_0.pdf.

Center for Research Libraries. (2013), *CRL Certification Report on Scholars Portal Audit Findings*, Center for Research Libraries, Chicago, IL, available at: http://www.crl.edu/sites/default/files/attachments/pages/ScholarsPortal_Report_2013_%C6%92.pdf (accessed 1 May 2019).

Center for Research Libraries. (2014), *CRL Certification Report on CLOCKSS Audit Findings*, Center for Research Libraries, available at: http://www.crl.edu/archiving-preservation/digital-archives/certification-and-assessment-digital-repositories/clockss-report (accessed 11 August 2014).

Center for Research Libraries. (2015), *CRL Certification Report on the Canadiana.Org Digital Repository*, Center for Research Libraries, Chicago, IL, available at: https://www.crl.edu/sites/default/files/reports/CANADIANA_AUDIT%20REPORT_2015.pdf.

Center for Research Libraries. (2018), *2018 Updated Certification Report on CLOCKSS*, Center for Research Libraries, Chicago, IL, available at: https://www.crl.edu/sites/default/files/reports/CLOCKSS_Report_2018_0.pdf.

Clarke, C.T. and Shiue, H.S.Y. (2020), *Final Report and Recommendations of the Data Rescue Project at the National Agricultural Library*, National Agricultural Library, College Park, Maryland, available at: https://doi.org/10.13016/kpt7-cqgr (accessed 27 August 2020).

CLOCKSS. (2014), "CLOCKSS Archive Certified as Trusted Digital Repository; Garners top score in Technologies...", *CLOCKSS News*, Nonprofit, , 28 July, available at: https://www.clockss.org/clockss/News (accessed 30 March 2016).

Consultative Committee for Space Data Systems. (2011), *Audit and Certification of Trustworthy Digital Repositories*, Magenta Book No. CCSDS 652.0-M-1, Consultative Committee for Space Data Systems, Washington, D.C., available at: https://public.ccsds.org/Pubs/652x0m1.pdf (accessed 19 July 2022).

Consultative Committee for Space Data Systems. (2012), *Reference Model for an Open Archival Information System (OAIS)*, Magenta Book No. CCSDS 650.0-M-2, Consultative Committee for Space Data Systems, Washington, D.C., p. 135.

CoreTrustSeal Standards and Certification Board. (2019), "CoreTrustSeal Trustworthy Data Repositories Requirements 2020–2022 (v02.00-2020-2022)", Zenodo, available at: https://doi.org/10.5281/ZENODO.3638211.

Craig, R.T. (1981), "Generalization of Scott's Index of Intercoder Agreement", *Public Opinion Quarterly*, Vol. 45 No. 2, pp. 260–264.

Donaldson, D.R. (2020), "Certification Information on Trustworthy Digital Repository Websites: A Content Analysis", *PLoS ONE*, Public Library of Science, Vol. 15 No. 12, p. e0242525.

Donaldson, D.R., Zegler-Poleska, E. and Yarmey, L. (2020), “Data Managers’ Perspectives on OAIS Designated Communities and the FAIR Principles: Mediation, Tools and Conceptual Models”, *Journal of Documentation*, Vol. 76 No. 6, pp. 1261–1277.

Dryden, J. (2011), “Measuring Trust: Standards for Trusted Digital Repositories”, *Journal of Archival Organization*, Vol. 9 No. 2, pp. 127–130.

van Est, R., Walhout, B. and Brom, F. (2012), “Risk and Technology Assessment”, in Roeser, S., Hillerbrand, R., Sandin, P. and Peterson, M. (Eds.), *Handbook of Risk Theory: Epistemology, Decision Theory, Ethics, and Social Implications of Risk*, Springer, Dordrecht Netherlands, pp. 1067–1091.

Faundeen, J. (2017), “Developing Criteria to Establish Trusted Digital Repositories”, *Data Science Journal*, Vol. 16, p. 22.

Frank, R.D. (2018), *The Social Construction of Risk in Trustworthy Digital Repository Audit and Certification*, Dissertation, University of Michigan, Ann Arbor, MI, available at: https://deepblue.lib.umich.edu/handle/2027.42/147539.

Frank, R.D. (2020), “The Social Construction of Risk in Digital Preservation”, *Journal of the Association for Information Science and Technology*, Vol. 71 No. 4, pp. 474–484.

Frank, R.D. (2022), “Risk in Trustworthy Digital Repository Audit and Certification”, *Archival Science*, Vol. 22 No. 1, pp. 43–73.

Giaretta, D. (2011), *Advanced Digital Preservation*, Springer-Verlag, Berlin Heidelberg, available at:https://doi.org/10.1007/978-3-642-16809-3.

Giaretta, D., Conrad, M., Garrett, J., Longstreth, T., Lambert, S., Sierman, B., Hughes, S., *et al.* (2011), “Audit and Certification Process for Digital Repositories”, presented at the PV2011, Toulouse, France, available at: http://www.iso16363.org/assets/PV2011Giaretta.pdf.

Gubrium, J.F. and Holstein, J.A. (Eds.). (2001), *Handbook of Interview Research*, SAGE Publications, Inc., Thousand Oaks, CA, US, available at: https://dx.doi.org/10.4135/9781412973588 (accessed 17 May 2016).

Hilgartner, S. (1992), “The Social Construction of Risk Objects”, in Short, Jr., J.F. and Clarke, L. (Eds.), *Organizations, Uncertainties, and Risk*, Westview Press, Boulder, CO, pp. 39–53.

Husen, S., de Wilde, Z., de Waard, A. and Cousijn, H. (2017), *Recommended versus Certified Repositories: Mind the Gap*, SSRN Scholarly Paper No. ID 3020994, Social Science Research Network, Rochester, NY, available at: https://papers.ssrn.com/abstract=3020994 (accessed 5 July 2018).

International Organization for Standardization Technical Committee. (2018), *Risk Management - Guidelines*, Standard No. ISO 31000:2018, International Organization for Standardization, Washington, D.C., available at: https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:en (accessed 21 February 2019).

Kärberg, T. (2014), “Digital Preservation and Knowledge in the Public Archives: For Whom?”, *Archives and Records*, Routledge, Vol. 35 No. 2, pp. 126–143.

Kim, Y. (2015), “‘Designated Communities’: Through the Lens of the Web”, *International Journal of Digital Curation*, Vol. 10 No. 1, pp. 184–195.

Kirchhoff, A., Fenton, E., Orphan, S. and Morrissey, S. (2010), “Becoming a Certified Trustworthy Digital Repository: The Portico Experience”, *Proceedings of the 7th International Conference on Preservation of Digital Objects*, presented at the iPres 2010, Vienna, Austria, pp. 87–94.

Leveson, N., Dulac, N., Marais, K. and Carroll, J. (2009), “Moving Beyond Normal Accidents and High Reliability Organizations: A Systems Approach to Safety in Complex Systems”, *Organization Studies*, Vol. 30 No. 2–3, pp. 227–249.

Locher, A.E. (2017), *Characterization of Designated Communities of Geospatial Legacy Information and Their Application in Appraisal and Digital Preservation Decisions: A Case Study*, Dissertation, Universitat de Barcelona, Barcelona, Spain, 13 September, available at: http://diposit.ub.edu/dspace/handle/2445/117369 (accessed 19 April 2021).

McHugh, A. (2012), “A Model for Digital Preservation Repository Risk Relationships”, *Proceedings of World Library and Information Congress: 78th IFLA General Conference and Assembly*, presented at the World Library Information Congress: 78th IFLA General Conference and Assembly, Helsinki, Finland, available at: http://eprints.gla.ac.uk/65420 (accessed 1 July 2014).

Moles, N. (2019), *Inside Open Government Data Curation: Exploring Challenges to the Concept of a ‘Designated Community’ through a Case Study of the City of Toronto*, Thesis, University of Toronto, Toronto, Ontario, Canada, November, available at: https://tspace.library.utoronto.ca/handle/1807/97579 (accessed 23 February 2020).

Moles, N. (2022), “Preservation for Diverse Users: Digital Preservation and the ‘Designated Community’ at the Ontario Jewish Archives”, *Journal of Documentation*, Vol. 78 No. 3, pp. 613–630.

Nelkin, D. (1989), “Communicating Technological Risk: The Social Construction of Risk Perception”, *Annual Review of Public Health*, Annual Reviews, Vol. 10 No. 1, pp. 95–113.

nestor Certification Working Group. (2013), *Explanatory Notes on the Nestor Seal for Trustworthy Digital Archives*, No. nestor-materials 17, Deutsche Nationalbibliothek, Frankfurt am Main, available at: http://files.d-nb.de/nestor/materialien/nestor_mat_17_eng.pdf (accessed 20 July 2014).

nestor Working Group Trusted Repositories - Certification. (2009), *Nestor Criteria: Catalogue of Criteria for Trusted Digital Repositories, Version 2*, Deutsche Nationalbibliothek, Frankfurt am Main, available at: http://nbn-resolving.de/urn:nbn:de:0008-2010030806.

Parsons, M. and Duerr, R. (2006), “Designating user communities for scientific data: challenges and solutions”, *Data Science Journal*, Ubiquity Press, Vol. 4 No. 0, pp. 31–38.

Perrow, C. (1999), *Normal Accidents: Living with High-Risk Technologies*, Updated., Princeton University Press.

Phillips, M.E., Alemneh, D.G., Krahmer, A., Tarver, H. and Waugh, L. (2015), *UNT Libraries: TRAC Conformance Document*, University of North Texas Libraries, UNT Digital Library, Denton, Texas, p. 291.

Reilly, Jr., B.F. and Waltz, M.E. (2013), “Trustworthy Data Repositories: The Value and Benefits of Auditing and Certification”, in Ray, J.M. (Ed.), *Research Data Management : Practical Strategies for Information Professionals*, Purdue University Press, Ashland, OH, pp. 109–126.

RLG-NARA Digital Repository Certification Task Force. (2007), *Trustworthy Repositories Audit & Certification: Criteria and Checklist, Version 1.0*, available at: http://www.crl.edu/sites/default/files/attachments/pages/trac_0.pdf (accessed 19 July 2014).

Royal Society (Great Britain) and Study Group on Risk. (1983), *Risk Assessment: Report of a Royal Society Study Group.*, Royal Society, London.

Saffady, W. (2020), *Managing Information Risks: Threats, Vulnerabilities, and Responses*, Rowman & Littlefield, Lanham, MD.

Scott, W.A. (1955), “Reliability of Content Analysis: The Case of Nominal Scale Coding”, *Public Opinion Quarterly*, Vol. 19 No. 3, p. 321.

Silver, N. (2012), *The Signal and the Noise: Why So Many Predictions Fail--But Some Don’t*, Penguin Press, New York.

Slovic Paul. (1987), “Perception of Risk”, *Science*, American Association for the Advancement of Science, Vol. 236 No. 4799, pp. 280–285.

Starr, C. (2003), “The Precautionary Principle Versus Risk Analysis”, *Risk Analysis*, Vol. 23 No. 1, pp. 1–3.

Sudman, S., Bradburn, N.M. and Schwarz, N. (1996), *Thinking About Answers: The Application of Cognitive Processes to Survey Methodology*, Jossey-Bass Publishers, San Francisco.

Tversky, A. and Kahneman, D. (1982), “Judgment Under Uncertainty: Heuristics and Biases”, in Kahneman, D., Slovic, P. and Tversky, A. (Eds.), *Judgment Under Uncertainty: Heuristics and Biases*, Cambridge University Press, Cambridge ; New York, pp. 3–20.

Vaughan, D. (1996), *The Challenger Launch Decision: Risky Technology, Culture, and Deviance at NASA*, University of Chicago Press, Chicago.

Vermaaten, S., Lavoie, B. and Caplan, P. (2012), “Identifying Threats to Successful Digital Preservation: the SPOT Model for Risk Assessment”, *D-Lib Magazine*, Vol. 18 No. 9/10, available at: https://doi.org/10.1045/september2012-vermaaten.

Yakel, E. (2007), “Digital Curation”, *OCLC Systems & Services: International Digital Library Perspectives*, Vol. 23 No. 4, pp. 335–340.