Journal of Documentation

Constructing risk in trustworthy digital repositories

Rebecca D. Frank
School of Information Sciences, The University of Tennessee Knoxville, Knoxville, Tennessee, USA

Received 18 August 2023
Revised 2 June 2024
Accepted 9 June 2024

Abstract

Purpose – This article investigates the construction of risk within trustworthy digital repository audits. It contends that risk is a social construct, and social factors influence how stakeholders in digital preservation processes comprehend and react to risk.

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 (TRAC) process, and document analysis of the TRAC checklist and audit reports. I apply an analytic framework based on the Model for the Social Construction of Risk in Digital Preservation to this data.

Findings – The findings validate the argument that risk in digital preservation is indeed socially constructed and demonstrate that the eight factors in the Model for the Social Construction of Risk in Digital Preservation do indeed influence how stakeholders constructed their understanding of risk. Of the eight factors in the model, communication, expertise, uncertainty and vulnerability were found to be the most influential in the construction of risk during the TRAC audit process. The influence of complexity, organizations political culture, were more limited.

Originality/value – This article brings new insights to digital preservation by demonstrating the importance of understanding risk as a social construct. I argue that risk identification and/or assessment is only the first step in the long-term preservation of digital information and show that perceptions of risk in digital preservation are shaped by social factors by applying theories of social construction and risk perception to an analysis of the TRAC process.

Keywords Digital preservation, Trustworthy digital repository, ISO 16363, Risk, Social construction

Paper type Research paper

Introduction

Risk in digital preservation has been understood in a probabilistic way, treating it as a discrete fact that rational actors will interpret and respond to in the same way. This approach is outdated. Instead, I argue that risk should be understood as a social construct influenced by various social factors. These factors shape how stakeholders in digital preservation processes understand and respond to risk information, ultimately influencing the outcomes and actions taken in response to that information.

Recent research has highlighted challenges in digital preservation by demonstrating that organizations, systems, and tools with a preservation focus are in fact failing to properly safeguard digital content (Rieger *et al.*, 2022). This, coupled with the 2022 memorandum from the Office of Science and Technology Policy (OSTP) recommending that federal funding agencies in the US update their guidelines to require data produced through publicly funded research be deposited in digital repositories (Nelson, 2022), brings urgency to the work of ensuring that repositories entrusted with valuable digital information are up to the task of long-term preservation.

Certification systems for trustworthy digital repositories (TDRs) are one mechanism that the digital preservation community has developed to evaluate whether repositories are indeed able

I 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. I 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.

Journal of Documentation

0022-0418
DOI 10.1108/JD-08-2023-0157

to preserve their content long-term. In this article, I apply the Model for the Social Construction of Risk in Digital Preservation (Frank, 2020) to the Trustworthy Repositories Audit and Certification (TRAC) process in order to examine how stakeholders in a TRAC audit construct their understanding of risk. This article is motivated by the following research questions:

RQ1. To what degree do the following eight factors which influence risk perception come into play in the audit process: communication, complexity, expertise, organizations, political culture, trust, uncertainty, and vulnerability?

RQ2. In what ways and why do they emerge when repository staff and auditors consider risk as articulated in the TRAC standard?

My findings extend this previous research to support the argument that risk in digital preservation is socially constructed and that the eight factors in the Model for the Social Construction of Risk in Digital Preservation – communication, complexity, expertise, organizations, political culture, trust, uncertainty, and vulnerability – influence the construction of risk in the TRAC audit process. I also found that communication, expertise, uncertainty, and vulnerability emerged as the most influential factors in how auditors and repository staff members perceived risk during TRAC audits. Complexity, organizations, political culture, and trust had a distinct but more limited impact.

Literature review

Digital preservation and risk

Digital preservation consists of those actions that ensure the viability and authenticity of digital objects over time (e.g. Berman, 2008; Hitchcock *et al.*, 2007). Risk is a foundational element of digital preservation (e.g. Barons *et al.*, 2021; Conway, 1996; Schaefer *et al.*, 2021). The long-term preservation of digital information is an ongoing exercise in risk management. In order to ensure the longevity of digital content, repositories preserving digital assets need to develop a sustainable organizational structure and financial stability as well as create robust processes to ensure the viability and accessibility of file formats and the long-term storage and management of data. Digital repositories must have the ability to manage risk in all of these areas (Anderson, 2005; Garrett and Waters, 1996; Hey *et al.*, 2009).

The relationship between risk and digital preservation has been well documented. Some definitions characterize digital preservation as a type of risk assessment (Conway, 1996; Vermaaten *et al.*, 2012) or risk management (Barateiro *et al.*, 2010), and others describe digital preservation as consisting of actions or practices that include risk assessment and/or risk management (Barateiro *et al.*, 2010; Ross and McHugh, 2006a, b; Strodl *et al.*, 2007).

In digital preservation risk has tended to be examined and discussed in a deterministic way that treats it as both knowable and calculable. Recent initiatives have taken steps to develop systems that will help repositories quantify their risk exposure (e.g. Barons *et al.*, 2021). Research and scholarship about risk in digital preservation has tended to focus on identifying and/or classifying types of threats and vulnerabilities (e.g. Saffady, 2020; Schaefer *et al.*, 2021; Vermaaten *et al.*, 2012), and developing typologies of risk (e.g. Barateiro *et al.*, 2010; Clifton, 2005; Dappert, 2009; Mayernik *et al.*, 2020).

Although it is useful to carry out this descriptive work, it is also important to understand how people in digital preservation perceive and construct their understanding of risk (e.g. Nelkin, 1989) because digital preservation outcomes depend on the actions of people in response to risk information – not just on the identification of risk (e.g. Dearborn and Meister, 2017).

Trustworthy digital repositories

Certification as a TDR is one way that digital repositories have demonstrated their trustworthiness for long-term preservation (Center for Research Libraries, n.d.). Processes for

TDR certification include TRAC/ISO 16363, CoreTrustSeal and the nestor seal (Center for Research Libraries, n.d.; Consultative Committee for Space Data Systems, 2012a; CoreTrustSeal Standards and Certification Board, 2022; nestor-Siegel, 2018). These certification systems have developed different criteria to assess how well a repository's policies and practices align with the OAIS model (Consultative Committee for Space Data Systems, 2012a, 2012b; CoreTrustSeal Standards and Certification Board, 2022; Nestor Working Group Trusted Repositories - Certification, 2009). Developments such as the TRUST Principles echo the need for trustworthiness via transparency, but do not require a formal certification (Lin *et al.*, 2020).

Risk is foundational for repository certification (e.g. Frank, 2022), but scholarship has tended to focus on trust and trustworthiness (e.g. Bak, 2016; Dryden, 2008; Faundeen, 2017). Research about TDR certification has examined the trustworthiness of repositories that have received certification (e.g. Donaldson, 2020; Donaldson and Russell, 2023), investigated the process and/or value proposition of certification (e.g. Lindlar and Schwab, 2019) and examined particular elements of certification such as the Designated Community (e.g. Bettivia, 2016; Moles, 2022). Other scholarship has described the process of developing and maintaining certification systems (e.g. Dobratz and Neuroth, 2008; Giaretta, 2011; L'Hours *et al.*, 2019), and reported on the experience of becoming certified as a TDR (e.g. CLOCKSS, 2014; Free, 2011; Kirchhoff *et al.*, 2010).

The majority of this work has operated from the baseline assumption that TDR certification delivers on its promise to evaluate the trustworthiness of digital repositories for long-term preservation. Meaning, repositories that become certified have shown that they can preserve digital information. For example, Donaldson and Russell investigated whether repositories' CTS certification scores improved over time, but asked whether repositories "improved their trustworthiness" (2023, p. 553).

While some scholarship has been critical of TDR certification (e.g. Bak, 2016), there is a need for research that critically investigates the theories and concepts that form the foundations of repository certification.

TRAC: trustworthy digital repository audit and certification

In this article I focus on the TRAC certification system, which was administered by the Center for Research Libraries. TRAC was developed by a group consisting of CRL, the Research Libraries Group (RLG), the National Archives and Records Administration (NARA), and the Consultative Committee for Space Data Systems (CCSDS) (Yakel, 2007). The TRAC checklist was created in 2007 and the ISO 16363 standard was approved in 2012 and confirmed again in 2017 (Consultative Committee for Space Data Systems, 2012a; RLG-NARA Digital Repository Certification Task Force, 2007). CRL conducted audits using the TRAC checklist from 2010 to 2014 (Center for Research Libraries, 2010, 2011, 2012, 2013, 2014, 2015), and maintained the resulting certifications until at least 2018 (Center for Research Libraries, 2018).

TRAC was a process through which digital repositories could demonstrate their adherence with best practices in digital preservation, and the OAIS Model, in order to show that they could be trusted as long-term stewards of valuable digital information (Center for Research Libraries, n.d.). In order to demonstrate their trustworthiness, repository staff members would document their risk assessment and mitigation efforts for a team of external auditors (Frank, 2022).

In 2014 a standard for accreditation of ISO 16363 auditors was approved (Consultative Committee for Space Data Systems, 2014). The Primary Trustworthy Digital Repository Authorisation Body (PTAB) is currently (as of 2023) the only organization accredited to issue ISO 16363 certifications, and is the only organization that has carried out audits since CRL suspended their work (Giaretta, 2018; PTAB–Primary Trustworthy Digital Repository Authorisation Body Ltd, 2021).

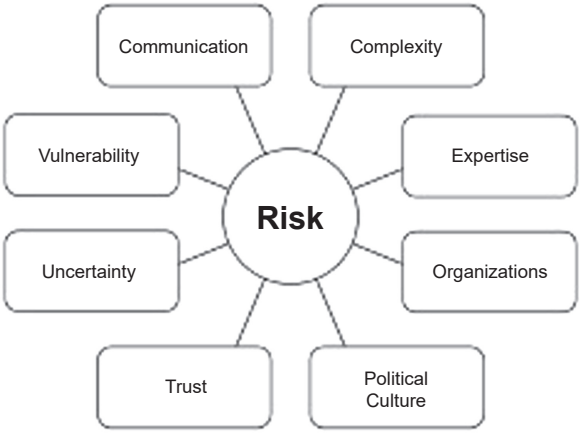
Theoretical framework: model for the social construction of risk in digital preservation

There is a need for empirical research that interrogates underlying assumptions embedded in repository certification systems. In this article, I apply the Model for the Social Construction of Risk in Digital Preservation (Frank, 2020) to the TRAC audit and certification process (see Figure 1: Model for the Social Construction of Risk in Digital Preservation (Frank, 2020)). This model argues that digital preservation is a social process in which risks are interpreted by individuals, whose behaviors and actions are shaped by those interpretations.

Burgess explains, "the essence of the social construction perspective is to direct us to understand the particular economic, social, political, and cultural influences and actors that lead to the singling out and elevation of some things over others," and argues that social construction is particularly relevant to the study of risk, because risk concerns itself with building – or constructing – a picture of future possible events and outcomes (2015, p. 57). The goal of applying social construction to digital preservation risk is to acknowledge that phenomena such as risks develop through interaction between people, organizations, technology, and the natural world. The varying perceptions of individuals matter, as well as the social factors that influence their perceptions and the resulting behaviors and decisions. By introducing a framework which addresses factors that can influence the ways in which people construct their understanding of risk, this study reinforces the notion that digital preservation outcomes depend on actions taken in response to interpretations of risk information. Applying this framework to an examination of three different groups of stakeholders in a TRAC audit (standard developers, auditors, and repository staff members) will provide an understanding of the social factors that contribute to their attitudes, and will facilitate an examination of the TRAC audit process that is human-centered rather than organizationally-, economically- and/or materials-centered.

(1) *Communication*: Perceptions of risk change depending on how information is communicated, such as the source, method, and means. These factors can amplify or attenuate perceptions of risk (e.g. Kasperson and Kasperson, 1996).

(2) *Complexity:* High levels of complexity can make it difficult to identify hazards, and their probabilities and consequences. Complexity in systems can also lead to increased risk due to unexpected interactions between component parts (e.g. Perrow, 1999; Wilkinson, 2001).



Source(s): Frank (2020) figure by author

Figure 1.
Model for the social construction of risk in digital preservation

(3) *Expertise*: Both expertise and lack of expertise can influence perceptions of risk. Experts may have specific knowledge but can be limited in their perspective, while non-experts may have a broader understanding of social contexts (e.g. Wynne, 1992).

(4) *Organizations*: Organizations both produce and manage risk, and perceptions of risk are impacted by the roles of individuals within them. Risk management activities occur within an organizational context, and are affected by the organization and the individuals participating in them (e.g. Vaughan, 1996).

(5) *Political Culture:* National context influences how risks are defined. Perceptions of risk are shaped by the political culture within which individuals exist, and by their place or role within that culture (e.g. Jasanoff, 1986).

(6) *Trust*: Perceptions of risk can vary depending on the trust among individuals and groups with different knowledge and expertise in an organization (e.g. Wildavsky and Dake, 1990).

(7) *Uncertainty*: Risk and its components (hazard, probability, consequences) are hard to identify and understand in uncertain situations, and uncertainty affects how people perceive risk (e.g. van Est *et al.*, 2012).

(8) *Vulnerability*: Risk exposure, or vulnerability, influences perceptions of risk. Those who can manage their exposure to risks may view them differently than those who cannot (e.g. Murphy, 2006).

Research methods

This article presents findings from a larger research project focused on understanding how stakeholders (e.g. standard developers, auditors, and repository staff members) in the TRAC audit and certification process construct their understanding of risk as it relates to the long-term preservation of digital information. The results are based on 42 interviews and content analysis of the standards and audit reports.

Sites and participants

At the time of data collection for this study (2016), six repositories were certified by CRL as TDRs using the TRAC checklist. Four repositories received certification for the entire repository: Canadiana.org, Chronopolis, HathiTrust, and Portico (Center for Research Libraries, 2010, 2011, 2012, 2015), and two for their e-journal content only: CLOCKSS and Scholars Portal (Center for Research Libraries, 2013, 2014). These six repositories formed the sites for my research. A brief overview of each site follows:

(1) Canadiana.org: a nonprofit coalition of memory institutions in Canada. Preserved and provided access to digital resources as well as aggregating metadata from partner organizations (Canadiana.org, 2015). Merged with the Canadian Research Knowledge Network in 2018 (Canadian Research Knowledge Network, 2021).

(2) Chronopolis: a digital preservation network managed by the University of California, San Diego Library (UCSDL), National Center for Atmospheric Research (NCAR), and University of Maryland Institute for Advanced Computer Studies (UMIACS) (UC San Diego: The Library, 2021).

(3) CLOCKSS: a repository that is a partnership with Stanford University and member organizations which pay a fee for participation that preserves e-journal content (UC San Diego: The Library, 2021).

(4) HathiTrust: a repository that preserves and provides access to digitized content from partner organizations, including the Google Books project (HathiTrust Digital Library, 2024)

(5) Portico: a not-for-profit organization that focuses on preserving e-journals and e-books (ITHAKA, 2021).

(6) Scholars Portal: a repository in Ontario, Canada that preserves and provides access to digital information collected and shared by Ontario university libraries (Ontario Council of University Libraries, 2021).

The participants were recruited from three groups who are involved in the TRAC certification system: (1) standard developers, (2) auditors and advisory board members from CRL, and (3) staff members from the six repositories listed above. See Table 1 for a breakdown of participants by professional role and role in the certification process.

Data collection

Mixed methods data collection (interviews and content analysis) was completed for the six sites. I conducted in-depth interviews with the participants. Each interview lasted 1–2 h, depending on the participant's role in the TRAC audit process. The interviews were divided into two parts. The first half was based on a vignette sent to participants before the interview. The vignette was a one-page repository description I created using profiles of six TRAC certified repositories and certification requirements in the TRAC standard. Participants discussed the vignette, identified potential risks for the repository and discussed ways to manage or mitigate them. Vignettes are a useful interviewing method for research when participants are identifiable within their community, as standard developers, auditors, and repository staff members likely are (Gubrium and Holstein, 2001).

The second half of the interview focused on the participant's experiences. The questions asked them to talk about their own experiences with the repository audit and certification process and identify potential sources of risk for digital repositories. The interviews were recorded and transcribed for analysis.

Documents collected included the three standards upon which TRAC certification is based, ISO 14721, ISO 16363, and ISO 16919 (Consultative Committee for Space Data Systems, 2012a, 2012b, 2014), the certification reports created by CRL (Center for Research Libraries, 2010, 2011, 2012, 2013, 2014, 2015, 2018), and any publicly available documents from the six certified repositories about their certification.

This study was reviewed and deemed "not regulated" by the Institutional Review Board at the author's university.

Data analysis

I analyzed the interview transcripts using the qualitative data analysis program NVivo. I used an open coding approach that combined descriptive, analytic, and thematic codes. The

Table 1. Participants by role

		Professional roles			
		Administration	Digital preservation	IT	Total
Certification roles	Standard developers	0	8	3	11
	Auditors	4	6	0	10
	Repository staff	9	6	6	21
	Total	13	20	9	42

analysis started with an initial list of codes based on concepts from literature and added themes that came up during a pilot study and the interviews. Codes were related to the eight factors in the Model for the Social Construction of Risk in Digital Preservation (Frank, 2020), and concepts like interaction between auditors and repository staff, challenges during the audit process, and potential risks identified by participants.

Interview transcripts were analyzed in two groups: (1) standard developers ($N = 11$) and auditors ($N = 10$) and (2) repository staff members ($N = 21$). I enlisted the assistance of additional coders and together we achieved a Scott's Pi, a statistic measuring interrater reliability, of 0.719 for the first set of interviews and 0.711 for the second. This process provided assurance of the reliability of my analysis (Craig, 1981; Scott, 1955).

Limitations

Participants experienced some memory and recall issues, particularly those involved in earlier audits. To address this, links to each repository's TRAC certification report were sent to participants before interviews and they were advised to refer to their own notes, documents, emails, or calendars before and during interviews. Many participants did so. The TRAC audit and certification system was relatively new and the population of standard developers, auditors, and repository staff members small, which may have led to social desirability effects during interviews (Bernard, 2013). To offset this, the vignette portion of interviews were included. The anonymity of participants had to be maintained, limiting the analysis in some areas. Future research may be able to address issues such as political and legal risks in greater depth as the number of certified repositories, standard developers, and auditors increases.

Additionally, the data for this research was collected in 2016, a time when the TDR certification landscape was smaller and less well-developed than 2024. However, in the time since data collection the TRAC and ISO 16363 criteria have remained largely unchanged, and no additional repositories have become TRAC certified.

Findings

This research applied the Model for the Social Construction of Risk in Digital Preservation to qualitative data relating to the TRAC audit process to examine whether and how the eight factors in the model (i.e. communication, complexity, expertise, organizations, political culture, trust, uncertainty, and vulnerability) influence the ways in which standard developers, auditors, and/or repository staff members construct their understanding of risk in the context of a TRAC audit.

My findings support the argument that digital preservation should treat risk as a socially constructed phenomenon and consider how social factors contribute to an understanding of risk in the audit and certification of TDRs. I found that all eight factors from the model were present in the data, and four factors – communication, expertise, uncertainty, and vulnerability – were particularly strong factors that influenced how auditors and repository staff members understood risk in the context of a TRAC audit. As such, these four factors are designated as "primary factors," and complexity, organizations, political culture, and trust are designated as "secondary factors."

Primary factors

Communication. Communication among certification stakeholders influenced the ways in which they constructed their understanding of risk. The development of a shared understanding of risk in the certification process depended on how information about the repository was communicated to auditors and how information about the certification

process itself was communicated to repository staff members. Face-to-face communication enabled auditors and repository staff to establish a shared understanding of repository policies and practices during the TRAC audit site visit. Standard developers, auditors, and repository staff described the site visit as an important element of the audit process. While standard developers and auditors characterized the site visit as an opportunity to address gaps and identify problems, repository staff described the site visit as an opportunity to confirm the accuracy of their documentation.

Standard Developers 01, 03, 08, and 10 described a process whereby the audit team would review documentation provided by a repository and then visit the repository to determine the accuracy of the documentation. Standard Developer 03 explained that the face-to-face communication during the site visit was crucial for developing a shared understanding between auditors and repository staff, "often what you find when you get on-site is, you can develop sort of a picture of what a repository is doing from that documentation, but when you're actually there with the folks in front of you and you actually sit down with them and have them demonstrate some of the processes that they use you find new questions that you hadn't thought of that you need to ask them about."

Auditors stressed the importance of the information that they gathered on-site for their assessment of each repository, "you come to understand certain policies or decisions, when you're on site, that may be a little bit more difficult to grasp from paper" (Auditor 10).

Repository Staff 07, 11, 13, 16, 18, and 19 characterized the site visit as a positive experience. Repository Staff 11 and 13 both said that their site visits went smoothly because they had planned ahead in order to manage the process and keep both repository staff members and auditors focused: "We managed the on-site review pretty carefully . . . we tried to control the on-site review process as much as possible, and I think that ended up working well" (Repository Staff 13).

In contrast, Repository Staff 21 said that she found the site visit superficial. She expected the auditors to be more skeptical of the repository, and to seek out evidence to support the repository's documentation rather than trusting repository staff members at their word, "I just felt, they're not really diving in deep enough. It's just asking surface questions based off of the checklist criteria and not really going in depth in terms of evaluating the content" (Repository Staff 21).

Standard developers, auditors, and repository staff agreed about the importance of the site visit and the value of direct, face-to-face communication between auditors and repository staff in establishing a shared understanding of repository policies and practices. While standard developers and auditors described the site visit as an opportunity to ask questions, gather additional information, and verify the accuracy of documentation, repository staff described it as a chance to demonstrate the accuracy of their documentation and provide auditors with context. Auditors described a focus on getting answers to their questions, while repository staff expressed mixed opinions about the depth of understanding that auditors were able to reach in just a couple of days and in some cases argued that maintaining strict control over the site visit agenda helped them to shape the process.

Expertise. Expertise was influential in how interviewees understood potential sources of risk. For example, expertise came up in relation to the TRAC requirement that repositories have documentation about organizational structure and staffing to ensure that they have (1) appropriate staffing levels, and (2) staff with sufficient expertise to carry out the work necessary for long-term digital preservation. While standard developers and auditors thought that the required documentation was evidence that a repository had the expertise necessary for the work of long-term preservation, repository staff said that there was a big difference between understanding the types of expertise needed, and maintaining staff with that expertise.

Several interviewees described their repositories as lacking appropriate staffing to carry out the work of long-term digital preservation, or their fellow staff members as having a narrow view of the repository based on their roles rather than understanding their work in the context of the larger mission of long-term preservation. For example, Repository Staff 21 described the staffing model of her repository as one that was too small to carry out the work necessary for long-term preservation, and as a result most of her team members did not understand the concept of risk in the context of long-term preservation, "I don't think people there really, the people on the team aside from a few individuals, really understood that kind of concept of long-term risk outside of just technical stuff" (Repository Staff 21).

The issue of auditor expertise was also discussed by repository staff members. Interviewees noted the importance of auditors with expertise in both the audit process and the digital preservation processes that they were evaluating, "I think expertise and background, the experience of the auditors matters a lot" (Repository Staff 08). This interviewee went on to say that the value of a TRAC audit is directly linked to the level of expertise held by the auditors: "a TRAC audit is only as good as the knowledge of the auditors deploying that model."

Some interviewees expressed concern that the auditors assigned to their review lacked the necessary expertise to assess their repository, "I would say the most time consuming was the technical section . . . Because I think it's in many ways the section that the auditors and the people we were talking to understood the least" (Repository Staff 04). This interviewee explained further that the audit process involved a lot of activity that felt irrelevant or inefficient: "A lot of times the questions we got didn't make a lot of sense. They sounded like they were questions written by someone who was being asked to ask them, but wasn't an expert in them."

My findings indicate that interviewees viewed expertise as important for identifying and managing risks within repositories, and for the TRAC certification process. While standard developers and auditors assumed that knowing what types of expertise were needed would ensure that repositories could maintain that expertise on staff, repository staff thought that knowing what types of expertise were necessary for repository management was only the first step toward maintaining that expertise. In addition to the certification requirements about the expertise of repository staff, interviewees also expressed strong views about the importance of auditor expertise in understanding and evaluating repositories.

Uncertainty. Uncertainty throughout the TRAC audit process influenced the ways that interviewees understood risk. For example, interviewees from all three groups agreed that repositories should undergo periodic reviews to maintain TRAC certification. However, there was uncertainty about how frequently reviews should happen and who should initiate them. The TRAC standard provided little guidance about how repositories should maintain certification, but many auditors and repository staff members were under the impression that it called for recertification every three years. This schedule was not supported by the CRL certification reports, nor by the auditors who were directly involved in helping repositories to maintain their certification. Auditors anticipated repository staff reaching out for new disclosures or inspections, while staff expected CRL to initiate recertification reviews.

While the TRAC standard does not specify a schedule, one standard developer explained that certification should entail annual audits as well as recertification every three years, "You have continuing audits. You have yearly maintenance audits and you have to get recertified . . . every three years" (Standard Developer 08).

Interviews with auditors revealed a lack of consensus about how repositories should maintain their certification. Auditor 03 explained: "As long as their conditions remain about the same as when they were certified, the TRAC certification holds. It doesn't have an expiration" (Auditor 03). She added that repositories should notify CRL of any substantial

changes, "They're supposed to tell us if there's any significant changes within the organization, and then we would decide whether or not we needed to review it" (Auditor 03). In contrast, Auditor 06 said that the repositories were told that they would be reviewed for recertification after three years, and Auditors 08 and 10 both agreed that repositories should undergo regular audits in order to maintain certification, but were uncertain about what the schedule should be.

While repository staff shared similarly mixed opinions about the audit schedule for recertification, most expected that CRL would initiate the process, and several indicated that their repositories expected to be contacted for their recertification audit. In contrast, Repository Staff 11 and 17 were the only interviewees to report that their repositories were in regular contact with CRL to advise them of major changes. Repository Staff 11 said that her repository would reach out to CRL as needed to update documentation, "As things change or shift, we'll reach out to CRL and let them know what we've got going on." Repository Staff 17 was the only repository staff member who described a process of updating documentation and notifying CRL, which aligned with the process described by Auditor 03 above, "We do an annual review that we submit to them. Sometimes they follow up, sometimes they don't."

Repository staff members described their organizations as continually changing to meet the needs of their stakeholders and keep up with new technologies. Most repository staff members who were interviewed for this study said that their repositories had implemented substantial changes since they achieved TRAC certification. Repositories claiming certification but operating under policies and practices that have not been reviewed – even when repository staff believe them to be improvements over the versions that were reviewed during their audit – calls into question whether external stakeholders can trust claims of TRAC certification to tell them anything about the current state of a repository.

Vulnerability. Risk research has shown that lived experience, including exposure or vulnerability to risk, can influence risk perception. Standard developers, auditors and repository staff all described reliance on short-term funding sources, such as grants, as increasing the vulnerability of a repository. A lack of stable long-term funding was described as a significant source of potential risk for digital repositories by Standard Developers 01, 02, 03, 06, 07, 08, 09, and 10, who emphasized that digital preservation requires continuous funding, "Money, funding. Long-term availability of the data, depending upon – since long-term availability is dependent on containing funds for the data being preserved, for keeping the data preserved or at least continuous monitoring of the data" (Standard Developer 01).

Following the lead of the standard developers, auditors also framed financial vulnerability as a source of potential risk for digital repositories. Auditors 01, 03, 04, 07, and 08 argued that sufficient funding was a basic requirement for repositories engaged in long-term preservation of digital content and that without adequate funding repositories would fail, "Basically, money is life in this case. If they don't have adequate funding, they're going to fail" (Auditor 03). Auditor 02 expressed a similar position, saying that no policy could compensate for a lack of funding, "if money dries up it doesn't matter how many policies they have in place. They don't have the funding to do it" (Auditor 02).

Repository staff framed financial sustainability as a potential source of risk for digital repositories generally, and for their own repositories more specifically. They shared an understanding of the importance of funding for their repositories and the threat that loss of funding posed for both their repositories as well as their digital content. They also described an environment in which resources were scarce and shifting organizational priorities meant that they felt that their budgets were vulnerable and under constant threat, "people don't want to pay for preservation at all . . . It's always been the money is the hardest, most riskiest challenge" (Repository Staff 04).

Several repository staff members said that their repositories fell short of the requirements set forth by the TRAC standard to demonstrate mitigation of threats to financial sustainability, but all received TRAC certification. Their views about whether their repositories had sufficiently addressed threats to financial sustainability were influenced by their own vulnerability to those risks. Repository staff members, who experienced greater vulnerability than either the standard developers or auditors to the potential sources of risk facing their repositories, were less likely to view those risks as manageable. Additionally, they did not believe that meeting the requirements described in the TRAC standard that the auditors were enforcing would make their repository trustworthy in terms of their ability to preserve digital content.

The TRAC audit process assumed that individuals would identify risks and agree about the appropriate mitigation techniques regardless of their closeness to the repository and/or digital content. Yet, findings from this study indicate that individuals outside of the repository, who may not have a strong understanding of a particular repository's policies and processes and whose livelihoods would not be threatened by repository failure, viewed risks as manageable while repository staff did not.

Secondary factors

Complexity. Interviewees found the organizational, legal, and technical aspects of repository management complex, and identified this complexity as a potential source of risk. While all three groups described digital object management processes as complex, they disagreed about whether risks in this area could be mitigated through documentation. A common theme among standard developers was the challenge that file formats posed to long-term preservation of digital content, "the more formats that you are taking in and using for your AIPs [archival information packages], the more complex that gets" (Standard Developer 03). Standard Developers 03, 04, 06, and 08 all discussed potential threats to repositories and digital content relating to file formats and digital object management.

Auditors explained that the work of coordinating and managing the complex set of tasks for digital object management was difficult, "Being able to coordinate those functions and have clear lines of authority about when a policy is put in place, who has to adhere to it, and where the responsibility lies, that can be very difficult to do" (Auditor 01).

Standard developers and auditors said that it was difficult for repository staff to meet the criteria in the TRAC standard for digital object management and argued that the discrepancy between the ideal and what repositories were realistically able to accomplish presented a risk to repositories and content. In contrast, repository staff members argued that the complexity of digital object management cannot be captured in documentation and that this was a potential area of risk for digital repositories because best practices for this complex work have yet to be established. "It quickly gets mind numbingly complex and we've talked about it a lot and have not come to any really good future-proof answers that we're comfortable with" (Repository Staff 07).

The complexity of the repository environment made it difficult for interviewees to agree on the effectiveness of mitigation strategies for potential sources of risk in the context of long-term digital preservation.

Organizations. Each TRAC audit was ultimately an exercise in assessing the risk of a particular organization. The standard developers and auditors each represented separate organizations as well. The findings from this study demonstrate that the standard developers, auditors, and repository staff involved in a TRAC audit represent different organizations that construct their own understandings of risk through the audit process.

While standard developers and auditors tended to agree on their definitions of risk, repository staff members held opposing views about whether and how the risks that they identified during a TRAC audit could be mitigated. This difference in perspective largely fell

across organizational lines – that is, the organization setting the standard and the organization enforcing the standard agreed about the effectiveness of the measures required, but members of the organizations being audited viewed the required risk mitigation measures as ineffective for long-term preservation.

In addition to notions of risk differing along organizational lines, interviewees viewed organizational instability as a potential source of risk for digital repositories. Standard developers focused on the ways the requirements laid out in the TRAC standard would mitigate potential threats to organizational instability: "I think that the main question of uncertainty is related to the low level of organizational infrastructure, more than any other thing. Because if you have good people, at the right point, and the responsibility is well developed, the uncertainty could be covered" (Standard Developer 05). In contrast, auditors and repository staff were skeptical about whether policies and documentation could accurately capture repository practices: "I think it probably could be quite difficult for any kind of certification program to validate how functional a governance system is" (Repository Staff 05).

The difference in perspective between those who developed the standard and those who enact it that this study has identified echoes findings from previous research about the ways that notions of risk are shaped within organizations, and the difficulties or disagreements that arise when those views are challenged by external actors, such as auditors (e.g. Vaughan, 1996).

Political culture. Political culture, both in terms of cultural and political context, and feelings of power and/or powerlessness in relation to risk, influenced how interviewees understood risk in the context of a TRAC audit. Interviewees identified national context as a potential source of risk for the repository described in the vignette. Specifically, they discussed potential problems for the repository that could arise from having data storage locations in two different countries: "[A]nother potential risk is, I'm not sure what the nature of the partnership is, but it is going across borders" (Standard Developer 02).

Several interviewees identified national context and/or moving data across borders as a potential source of risk for the digital repository described in the vignette. Of the two standard developers, three auditors, and five repository staff members who thought that having a data backup location in a different country was a potential source of risk, five were from the United States, and five were from Canada and Europe. Standard developers, auditors, and repository staff also agreed that having data storage sites in two different countries could endanger or limit federal and/or state funding for repositories, could introduce complexity by adding additional laws and/or regulations that a repository must comply with, and could create problems for material under copyright, "copyright law, liability law, these are all different in every country" (Auditor 09).

My findings indicate that long-term digital preservation relies upon a complex arrangement of legal agreements, and that working across international borders was viewed as a potential source of risk for repositories and the digital information that they sought to preserve. Interviewees across all three groups viewed the legal environment to be complex and difficult to navigate. Repository staff members were also skeptical about the enforceability of legal agreements regarding succession planning and therefore about the prospects for long-term preservation of their content.

Trust. Trust but verify was a sentiment that ran through responses from auditors and repository staff, and the site visit was the element of the audit that provided an opportunity for auditors to verify the trustworthiness of repository documentation. Auditor 10 explained that the act of observing repository practices in-person is an important part of the audit process, and that the site visit itself is part of the evidence that auditors should consider during an audit, rather than just trusting the documentation. "You see staff, you see equipment, you see servers, you're shown auditing software, and audit reports, and system

logs, and all kinds of things. You see them live. So you're bringing evidence yourself, you're a witness" (Auditor 10).

Repository staff members, however, had mixed opinions about the site visit. Repository Staff 13 described the site visit as an element of the audit in which auditors needed to be managed closely and guided to a positive outcome, rather than trusting that the auditors would be able to examine the repository and reach an informed decision: "We tried to control the on-site review process as much as possible, and I think that ended up working well" (Repository Staff 13).

Repository staff members also expected more rigorous examinations than the site visits afforded. Auditors went into the site visit with an expectation that the repository documentation could be trusted, while repository staff expected the auditors to be more skeptical. Repository Staff 21 said that she found the site visit superficial: "I do remember feeling like they were giving examples, but it wasn't an in-depth look into the content at a granular level."

While auditors tended to consider repository documentation to be trustworthy, and the site visit as an opportunity to verify its accuracy, repository staff members expected an audit process to be one in which auditors would be more skeptical and less trusting, thereby making the certification requirements more stringent.

Discussion

Risk is foundational for digital preservation (e.g. Conway, 1996) and the central role that it plays in this space is exemplified in the audit and certification of TDRs, processes which ask staff members of digital repositories to identify risks and create documentation to demonstrate evidence of risk management and/or mitigation efforts (Consultative Committee for Space Data Systems, 2012a; CoreTrustSeal Standards and Certification Board, 2022; Keitel, 2012). Despite the centrality of risk in digital preservation and TDR certification, the discipline continues to rely on an outdated understanding that treats risk in a probabilistic, deterministic way (e.g. De Vorsey and McKinney, 2010; Lawrence *et al.*, 2000; Saffady, 2020; Vermaaten *et al.*, 2012), rather than engaging with the extensive bodies of research which demonstrate that risk is socially constructed (e.g. Burgess, 2015; Gordy, 2016; Hilgartner, 1992; Nelkin, 1989). This study extends the current scope of research about risk in digital preservation to include theories that examine risk as a social construct, by critically examining the TRAC audit and certification system through the lens of the Model for the Social Construction of Risk in Digital Preservation (Frank, 2020).

In several cases, the factors from the model showed up in overlapping ways. For example, uncertainty about the TRAC audit process was amplified by poor communication between auditors and repository staff members. Information about how repositories should maintain their certification was communicated inconsistently, and as a result auditors and repository staff members expressed a great deal of uncertainty about what repositories should do to maintain their certification. Standard developers, auditors, and repository staff members agreed that repositories should undergo periodic reviews to maintain their TRAC certification. However, they disagreed about how frequently those reviews should happen and who should initiate them. The TRAC standard did not provide much guidance about how repositories should maintain certification, and standard developers did not discuss recertification much during their interviews, but many auditors and repository staff members were under the impression that the TRAC standard called for recertification every three years. This recertification schedule was not supported by the CRL certification reports, nor by the auditors who were directly involved in helping repositories to maintain their certification. Rather, these auditors expected that repository staff members would contact them any time a new disclosure and/or inspection was needed, while repository staff members expected that their recertification reviews would be initiated by the CRL auditors.

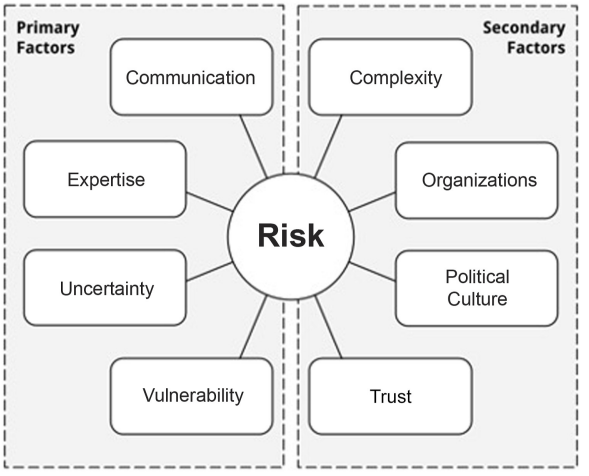
Revised model for the social construction of risk in digital preservation

In light of the findings described above I propose the following revision to the Model for the Social Construction of Risk in Digital Preservation (see Figure 2: Revised Theoretical Model for the Social Construction of Risk in Digital Preservation below), to reflect the fact that communication, expertise, uncertainty, and vulnerability emerged as particularly strong factors that influenced how auditors and repository staff members constructed their understanding of risk in the context of TRAC audit processes. In contrast, complexity, organizations, political culture, and trust also influenced the social construction of risk in the context of a TRAC audit, but to a lesser degree.

Scholarship about TDR certification tends largely to fall into a few categories: case studies and self-reports of repositories that have gone through certification processes (e.g. Kirchhoff *et al.*, 2010); scholarship produced by people and organizations that create, maintain, and/or administer TDR certifications (e.g. Giaretta, 2012; L'Hours *et al.*, 2019); research that seeks to understand the value of TDR certification (e.g. Donaldson and Russell, 2023; Lindlar and Schwab, 2019); and research that seeks to examine or interpret specific elements of TDR certification such as the Designated Community (e.g. Donaldson *et al.*, 2020; Moles, 2022). Scholarship across these areas tends to begin with the assumption that the certification processes do indeed evaluate the trustworthiness of repositories regarding long-term preservation, and that a repository which meets the criteria in the checklist will therefore be trustworthy. In contrast, this article interrogates one of the core concepts underlying TDR certification. Repository certification is fundamentally a process of risk assessment, but I have demonstrated here that a variety of social factors influenced the ways in which people involved in the TRAC audit and certification process constructed their understanding of risk.

Future research

This study also suggests some directions for future research. TRAC is just one type of certification that digital repositories can achieve, and was an early and influential certification system in the TDR landscape. In addition to applying the Model for the Social Construction of Risk in Digital Preservation to the TRAC audit and certification system, it



Source(s): Figure by author

Figure 2.
Revised theoretical model for the social construction of risk in digital preservation

could be applied to others such as CoreTrustSeal or the nestor seal, both of which have expanded greatly since 2016. Future research should investigate which of the factors in the model operate at the group level and which exert more influence at the level of the individual, as well as examining whether there are sub-factors at work within each. Future research should also examine the relationships between factors in this model in order to develop an understanding of the ways that they may amplify risk for repository stakeholders.

Conclusion

I presented a qualitative study of risk in trustworthy digital repository audit and certification, examining TRAC – an early and prominent TDR certification system. This study showed that the eight factors in the model for the social construction of risk influenced how interviewees understood risk in the context of a TRAC audit, and demonstrated that communication, expertise, uncertainty, and vulnerability showed up in particularly strong ways. As a result, I have revised the Model for the Social Construction of Risk in Digital Preservation that recognizes primary and secondary factors (see Figure 2: Revised Theoretical Model for the Social Construction of Risk in Digital Preservation above).

This research makes several contributions to the fields of information science and digital preservation research. First, the findings from this study support the social construction of risk in digital preservation, moving beyond previous views that treated it as a technical, economic, or organizational phenomenon. The demonstrated applicability of this theoretical model to the TRAC certification process demonstrates that risk cannot be examined solely as a calculable phenomenon. Instead, future research, including research about TDR audit and certification processes, should consider digital preservation as a social phenomenon.

Risk, although a foundational concept in digital preservation, has been largely overlooked. This study reveals that actors in the TRAC certification process have varied understandings of risk, challenging the conventional view that risk is calculable and responses are predictable. The findings advocate for recognizing risk as a social construct and understanding diverse perceptions of risk before proposing risk management solutions for digital repositories. Understanding risk as a social construct, and considering the ways in which perceptions of risk are influenced by social factors, can impact the adoption and implementation of risk assessment processes in digital preservation.

Third, scholars, such as Becker *et al.* (2020), have argued that there is a need for clarity around the definitions of key terms in digital preservation, a field in which various stakeholder groups understand key concepts differently. This research echoes that argument, demonstrating that assumptions about risk have led to a more narrow understanding of the term than is warranted. Rather than a deterministic classical view of risk, I argue that digital preservation should treat risk as a social construct.

References

Anderson, C. (2005), "Digital preservation: will your files stand the test of time?", *Library Hi Tech News*, Vol. 22 No. 6, pp. 9-10, doi: 10.1108/07419050510620226.

Bak, G. (2016), "Trusted by whom? TDRs, standards culture and the nature of trust", *Archival Science*, Vol. 16 No. 4, pp. 373-402, doi: 10.1007/s10502-015-9257-1.

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, doi: 10.2218/ijdc.v5i1.140.

Barons, M., Bhatia, S., Double, J., Fonseca, T., Green, A., Krol, S., Merwood, H., Mulinder, A., Ranade, S., Smith, J.Q., Thornhill, T. and Underdown, D.H. (2021), "Safeguarding the nation's digital

memory: towards a Bayesian model of digital preservation risk", *Archives and Records*, Vol. 42 No. 1, pp. 58-78, doi: 10.1080/23257962.2021.1873121.

Becker, C., Maemura, E. and Moles, N. (2020), "The design and use of assessment frameworks in digital curation", *Journal of the Association for Information Science and Technology*, Vol. 71 No. 1, pp. 55-68, doi: 10.1002/asi.24209.

Berman, F. (2008), "Got data?: a guide to data preservation in the information age", *Communications of the ACM - Surviving the Data Deluge*, Vol. 51 No. 12, pp. 50-56, doi: 10.1145/1409360.1409376.

Bernard, H.R. (2013), *Social Research Methods: qualitative and Quantitative Approaches*, 2nd ed., SAGE, 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, doi: 10.1002/pra2.2016.14505301038.

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

Canadian Research Knowledge Network (2021), "Heritage content", available at: https://www.crkn-rcdr.ca/en/heritage-content (accessed 5 May 2021).

Canadiana.org (2015), "About Canadiana.org", *Canadiana*, available at: http://www.canadiana.ca/en/about (accessed 30 March 2016).

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

Center for Research Libraries (n.d.), "TRAC metrics", available at: https://www.crl.edu/archiving-preservation/digital-archives/metrics-assessing-and-certifying/trac (accessed 7 March 2023).

Clifton, G. (2005), "Risk and the preservation management of digital collections", *International Preservation News*, Vol. 36, pp. 21-23.

CLOCKSS (2014), "CLOCKSS archive certified as trusted digital repository; garners top score in technologies", CLOCKSS News, available at: https://www.clockss.org/clockss/News (accessed 30 March 2016).

Consultative Committee for Space Data Systems (2012a), *Audit and Certification of Trustworthy Digital Repositories. Space Data and Information Transfer Systems ISO 16363:2012 (CCSDS*

652-R-1), Standard, Consultative Committee for Space Data Systems, Washington, DC, available at: http://www.iso.org/iso/catalogue_detail.htm?csnumber=56510 (accessed 5 August 2013).

Consultative Committee for Space Data Systems (2012b), *Reference Model for an Open Archival Information System (OAIS). CCSDS 650.0-M-2, Magenta Book*, Consultative Committee for Space Data Systems, Washington, DC, available at: https://public.ccsds.org/Pubs/650x0m2.pdf (accessed 19 July 2022).

Consultative Committee for Space Data Systems (2014), *Requirement for Bodies Providing Audit and Certification of Candidate Trustworthy Digital Repositories. Space Data and Information Transfer Systems ISO/DIS 16919, Standard*, Consultative Committee for Space Data Systems, Washington, DC, available at: https://public.ccsds.org/Pubs/652x1m2.pdf (accessed 11 February 2014).

Conway, P. (1996), *Preservation in the Digital World*, Commission on Preservation and Access, Washington, DC.

CoreTrustSeal Standards and Certification Board (2022), "CoreTrustSeal requirements 2023-2025", Zenodo. Epub ahead of print, available at: https://doi.org/10.5281/zenodo.7051012 (accessed 5 September 2022).

Craig, R.T. (1981), "Generalization of Scott's index of intercoder agreement", *Public Opinion Quarterly*, Vol. 45 No. 2, pp. 260-264, doi: 10.1086/268657.

Dappert, A. (2009), "Report on the conceptual aspects of preservation, based on policy and strategy models for libraries, Archives and data centres", IST-2006-033789. PLANETS-Project, available at: http://www.planets-project.eu/docs/reports/Planets_PP2_D3_ReportOnPolicyAndStrategyModelsM36_Ext.pdf (accessed 10 August 2014).

De Vorsey, K. and McKinney, P. (2010), "Digital preservation in capable hands: taking control of risk assessment at the national library of New Zealand", *Information Standards Quarterly*, Vol. 22 No. 2, pp. 41-44, doi: 10.3789/isqv22n2.2010.07.

Dearborn, C. and Meister, S. (2017), "Failure as process: interrogating disaster, loss, and recovery in digital preservation", *Alexandria: The Journal of National and International Library and Information Issues*, Vol. 27 No. 2, pp. 83-93.

Dobratz, S. and Neuroth, H. (2008), "Nestor: network of expertise in long-term storage of digital resources. A digital preservation initiative for Germany", *Microform and Imaging Review*, Vol. 33 No. 2, pp. 52-58, doi: 10.1515/mfir.2004.52.

Donaldson, D.R. (2020), "Certification information on trustworthy digital repository websites: a content analysis", *PLoS One*, Vol. 15 No. 12, e0242525, doi: 10.1371/journal.pone.0242525.

Donaldson, D.R. and Russell, S.V. (2023), "Trustworthy digital repository certification: a longitudinal study", in Sserwanga, I., Goulding, A, Moulaison-Sandy, H., Du, J.T., Soares, A.L., Hessami, V., and Frank, R.D. (Eds), *Information for a Better World: Normality, Virtuality, Physicality, Inclusivity, Lecture Notes in Computer Science*, Springer Nature Switzerland, Cham, pp. 552-562, available at: https://link.springer.com/10.1007/978-3-031-28032-0_42 (accessed 15 March 2023).

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, doi: 10.1108/jd-10-2019-0204.

Dryden, J. (2008), "From authority control to context control", *Journal of Archival Organization*, Vol. 5 Nos 1-2, pp. 1-13, doi: 10.1300/j201v05n01_01.

Faundeen, J. (2017), "Developing criteria to establish trusted digital repositories", *Data Science Journal*, Vol. 16, p. 22, doi: 10.5334/dsj-2017-022.

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, doi: 10.1002/asi.24247.

Frank, R.D. (2022), "Risk in trustworthy digital repository audit and certification", *Archival Science*, Vol. 22 No. 1, pp. 43-73, doi: 10.1007/s10502-021-09366-z.

Free, D. (2011), "HathiTrust certified trustworthy repository", *College and Research Libraries News*, Vol. 72 No. 5, pp. 254-257, doi: 10.5860/crln.72.5.8558.

Garrett, J. and Waters, D.J. (1996), *Preserving Digital Information: Report of the Task Force on Archiving of Digital Information*, The Commission on Preservation and Access & Research Libraries Group, Washington, DC, 9781887334501 1887334505, available at: https://www.clir.org/wp-content/uploads/sites/6/pub63watersgarrett.pdf

Giaretta, D. (2011), "Introduction to OAIS: OAIS concepts and terminology", in *Advanced Digital Preservation*, Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 13-30, available at: http://link.springer.com/10.1007/978-3-642-16809-3_3 (accessed 20 May 2016).

Giaretta, D. (2012), "OAIS model and certification of trusted digital repositories", *Fondazione Rinascimento Digitale*, available at: http://93.63.166.138:8080/dspace/handle/2012/117 (accessed 11 August 2014).

Giaretta, D. (2018), "First repository in the world has been awarded ISO 16363 certification", in *PTAB: Primary Trustworthy Digital Repository Authorisation Body Ltd*, News, available at: http://www.iso16363.org/first-repository-in-the-world-has-been-awarded-iso-16363-certification/ (accessed 23 July 2018).

Gordy, M. (2016), "The social construction of risk", in *Disaster Risk Reduction and the Global System*, Springer International, Cham, pp. 13-15, available at: http://link.springer.com/10.1007/978-3-319-41667-0_3 (accessed 19 February 2017).

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

HathiTrust Digital Library (2024), "Welcome to HathiTrust", available at: https://www.hathitrust.org/about (accessed 10 July 2024).

Hey, A.J.G., Tansley, S. and Tolle, K.M. (2009), *The Fourth Paradigm: Data-Intensive Scientific Discovery*, Microsoft Research, Redmond, Washington.

Hilgartner, S. (1992), "The social construction of risk objects", in Short, J.F. Jr and Clarke, L. (Eds), *Organizations, Uncertainties, and Risk*, Westview Press, Boulder, pp. 39-53.

Hitchcock, S., Brody, T., Hey, J. and Carr, L. (2007), "Digital preservation service provider models for institutional repositories: towards distributed services", *D-lib Magazine*, Vol. 13 Nos 5/6, pp. 5-6, doi: 10.1045/may2007-hitchcock.

ITHAKA (2021), "Why Portico", available at: https://www.portico.org/why-portico/ (accessed 5 May 2021).

Jasanoff, S. (1986), *Risk Management and Political Culture: A Comparative Study of Science in the Policy Context. Social Research Perspectives: Occasional Reports on Current Topics 12*, Russell Sage Foundation, New York.

Kasperson, R.E. and Kasperson, J.X. (1996), "The social amplification and attenuation of risk", *Annals of the American Academy of Political and Social Science*, Vol. 545 No. 1, pp. 95-105, doi: 10.1177/0002716296545001010.

Keitel, C. (2012), *DIN Standard 31644 and Nestor Certification*, Florence, Italy, available at: https://web.archive.org/web/20121127235326/http://www.rinascimento-digitale.it/conference2012-culturalheritageonline-programme.phtml

Kirchhoff, A., Fenton, E., Orphan, S., Morrissey, S. (2010), "Becoming a certified trustworthy digital repository: the Portico experience", *Proceedings of the 7th International Conference on Preservation of Digital Objects*, Vienna, Austria, 2010, pp. 87-94, available at: https://phaidra.univie.ac.at/o:185497

Lawrence, G.W., Kehoe, W.R., Rieger, O.Y., Walters, W.H., and Kenney, A.R. (2000), *Risk Management of Digital Information: A File Format Investigation, Council on Library and Information Resources*, Washington, DC, available at: http://eric.ed.gov/?id=ED449802 (accessed 5 November 2014).

Lin, D., Crabtree, J., Dillo, I., Downs, R.R., Edmunds, R., Giaretta, D., De Giusti, M., L'Hours, H., Hugo, W., Jenkyns, R., Khodiyar, V., Martone, M.E., Mokrane, M., Navale, V., Petters, J., Sierman, B., Sokolova, D.V., Stockhause, M. and Westbrook, J. (2020), "The TRUST Principles for digital repositories", *Scientific Data*, Vol. 7 No. 1, p. 144, doi: 10.1038/s41597-020-0486-7.

Lindlar, M. and Schwab, F. (2019), "All that work . . . for what? Return on investment for trustworthy archive certification processes – a case study", *Proceedings of the 15th International Conference of Digital Preservation*, Open Science Framework, Boston, MA, available at: https://osf.io/8a3sc/ (accessed 1 March 2022).

L'Hours, H., Kleemola, M. and De Leeuw, L. (2019), "CoreTrustSeal: from academic collaboration to sustainable services", *IASSIST Quarterly*, Vol. 43 No. 1, pp. 1-17, doi: 10.29173/iq936.

Mayernik, M.S., Breseman, K., Downs, R.R., Duerr, R., Garretson, A. and Hou, C.Y.S. (2020), "Risk assessment for scientific data", *Data Science Journal*, Vol. 19 No. 1, doi: 10.5334/dsj-2020-010.

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, doi: 10.1108/jd-02-2021-0041.

Murphy, M. (2006), *Sick Building Syndrome and the Problem of Uncertainty: Environmental Politics, Technoscience, and Women Workers. Durham [N.C.]*, Duke University Press, Durham.

Nelkin, D. (1989), "Communicating technological risk: the social construction of risk perception", *Annual Review of Public Health*, Vol. 10 No. 1, pp. 95-113, doi: 10.1146/annurev.pu.10.050189.000523.

Nelson, A. (2022), "Memorandum for the heads of executive departments and agencies: ensuring free, immediate, and equitable access to federally funded research. Office of science and technology policy (OSTP)", available at: https://www.whitehouse.gov/wp-content/uploads/2022/08/08-2022-OSTP-Public-Access-Memo.pdf (accessed 28 August 2022).

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

Nestor-Siegel (2018), "Evaluated Archives", available at: http://www.dnb.de/Subsites/nestor/EN/Siegel/siegel.html (accessed 23 July 2018).

Ontario Council of University Libraries (2021), "Scholars portal homepage", available at: https://scholarsportal.info/(accessed 5 May 2021).

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

PTAB - Primary Trustworthy Digital Repository Authorisation Body Ltd (2021), "Certified clients", available at: http://www.iso16363.org/iso-certification/certified-clients/ (accessed 26 May 2021).

Rieger, O.Y., Schonfeld, R. and Sweeney, L. (2022), "The effectiveness and durability of digital preservation and curation systems", 19 July. Ithaka S+R, available at: http://sr.ithaka.org/?p=316990 (accessed 21 July 2022).

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).

Ross, S. and McHugh, A. (2006a), "Preservation pressure points: evaluating diverse evidence for risk management", in *iPRES 2006*, Digital Curation Centre, New York, NY.

Ross, S. and McHugh, A. (2006b), "The role of evidence in establishing trust in repositories", *D-lib Magazine*, Vol. 12 Nos 7/8, doi: 10.1045/july2006-ross.

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

Schaefer, S.K., McGovern, N.Y., Zierau, E.M., Goethals, A.L. and Wu, C.C.M. (2021), "Deciding how to decide: using the digital preservation storage criteria", *IFLA Journal*, Vol. 48 No. 2, pp. 318-331, doi: 10.1177/03400352211011490.

Scott, W.A. (1955), "Reliability of content analysis: the case of nominal scale coding", *Public Opinion Quarterly*, Vol. 19 No. 3, p. 321, doi: 10.1086/266577.

Strodl, S., Becker, C., Neumayer, R. and Rauber, A. (2007), "How to choose a digital preservation strategy: evaluating a preservation planning procedure", *Proceedings of the 7th ACM/IEEE-CS Joint Conference on Digital Libraries*, New York, NY, pp. 29-38, available at: http://doi.acm.org/10.1145/1255175.1255181 (accessed 20 April 2014).

UC San Diego: The Library (2021), "About Chronopolis", available at: https://libraries.ucsd.edu/chronopolis/about/index.html (accessed 5 May 2021).

van Est, R., Walhout, B. and Brom, F. (2012), "Risk and technology assessment", in Roeser, S., Hillerbrand, R., Sandin, P., Peterson, M. (Eds) *Handbook of Risk Theory: Epistemology, Decision Theory, Ethics, and Social Implications of Risk*, Springer, Dordrecht, pp. 1067-1091, available at: https://doi.org/10.1007/978-94-007-1433-5_43 (accessed 18 June 2021).

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 Nos 9/10, doi: 10.1045/september2012-vermaaten.

Wildavsky, A. and Dake, K. (1990), "Theories of risk perception: who fears what and why?", *Daedalus*, Vol. 119 No. 4, pp. 41-60.

Wilkinson, I. (2001), "Social theories of risk perception: at once indispensable and insufficient", *Current Sociology*, Vol. 49 No. 1, pp. 1-22, doi: 10.1177/0011392101049001002.

Wynne, B. (1992), "Misunderstood misunderstanding: social identities and public uptake of science", *Public Understanding of Science*, Vol. 1 No. 3, pp. 281-304, doi: 10.1088/0963-6625/1/3/004.

Yakel, E. (2007), "Digital curation", *OCLC Systems and Services: International Digital Library Perspectives*, Vol. 23 No. 4, pp. 335-340, doi: 10.1108/10650750710831466.

About the author

Rebecca D. Frank, PhD is an Assistant Professor at the School of Information Sciences at the University of Tennessee, Knoxville and the Einstein Center Digital Future in Berlin, Germany. Her research examines the social construction of risk in digital preservation. She also conducts research about open data, digital preservation, digital curation and data reuse, focusing on social and ethical barriers that limit or prevent the preservation, sharing and reuse of digital information. Her work has been supported by the Deutsche Stiftung Friedensforschung, Einstein Centre Digital Future, InfraLab Berlin, National Science Foundation (US) and Australian Academy of Science. Rebecca D. Frank can be contacted at: frankrd@umich.edu