Archival Science (2022) 22:43–73
https://doi.org/10.1007/s10502-021-09366-z

ORIGINAL PAPER

Risk in trustworthy digital repository audit and certification

Rebecca D. Frank[1]

Accepted: 23 June 2021 / Published online: 20 July 2021

Abstract

Risk is a foundational concept in digital preservation. While it has been examined from technical, economic, and organizational perspectives, I argue that it is also a social phenomenon. In this study I report on the results from 42 interviews with stakeholders in the Trustworthy Repositories Audit & Certification (TRAC) system, and analysis of documents relating to the ISO 16363 standard in order to examine how standard developers, auditors, and repository staff members understand the concept of risk for digital repositories. The results of this research demonstrate that members of these three stakeholder groups identified risk in the TRAC audit and certification process in terms of specific potential threats or sources of risk, which I have organized into five main categories: finance, legal, organizational governance, repository processes, and technical infrastructure. While standard developers, auditors, and repository staff generally shared an understanding of the major sources of potential risk that face digital repositories, they disagreed about whether and how these risks can be mitigated and how mitigation can be proven. Individuals who were more removed from the day-to-day work of the repositories undergoing an audit were more likely to accept well-documented risk identification and mitigation strategies as sufficient evidence of trustworthiness, while repository staff were skeptical that documentation was sufficient evidence of risk assessment and mitigation and thus questioned whether this would translate to actual trustworthiness for long-term digital preservation.

Keywords Digital preservation · Trustworthy digital repositories · Social construction of risk · Trustworthy repository audit and certification

✉ Rebecca D. Frank
rebecca.frank@hu-berlin.de

[1] Berlin School of Library and Information Science, Humboldt-Universität zu Berlin, Unter den Linden 6, 10099 Berlin, Germany

Introduction

Digital information is a foundational element of many core values in our society including scientific research and scholarship, open government, and human rights. The right to benefit from scientific progress and its applications is a key element of the United Nations International Covenant on Economic, Social and Cultural Rights (United Nations Office of the High Commissioner 1966), and this right has been interpreted to include access to data (Porsdam Mann et al. 2018). Data produced through scientific research represent a tremendous investment of resources. In 2020, the National Science Foundation in the USA had a budget of approximately $8.35 billion and supported the work of 313,000 people (The National Science Foundation 2021b). During this time, 12,200 competitive awards were funded, including $198 million in funding to support COVID-related research (The National Science Foundation, 2021a). Since 2011, the NSF has required that all proposals include data management plans, including recommendations to deposit data into repositories for dissemination and preservation (National Science Foundation 2011). Despite the substantial investment of resources in the creation of this data, and mandates to ensure its longevity, risks abound in the processes of preservation of, and access to, digital information (Smith Rumsey 2016, p. 8).

In this article, I critically examine how individuals in three groups, standard developers, auditors, and repository staff, understand the concept of risk for digital repositories in the context of a Trustworthy Repositories Audit & Certification (TRAC) audit. I argue that although digital preservation has been examined from technical, economic, and organizational perspectives (e.g., Berman 2008; Dappert & Farquhar 2009; Jantz & Giarlo 2007), it is also a social phenomenon. This aligns with the understanding of risk as a socially constructed phenomenon proposed by scholars such as Burgess (2015) and Beck (1992), who describe risk as a concept that is constructed through social processes and situated within particular social contexts.

While the digital preservation community has regarded the concept of risk as a discoverable, calculable value, it is also socially constructed, and as such research that seeks to understand risk in digital preservation must consider the social context in which repositories exist and the ways in which social factors may influence how participants understand and behave in response to risk information.

This study is motivated by the following research questions:

1. How do standard developers, auditors, and repository managers conceptualize risk in the context of a TRAC audit?
2. What are the differences and similarities by which standard developers, auditors, and repository managers understand risk as it has been communicated by the TRAC standard?

    a. In what ways do these differences and similarities become manifest in the TRAC audit process?

3. What are the implications for repository certification?

My findings indicate that all participants (i.e., standard developers, auditors, and repository staff members) conceptualized risk in terms of concrete threats to the repository that I have organized into five categories: financial, legal, organizational governance, repository processes, and technical infrastructure. However, the social positionality of each group led them to define the nature of the risk differently and therefore view the efficacy of risk mitigation strategies differently. In contrast to the standard developers and auditors, the repository staff members were skeptical that the documentation required for TRAC certification was sufficient evidence of risk assessment and mitigation. They questioned whether this would translate to actual trustworthiness for long-term digital preservation. This research brings empirical research to the topic of trustworthy digital repository (TDR) certification and makes theoretical contributions about how the social construction of risk in the TRAC audit process influences the assessment of TDRs.

Literature review

The social construction of risk

A classical definition of risk, as described by the Royal Society, includes two elements that are commonly found in risk definitions across a variety of disciplines: an adverse event or hazard, and the likelihood of that event (Royal Society (Great Britain) & Study Group on Risk 1983). Hilgartner (1992) describes risk as consisting of three elements: an object that poses a risk, harm that could occur, and a linkage between the object and harm. Other definitions also include the magnitude of consequences of the adverse event (Leveson 2009). This view of risk as consisting of a source, an event, and the consequences and likelihood of that event is reflected in ISO 31000, an international standard for Risk Management (International Organization for Standardization Technical Committee 2018). This standard describes risk as the effect of uncertainty on objectives, and risk management as "the process whereby organisations methodically address the risks attaching to their activities with the goal of achieving sustained benefit within each activity and across the portfolio of all activities" (International Organization for Standardization Technical Committee 2018, p. 2).

Scholars such as van Est, Walhout, and Broum (2012) have noted the limitations of this view, and argued that the classical risk approach, which assumes that risks are calculable and knowable, fails to consider the complexity of situations in which risks occur. Indeed, scholars have argued that "risks are created and selected by human actors" (Renn 2008, p. 11). In contrast to the classical view of risk, those who understand risk as a social construct argue that risk is a concept which holds different meanings for different people, and that social, organizational, and political factors influence how they view and understand risk information (e.g., Beck 1992; Lachlan et al. 2009; Nelkin 1989; Nickel & Vaesen 2012; Renn 2008; Slovic 1987; van Est et al. 2012; Wildavsky & Dake 1990).

The classical view of risk is not entirely inconsistent with a constructivist view of risk. Rather, I argue that it is an incomplete view because it does not account for the different ways in which people construct their own understandings of risk in response to the information that comprises a classical definition (i.e., object, hazard, likelihood, and consequences).

Risk in digital preservation

Digital preservation has been characterized as a set of activities that ensure the viability of digital information over time (e.g., Berman 2008; Lazorchak 2011), and also as an ongoing process of risk management (Conway 1996). Definitions of digital preservation describe processes and actions that include risk assessment and/or risk management (e.g., Barateiro et al. 2010; Ross & McHugh 2006; Strodl et al. 2007). Across these characterizations, there is broad acceptance of the notion that the preservation of digital information and risk management practices are related.

Digital preservation as both an academic discipline and area of professional practice has engaged with risk as a knowable, calculable figure, reflecting the classical risk approach described above. As with the classical approach, this view of risk assumes that people will behave predictably in response to the same information. This positivistic view of risk is heavily influenced by computer science (e.g., Barateiro et al. 2011). Carried through into digital preservation research and practice, this manifests in the development of technical systems designed to overcome risks (e.g., Barateiro et al. 2010).

Scholarship in digital preservation has tended to focus on identifying and classifying vulnerabilities and/or threats, and case studies of individual repositories describing efforts to identify, manage, and/or mitigate those vulnerabilities (e.g., Saffady 2020; Vermaaten et al. 2012). This work does not reflect a constructivist view of risk, but rather assumes that stakeholders in digital preservation processes have the same perceptions of risk and therefore understand risk information in the same way. In making these assumptions, digital preservation scholarship has failed to engage meaningfully with research from other disciplines which has found that people construct their understandings of risk based on numerous social, organizational, and political factors, and that perceptions of risk—rather than risks themselves—drive decision-making and action (e.g., Ross & McHugh 2006).

Trustworthy repository audit and certification

Trust is a foundational concept for digital preservation (Hart & Liu 2003). Research about trust in digital preservation has addressed the development of repository assessment (e.g., Becker & Rauber 2011; Day 2008; RLG-OCLC Working Group on Digital Archive Attributes 2002). This has led to the establishment of the concept of TDRs: "trusted, reliable, sustainable digital repositories capable of handling the range of materials held by large and small research institutions" (Dale & Gore 2010, p. 16).

In response to calls for a formal certification process to assess digital repositories (e.g., Garrett & Waters 1996), the TRAC standard was developed. TRAC was a joint effort between the digital preservation and space data research communities, specifically by representatives from the Research Libraries Group (RLG), the National Archives and Records Administration (NARA), the Center for Research Libraries (CRL), and the Consultative Committee for Space Data Standards (CCSDS) (Yakel 2007). The Trustworthy Repositories Audit and Certification (TRAC): Criteria Checklist document was developed in 2007 (RLG-NARA Digital Repository Certification Task Force 2007), and the ISO standard was approved in 2012 (ISO 16363) (Consultative Committee for Space Data Systems 2012). TRAC certification assesses a digital repository's implementation of the Open Archival Information System (OAIS) (Consultative Committee for Space Data Systems 2012a) and "describes approximately 90 characteristics that must be demonstrable by repositories that aspire to a certifiable, trustworthy status" (McHugh et al. 2008, p. 132).

The view of risk described in the previous section above, as a knowable/calculable figure, is embedded in the OAIS standard (Consultative Committee for Space Data Systems 2012a) and TRAC certification process, as well as other certification processes such as the CoreTrustSeal (Dillo & De Leeuw 2018). For example, ISO 16363, which forms the basis for TRAC certification, defines a TDR as one that understands "threats and risks within its systems" (Consultative Committee for Space Data Systems 2012b, p. 19) and that can communicate this understanding to the public in order to engender trust. The standard provides criteria for assessment and examples for risk mitigation.

This approach treats risk as identifiable and asserts that risk assessment is an important part of digital preservation. For example, criteria 4.3.1 of the ISO 16363 checklist states: "The repository shall have documented preservation strategies relevant to its holdings" and posits this example of how repository staff members can demonstrate that their repository has met this requirement, "Documentation identifying each preservation risk identified and the strategy for dealing with that risk" (Consultative Committee for Space Data Systems 2012b, p. 52). Certification rests on the ability to identify risks and provide evidence of strategies in place to manage those risks.

In this article, I argue that risk identification is an important first step, but it is equally important to understand how digital preservation stakeholders construct those risks and how socially adaptive behavior is at play in response to that understanding.

Research methods

I conducted a mixed-methods study consisting of: (1) in-depth semi-structured interviews with standard developers, auditors, and repository staff, and (2) document analysis of the ISO 16363 standard, repository prepared responses to the TRAC checklist, CRL certification reports, and publications written by repository staff.

Sites

At the time of data collection for this study (2016), four comprehensive repositories were certified by the Center for Research Libraries (CRL) as TDRs: Portico, HathiTrust, Chronopolis, and Canadiana.org (Center for Research Libraries 2010, 2011, 2012, 2015). Two other repositories were certified as trustworthy for only their e-journal content: Scholars Portal and CLOCKSS (Center for Research Libraries 2013, 2014). These formed the sites for my study.

- *Canadiana.org* was a nonprofit coalition of Canadian memory institutions which preserved and provided access to digital resources, and was also an aggregator of metadata from partner organizations (Canadiana.org 2015). As of 2018, Canadiana.org merged with the Canadian Research Knowledge Network, and continues to focus on preserving and providing access to digital resources documenting Canada's national heritage (Canadian Research Knowledge Network 2021).
- *Chronopolis* is a digital preservation network that is managed by three organizations: University of California, San Diego Library (UCSDL), National Center for Atmospheric Research (NCAR), and University of Maryland Institute for Advanced Computer Studies (UMIACS) (*About* Chronopolis 2021).
- *CLOCKSS* is a repository that preserves e-journal content. The repository consists of a partnership with Stanford University and member organizations which pay a fee to participate (*Why CLOCKSS?*, 2021).
- *HathiTrust* is a partnership of research institutions and libraries. The repository contains digitized content from partner institutions, including from the Google Books project (*Welcome to HathiTrust!*, n.d.).
- *Portico* is a not-for-profit organization that preserves electronic scholarly content including e-journals and e-books (ITHAKA 2021).
- *Scholars Portal* is a repository that preserves and provides access to digital information collected and shared by university libraries in Ontario, Canada (Ontario Council of University Libraries 2021).

Participants

The participants for this study consisted of: (1) standard developers, (2) auditors and advisory board members from CRL, and (3) staff members from the six TRAC-certified repositories listed above. The standard developers group consists of individuals with a range of professional roles and affiliations who participated in standard development and maintenance on a voluntary basis. At the time of data collection for this study, CRL was the only organization that had conducted formal repository audits using the TRAC checklist. This group consisted of CRL staff members who participated in repository audits and advisory board members were individuals from CRL member organizations who were invited to participate in the audit process by reviewing documentation submitted by repositories and making recommendations to the auditors. The term auditors will refer to both groups throughout this article.

From previous research as well as a pilot study, I was able to determine that three primary types of repository staff members are typically involved in the TRAC audit process: repository administrators, digital preservation staff, and IT staff (Frank & Yakel 2013). I recruited three to five interviewees from each TRAC-certified repository who participated in the repository audit in some way, including at least one person from each functional area for every repository. Table 1 shows a breakdown of these interviewees, including information about their professional roles.

Data collection

Interviews lasted one to two hours, depending on the role of the interviewee. The first half of each interview focused on a vignette, which was sent to participants ahead of their interview. This vignette consisted of a repository description that I generated based on profiles of the six TRAC-certified repositories and the requirements described in the TRAC standard. Interviewees were asked to discuss the vignette, identify possible sources of risk for the repository described therein, and suggest ways to address or mitigate those sources of risk. The vignette provided common ground for making comparisons across interviewees and is a particularly helpful interview strategy when participants are highly visible and/or identifiable within their community, as standards developers, auditors, and staff members from TRAC-certified repositories were likely to be (Gubrium & Holstein 2001). In the second half of the interviews, participants were asked to discuss their own experiences because vignettes can help build an understanding of people's "perceptions, beliefs, attitudes, and behavior" but do not necessarily allow generalization to understanding real life (Hughes 2004). Interview questions asked participants to recall and discuss their own experiences with the repository audit and certification process. Interviewees were also asked to identify and discuss potential sources of risk for digital repositories. Interviews were audio recorded and transcribed for analysis.

In addition to interviews, I also collected documents relating to the six TRAC audits. Specifically, I gathered the ISO 16363 standard, the certification reports provided by CRL, the publicly available evidence provided by each repository in support of their audit, and publicly available documentation from each repository, where available. This study was reviewed and deemed "not regulated" by the Institutional Review Board at the author's university.

Table 1 Overview of Interviewees

	Roles			Total
	Administration	Digital preservation	IT	
Standard Developers	0	8	3	11
Auditors	4	6	0	10
Repository Staff	9	6	6	21
Total	13	20	9	42

Data analysis

Interview transcripts were coded and analyzed using NVivo, a qualitative data analysis software package. I employed an open coding approach that incorporated descriptive, analytic, and thematic codes. Starting with an initial set of codes based on my review of concepts from the literature, themes that emerged during a pilot study, and themes that arose during the interviews, I focused on concepts such as interaction between repository staff and auditors, types of evidence prepared for a TRAC audit, challenges encountered during the audit process, the eight factors that I identified as influencing how participants in the TRAC audit process constructed their understanding of risk (i.e., communication, complexity, expertise, organizations, political culture, trust, uncertainty, and vulnerability) (Frank 2020), and sources of risk that participants identified.

Using the code set that I developed, I coded the interview transcripts in two groups: (1) standard developers and auditors, and (2) repository staff members. Using Scott's Pi, a statistic measuring interrater reliability for coding text-based data (Scott 1955), I enlisted the help of additional coders and we achieved a score of 0.719 for the standard developers and auditors, and 0.711 for the repository staff members. This process provided assurance of the reliability of subsequent data analysis.

Document analysis focused on comparing the text of the ISO 16363 standard against documents created by auditors and repository staff members during the course of each TRAC audit. The comparative analysis of these documents looked: (1) within each audit to compare the interview data provided by repository staff to the response from auditors and also (2) across repositories to compare both the type and amount of evidence provided in response to each checklist item and to compare auditor responses to this evidence and finally the certification scores assigned by CRL. Document analysis helped to mitigate problems of memory and recall that arose during the interviews as many of the documents were created at the time of the audits and therefore could provide information about the social and organizational context in which the audits were conducted (Prior 2003; Sudman et al. 1996).

Limitations

I found that interviewees experienced some difficulties with memory and recall, particularly those whose experiences were in the earliest audits. In addition to memory and recall, rationalization and sensemaking happen over time. I addressed these challenges by including links to each repository's TRAC certification report in the interview request emails and by suggesting that participants may want to refer back to their own notes, documents, emails, or calendars either before or during the interview.

Audit and certification processes for TDRs are a relatively new phenomenon and the population that I examined in this study is small. Social desirability effects likely arose during interviews both within and across repositories, as well as among auditors and standards developers, due to the small size of the community (Bernard

2012, p. 205). Other response effects that likely arose included the expectancy effect, inaccuracy of self-reporting, and the deference effect (Bernard 2012). The vignette used in interviews was included in order to offset some of the limitations of conducting research with this small population.

Maintaining the anonymity of participants limited the analysis that I was able to conduct. For example, only a small number of participants were located outside of the USA. Potential sources of risk that emphasized political and/or legal issues were likely to reveal the nationality and/or location of participants, thereby making them identifiable within their professional community. Additionally, any risks discussed in the context of specific repository content or specific organizational relationships would also reveal the identity of participants. Future research may be able to address these topics in more detail as the number of TRAC-certified repositories grows and diversifies over time.

Findings

Overall the results present a nuanced picture of the TRAC audit process as one in which the actors involved agreed on a classical definition of risk, but differed about whether an audit process based on this definition can determine trustworthiness with regard to long-term digital preservation. My findings demonstrate that while standard developers, auditors, and repository staff generally shared an understanding of the major sources of potential risk that face digital repositories, and which are identified through a TRAC audit, they disagreed about whether and how these risks can be mitigated and whether the evidence required for TRAC certification was sufficient to demonstrate trustworthiness with regard to the long-term preservation of digital content.

Interviewees discussed risk in ways that were consistent with the classical definition discussed above. For example, when asked how confident he was in the accuracy and completeness of the risk information that he received from his own team members during his repository's audit, Repository Staff 18 explained that he did not think that his colleagues understood what risk meant for digital repositories, and that while it is relatively easy to find information about risk mitigation strategies it is more difficult to understand the probability and magnitude of consequences of a potential risk. This explanation highlighted an understanding of risk as calculable, but consisting of uncertain elements:

> *"Do I think that large amounts of people really understand how risk is constructed and what it means? No. … I think it's relatively easy to get information about solutions and how things are implemented, and it's harder to put that in a framework where you're measuring the likelihood of it happening against the potential of it happening, and what the downsides are there, and how you tie specific numbers to that."*

The view illustrated by this interviewee demonstrated an understanding of risk in digital preservation that assumes it is important to understand risk as a calculable figure, despite the uncertainty of being able to calculate the risk. As with the classical model of risk, this understanding is based on an underlying assumption that people are rational actors who will understand risk information in similar ways and behave predictably in response to that risk information.

Potential sources of risk

Standard developers, auditors, and repository staff members conceptualized risk in the TRAC audit and certification process in terms of specific potential threats or sources of risk, which I have organized into five main categories: finance, legal, organizational governance, repository processes, and technical infrastructure. In the following sections I will examine each category in greater detail.

Finance

Interviewees across all three groups described financial uncertainty as a potential source of risk to the long-term preservation of digital content and framed their understanding of this threat in terms of long-term business planning and risk identification, although each group understood this risk and appropriate measures of risk mitigation differently. While auditors and repository staff agreed with the conceptualization of financial risk presented by the standard developers, they thought that the types of evidence posited by the standard developers to mitigate financial risk were insufficient.

Standard Developers 01, 02, 03, 06, 07, 08, 09, and 10 described uncertainty about funding sources and the lack of stable long-term funding as a significant source of potential risk for digital repositories. For example, Standard Developer 03 argued that financial viability was a potential source of risk because so few repositories have managed to secure long-term funding and remain operational, "Well other than repositories that are institutionally mandated, a long-term business plan is very difficult to come by. You know, there are a few long-lived digital repositories that aren't institutional repositories, but there aren't many that have lasted very long. So just how do you ensure that you've got adequate funding over the long-term when people's interests change so rapidly?" This explanation highlights both the importance of long-term funding for digital repositories as well as the difficulty in securing that funding without an institutional mandate.

The perspectives presented by standard developers about financial sustainability as a potential source of risk for digital repositories is reflected in the text of the standard itself, which governed the audit process (Consultative Committee for Space Data Systems 2012b). It is through the development process for this document that the standard developers constructed and shaped an understanding of risk that includes threats to financial sustainability, and set expectations about how repository staff could demonstrate to auditors that they sufficiently identified and addressed those threats.

Despite their emphasis on the importance of financial sustainability, standard developers also recognized that securing long-term funding was a significant challenge for digital repositories. Thus, the succession plan requirement represented a workaround, or an alternate way for repositories to demonstrate the longevity of their digital content, “All of those sorts of things, and other repositories, the difficulty is the long-term funding, so in OAIS, the 16363, we kind of get around that by talking about having a succession plan” (Standard Developer 07).

As with the standard developers, auditors described succession planning as an important and necessary measure for repositories to mitigate the risk of organizational collapse due to insufficient funding, “I think that, in terms of the organization, they need to develop a succession plan and be very explicit about what’s going to happen if their grant funding dries up, and if the membership starts to drop” (Auditor 10). Taking that a step further, Auditor 01 said that while it was important to know that the repository had a succession plan, it was also necessary for the repository to have tested that plan to ensure that transfer of digital content was possible, “Has that been tested? How many times have they tested that? What kind of variety of data have they tested it with?”

Repository staff agreed with the standard developers and auditors that financial sustainability was a potential source of risk for repositories and their content, “There’s always a risk in that, with whatever might happen to that organization. Either a calamity, or loss of interest, or will, or funding, or whatever. There is a succession plan it says in there, so that’s obviously a significant mitigating tool for that kind of failure of the organization. I think succession is tricky” (Repository Staff 06). Echoing the sentiments of Auditors 06 and 08, Repository Staff 05 said that while funding challenges are a common and substantial threat to digital repositories, in his experience most repositories do not have a succession plan, “I think a lot of institutions have been facing significant funding challenges … Do you even have a succession plan? I think a lot of places don’t.”

Repository staff disagreed with standard developers and auditors about whether a succession plan was sufficient evidence of risk mitigation. Repository Staff 03, 06, 07, 12, and 21 all expressed skepticism that having a documented succession plan would ensure the longevity of a repository’s digital content, “I wasn’t necessarily convinced that writing that down necessarily meant that it would sustain it” (Repository Staff 03). Repository Staff 12 was quite blunt in her assessment of succession planning as a futile activity. In a discussion about the infrastructure and security risk management section of the vignette, she argued that succession planning did not make sense because it is unlikely that a second repository would be able to muster the funding and support the first was lacking:

> *“What is really going to be the reason repositories are at risk, is almost all around having enough money to take care of the material . . . a succession plan to move it someplace else, where the community isn’t going to have enough money to take care of it. Or there’s going to be a, someone who magically dumps money on the secondary repository. Why couldn’t they dump money on the first repository? … It doesn’t make sense.”*

Repository Staff 07 went a step further and explained that by their very nature succession plans are unenforceable because they are only enacted when a repository fails. When asked about the greatest specific risk for his repository at the time of their audit, he said that a succession plan does not ensure that the successor organization itself will be financially viable long-term:

> *" ... it's almost like that's a weak link too because if you have a succession by definition you're gone afterwards so you can put a plan in place but you're not around to make sure that it's going to be executed. Just like you're not around forever your successors aren't necessarily around forever. Our successors are primarily universities and government agencies which all claim and pretend that they will exist forever, but you can't guarantee that so the succession plan doesn't actually spell out what's going to happen from now until the end of forever it just says that there's an agreement in place, it's a time limited agreement."*

Standard developers, auditors, and repository staff all agreed that loss of funding and/or institutional support was a potential source of risk for digital repositories and their content. Standard developers and auditors viewed succession plans as more viable evidence that a repository was prepared to address financial risk than did repository staff. Repository staff understood the reasoning behind succession planning but did not agree that a succession plan provided evidence that the digital content would outlive the repository. While they were happy to provide documented succession plans in order to achieve TRAC certification, they felt that they were performing rather than demonstrating trustworthiness.

Legal

Interviewees described legal issues, such as contracts, agreements, licenses, and copyright, as potential sources of risk for digital repositories. Both auditors and repository staff members agreed with the conceptualization of risk presented by the standard developers in this area. However, the auditors and standard developers expressed a shared view that agreements among organizations governing relationships that would impact the long-term preservation of digital information should be the primary focus of concern. Repository staff members, on the other hand, were more concerned that intellectual property issues would threaten the repository itself. In short, repository staff members were primarily concerned with the ability of their own organization to carry out its work, while individuals external to the repositories were more interested in external relationships. As with the example of succession planning above, standard developers and auditors believed that it would be possible for digital content to outlive an individual repository, while repository staff were skeptical that this would be the case.

Standard developers framed legal risk to repositories in Section 3.5 of the TRAC standard as something that was of particular importance in relation to access. Through the process of creating this text the standard developers established an understanding of legal risk as one that was a threat to both the repository and the digital content, and communicated to both auditors and repository staff members that it was necessary and important to "ensure that the repository has the rights and authorizations needed to enable it to collect and preserve digital content over time, make that information available to its Designated Community, and defend those rights when challenged" (Consultative Committee for Space Data Systems 2012b, p. 31). Standard developers set expectations for auditors and repository staff that a repository could demonstrate that it met this standard through a variety of properly executed legal documents.

Standard Developer 01 explained that the legal repercussions of releasing protected data could threaten the continued existence of a repository, "There's laws in place in the U.S. I don't know about the rest of the world, but certainly in the U.S., depending on what your repository is storing you may have very severe penalties imposed on you if you release information that's supposed to be protected. The HIPAA [Health Insurance Portability and Accountability Act] is one example. There's a Title XIII, which is census data. Both of those are legal systems where keeping the data under security controls is tantamount to keeping your organization from being ground by the wheels of justice."

Alternately, Standard Developer 07 said that standard developers were not concerned with threats posed to a repository by legal issues, but rather to the digital information, "…we didn't care if the repository itself was sued out of existence. What we were concerned about is that they were sued out of existence before it could hand over its data, its information." For this interviewee, the legal danger to the organization, which a repository would be shut down before they could enact their succession plan, was a significant threat to the digital content.

Auditors did not devote much attention to legal risk during the interviews, but their discussions tended to express a shared understanding of risk in this area with the standard developers. Drawing from their experiences conducting audits as well as their own professional backgrounds in digital preservation, they focused on one aspect of the legal risk communicated through the TRAC standard. Namely, that it was important for repositories to have the appropriate legal agreements in place in order to ensure that their relationships with partners and members were secure. For example, Auditor 01 said that repositories "should probably have some legal staff on hand" to manage contracts among partner organizations because negotiating and executing things like service level agreements are complex and time-consuming. He also said that when assessing a repository it is important to understand whether those agreements are reciprocal or not in order to fully understand relationships among organizations and the potential sources of legal risk that the repository faces, "Is this a reciprocal agreement and what kind of risks does that expose them to?"

While standard developers and auditors emphasized the importance of having the necessary legal agreements in place in order to allow a repository to carry out the work necessary for long-term digital preservation, repository staff were not convinced that these legal agreements would be enough. Indeed, they were more concerned that even if these legal agreements were in place, execution of the access permissions and/or restrictions specified in, for example, intellectual property agreements would somehow fail, "a lot of the complexity came from … being able to provide access in the right ways" (Repository Staff 01).

Repository staff presented a view of legal risk that included a great deal of concern about copyright and the threat posed to repositories that provided inappropriate access to digital content. Repository Staff 06 explained that "the risk of compromise to the content that's in copyright" was an area of vulnerability for repositories. For this interviewee, the threat of providing inappropriate access to materials with copyright restrictions was a potential legal threat to a repository. He went on to argue that access in general is an area of risk for repositories, and that the push to provide repository users with meaningful ways to access and interact with data can interfere with the core mission of preservation by pulling resources away from that work, "I think access in general is complicated and getting more complicated."

Repository Staff 01, 02, 05, and 06 all described copyright as a potential source of risk for digital repositories. For example, intellectual property rights were described as a "ticking time bomb" by Repository Staff 02, who explained that repository cost models were complex sources of potential risk for repositories, "The way that national copyright factors into the cost model, which is two-dimensional and I think very complicated, but it probably needs to be multidimensional more than that because of copyright issues." Despite this concern, he felt that the auditors who assessed his repository had an inflated sense of the threat that copyright issues posed to his repository. He said that he disagreed with their "sense of risk" with regard to in-copyright materials, but "didn't feel it was worthy of dispute" in the final TRAC audit report.

While standard developers, auditors, and repository staff all found legal issues, such as contracts, agreements, licenses, and copyright, to be potential sources of risk for digital repositories, the groups focused on different types of legal risk (inter-organizational agreements versus copyright) and different foci of risk (repository versus digital content). Standard developers and auditors focused on relationships among partner and/or member organizations, and argued that those relationships were a potential threat to both repositories and digital content, and that agreements were necessary in order to ensure and enforce a commitment to the mission of long-term digital preservation. Repository staff, on the other hand, focused primarily on intellectual property issues and the threat that violating copyright posed to their repositories. They also spoke about the complexity of the legal agreements governing relationships among partner and/or member institutions and expressed some skepticism about whether an external party would be able to understand the legal landscape of their repositories.

With regard to legal risks, repository staff were focused on TRAC certification as a marker of whether a specific repository could be considered a trustworthy home for digital content, while standard developers and auditors focused on certification as a marker of how likely it was that digital content could outlive the repository itself.

Organizational governance

Interviewees described organizational instability as a potential source of risk for digital repositories and discussed the ways in which internal governance structures and the positioning of the repository within larger organizations (e.g., universities, consortia, partnerships, etc.) were possible threats to both a repository and its digital content. While standard developers emphasized the ways in which the requirements laid out in the TRAC standard would mitigate potential threats to organizational stability, auditors and repository staff members were skeptical whether policies and documentation were meaningful as risk mitigation tactics. There was additional disagreement between auditors and repository staff concerning the efficacy of mission statements and policies. Repository staff members cited TRAC-certified organizations without clear mission statements and where staff members lacked a clear understanding of the overall mission of long-term preservation.

Section 3 of the TRAC standard focuses on organizational infrastructure and includes several subsections that specifically target governance, including Section 3.1 “Governance and Organizational Viability” and Section 3.2 “Organizational Structure and Staffing” (Consultative Committee for Space Data Systems 2012b). The Governance and Organizational Viability section specifies that a trustworthy repository should have a mission statement that reflects a commitment to digital preservation, as well as a strategic plan, a succession plan, and a collection policy that all reflect the mission of long-term preservation. The Organizational Structure and Staffing section also focuses on the need for appropriate staffing, position descriptions, and ongoing professional development to carry out the mission of long-term preservation. The standard developers’ view of organizational infrastructure and governance as a potential source of risk for digital repositories reflects a view of digital repositories as organizations that are at risk of losing focus on long-term digital preservation either because of mission scope creep or because parent or partner organizations have goals that differ from the repository. In this sense, they articulated in the standard an expectation that repositories will need to defend their focus on long-term preservation and that repository staff members should all understand how their roles serve that mission.

Standard developers discussed three areas of organizational governance as potential sources of risk for digital repositories: (1) institutional support, (2) leadership changes, and (3) organizational structure. Loss of institutional support was described by several standard developers as a major threat to digital repositories. For example, Standard Developers 01, 02, 05, 06, 08, and 10 all emphasized the potential risk for repositories and digital content associated with loss of support for the mission of long-term digital preservation. Standard Developer 05 said that uncertainty about organizational structure and staffing was a potential source of risk for digital repositories, “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.” This attitude toward organizational infrastructure and the emphasis on appropriate staffing of people with expertise reflected the TRAC requirements.

TRAC auditors reinforced this conceptualization of governance as a source of risk for digital repositories, focusing primarily on institutional support, “the most important aspect of a repository is having an organizational commitment with a mission that aligns with the repository” (Auditor 06). Auditors 01, 03, 04, 05, 06, 07, 08, and 10 described governance and organizational stability issues as both complex and uncertain. When asked to discuss the most significant sources of uncertainty for digital repositories, Auditor 03 discussed the uncertainty of long-term institutional support:

> *"We don't know if libraries are going to survive. We don't know if universities are going to survive. These institutions that support the...repository, are also at risk...We've constructed this organizational structure that includes digital repositories... I don't know who's going to support it in 50 years. I don't know if it's still going to be a library or a university or it's going to be some crowd funded thing...so I think that is the biggest risk for almost everything that we're doing now is knowing what's going to happen to these institutions because a lot of things are at risk right now."*

Auditors expressed attitudes similar to the standard developers when discussing the importance of governance in a TRAC audit. Reflecting the requirement described in the standard that digital repositories should have explicit mission statements emphasizing long-term preservation, for example, auditors described ongoing organizational support for preservation as a challenge for repositories, "Bottom line is it's a tremendous amount of resources required to do long-term preservation. Organizational commitment to those types of resources often waxes and wanes" (Auditor 05). This auditor went on to say that he thought that the organizational infrastructure elements of the TRAC checklist were more aspirational than realistic because in practice repositories lack support for long-term preservation. Auditors described repositories as organizations with competing priorities who must continually fight for resources to support long-term digital preservation efforts, and whose parent and partner organizations may or may not share their commitment to preservation.

As with the standard developers and auditors, repository staff members described governance and organizational stability as potential sources of risk for digital repositories, "I feel like the funding, the organizational governance, all those things are inherently risky and problematic" (Repository Staff 02). Like the auditors, these interviewees questioned whether TRAC certification could assess the stability of repository governance over time, "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). Repository staff members described policies and practices at their organizations that were complex and continually evolving.

While all of the repository staff members described long-term preservation of digital content as important for their organizations, there was disagreement about whether this should be the central mission of the repository. One interviewee in particular reported that his repository did not have a mission statement, and that their long-term goals focused on meeting user needs, which happened to include providing long-term access to particular content that was of interest to their Designated Community. In the documentation that this repository provided to auditors, the goals of their preservation efforts were articulated in the description of their Designated Community as providing long-term access to specific digital content for that community, but these preservation efforts were not described as part of the repository's mission. When asked if there were any particular parts of the checklist or of the repository documentation that were particularly time-consuming to prepare, Repository Staff 18 described the workaround that his repository used to address the criteria in the standard without creating a mission statement for the repository that focused specifically on long-term preservation:

> *"One thing that was interestingly difficult to get was a sort of mission vision statement.... But it turns out we and a lot of other organizations don't have that existing in that form. Rather our mandate and our vision comes out of ... well, mandate comes out of the fact that the schools continue to pay money to us to exist. And our vision comes from our governance structure. So on some level you can say that our vision is to do what our community needs us to do. But that's not really useful in the context of the audit, so figuring out a way to answer those questions with our strategic plan, which we do have, took some time and some conversation."*

By questioning a central premise of TRAC certification and asserting that a repository need not have a mission statement reflecting a commitment to long-term preservation of digital content, the repository staff conceptualization of risk mitigation ran counter to that of the standard developers and auditors.

Overall auditors shared the standard developers' view of organizational instability as a potential source of risk for digital repositories. While the standard developers described, through interviews as well as in the text of the TRAC standard itself, strategies for repository staff to demonstrate that they had policies and procedures in place to mitigate this risk, the auditors took a more circumspect approach to verifying that repositories were mitigating this risk. They described institutional support for digital repositories as changeable and likely to decrease over time, and explained that it was easier for repositories to secure initial support for digital preservation than to maintain support. Auditor attitudes about governance as a potential source of risk questioned the notion that a one-time audit could assess whether a repository should be considered trustworthy in its ability to preserve digital content over the long-term. Auditors were enforcing requirements from the TRAC standard in order to certify a repository as trustworthy, but were also skeptical about whether long-term trustworthiness with regard to governance could be determined in this way.

While standard developers and auditors agreed that a clear mission statement supported by well-documented policies would offset potential threats to repositories and digital content by ensuring that the repository maintained a focus on the goal of long-term preservation, repository staff were skeptical about the effectiveness of this type of documentation to offset these potential threats. Indeed, repository staff members said that they were able to provide the necessary documentation to achieve certification despite the fact that their repositories lacked the governance structures that they knew the standard was meant to enforce. In the case of repository documentation such as a mission statement, the difference between standard developers and auditors on one hand, and repository staff on the other, was in part a difference in perspective of their functions. Unlike standard developers and auditors, repository staff did not see policies as necessarily reflecting actual repository practices. Repository staff characterized such policies as ideals, but also described their repositories as organizations that were shaped by power struggles and lacking in the social mechanisms needed to meet the ideals represented in their documentation.

Repository processes

Interviewees identified processes for digital object management as potential sources of risk for digital repositories and digital content. They discussed ways that metadata creation, file format management, and processes such as content ingest, threatened the longevity of digital content as well as the ability of digital repositories to carry out their mission of long-term preservation. Auditors tended to agree with the view of risk presented by standard developers, but repository staff members argued that the actual work of managing digital content over time was not as straightforward as the TRAC standard implied. Repository staff members described the section of the TRAC standard focusing on digital object management as the one that generated the most disagreement with auditors during their audits, although they were indeed able to sufficiently communicate their practices and policies, and the reasoning behind them to obtain certification.

Section 4 of the TRAC standard, "Digital Object Management," addresses repository processes as a potential source of risk (Consultative Committee for Space Data Systems, 2012b). Subsections covering ingest, preservation, management, and access of digital content make clear that potential threats exist throughout the entire lifecycle of a digital object, and suggest that repositories can demonstrate that they have sufficiently identified and addressed those threats through documentation such as policies and procedures, workflows, and curation logs. Thus, it is not surprising that standard developers discussed these repository processes (e.g., digital object management, such as ingest, transformations, capture/creation and management of metadata, and content delivery) as potential sources of risk for digital repositories and digital content. They described the goal of digital object management as "selecting and preserving the information in a way that will be useful … as part of the long-term preservation goal" (Standard Developer 01). This interviewee further explained that digital object management in the context of OAIS and TRAC was about more than "just managing digital formats," it was "concerned about preserving the information content, not just the format" (Standard Developer 01).

Metadata creation, capture, and maintenance were discussed by Standard Developers 01, 04, 08, and 09. They explained that it was important for repositories to understand their Designated Communities in order to know what type of representation information would be needed to preserve digital content for future use. In the words of Standard Developer 04, "The greatest risk is understanding what needs to be captured now so that the data can be understood in the future." When asked if there were any checklist criteria that repositories were commonly unprepared to provide evidence for, this interviewee went on to explain that lack of understanding about how important metadata are for long-term preservation was a threat to the long-term viability of digital content:

> *"[W]hat metadata they have, whether it's representational information or context information, which is necessary for the use of data, oftentimes was ignored." (Standard Developer 04)*

For developers of the TRAC standard, having sufficient, appropriate metadata was crucial for long-term preservation of digital content, and this emphasis on representation information was reinforced through the standard.

Another common theme among standard developers was the challenge that file formats posed to long-term preservation, "the more formats that you are taking in and using for your AIPs [archival information packages], the more complex that gets, the combinatorics when you start talking about multiple file formats, multiple record types, compound records, software dependence of the records" (Standard Developer 03). Standard Developers 03, 04, 06, and 08 all discussed potential threats relating to file formats, including obsolescence, difficulties in sufficiently documenting unusual file formats, and the lack the expertise, staffing, and funding to sustain the amount of work necessary to support a large number of different file formats within one repository. "I think most archives have preferred formats and then they have other formats that don't get the support that they need" (Standard Developer 08).

Standard Developers 04, 05, 07, 09, and 10 identified ingest, migration, and storage, as well as processes to verify the fixity or integrity of content as potential sources of risk, "The fixity or the integrity of the data is critical" (Standard Developer 04). Indeed, when asked to identify potential sources of risk in the digital object management section of the vignette, Standard Developer 05 explained that a number of factors during the ingest process that could negatively impact the repository and/or the longevity of the digital content:

> *"You have to maintain, as much as possible, the control of what is going to be transformed. Some properties [have] to be transformed. And of course in this case you can accept the transformation. You must accept. Because the digital preservation is dynamic. Formats change, digital signatures cannot be verified. So you have to build a documentation system able to document which kind of transformations have been done, on which basis. Because many of [these] transformation[s] are not reversible. They are forever. You have change and you are going to lose the original things and what was."*

The standard developers presented a view of repository processes for digital object management as one that required substantial documentation in order to ensure that future custodians and users of digital content would be able to access and understand that content. While standard developers focused on the potential threat to digital content posed by repository staff failing to understand what information to capture, create, and maintain, I found that auditors were more concerned that even when repository staff knew what policies and practices they should have, repositories lacked the staffing, expertise, funding, or organizational will to carry out that work.

Auditors described the work of digital object management as something that takes place across different functional areas of a repository, and explained that coordinating and managing this work was difficult. "In terms of the actual getting the work done from ingest to storage to metadata to access and all that, those functions can be spread all across the organization, whatever kind of organization they are. 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). Auditors 05 and 06 argued that repository processes for digital object management were a potential source of risk because of the likelihood that they would be abandoned or scaled back over time, "They start off with the goal of having defined processes, workflows, and all that sort of stuff, and over time a lot of that stuff gets either dropped or the period between things like migration activities or even just repository auditing activities expands as the organizations are pressed for resources and staff" (Auditor 05). Auditor 06 referred to these processes as "a series of handoffs…That you have to continually be touching, and curating, and evaluating content and digital collections or else they really will just die."

In terms of errors that could occur in these processes, auditors argued that the stakes were high for repositories that focused on long-term preservation because of the likelihood that errors would go unnoticed for very long periods of time. For example, Auditor 09 identified human error as the greatest threat to digital repositories, "I think human failure, or failure in human-driven processes, which include a lot of technical processes. I mean, technical processes are only as good as the humans that develop them."

Overall, auditors understood the view of risk provided by standard developers through the TRAC standard, and agreed that repository processes for digital object management were a potential source of risk for digital repositories and the content. Yet, auditors were more focused on how lack of human resources and human error or loss of resources would impact a repository's ability to carry out the processes necessary for long-term preservation, while standard developers were concerned about whether repositories would understand the needs of their Designated Communities well enough to capture appropriate representation information for preservation and reuse, and whether their workflows and procedures were comprehensive enough to capture all of the actions applied to their collections over time. Standard developers assumed that addressing this potential source of risk was a matter of having enough information and technical knowledge about digital object management, while auditors questioned whether that information was knowable and argued that it would not be possible over the short term to assess whether a repository's digital object management processes were successful.

As with the standard developers and auditors, repository staff members also focused on metadata, file formats, and repository processes for digital object management as potential sources of risk for digital repositories. Repository staff identified metadata as an area that could pose a potential threat to both the repository and the digital content. Repository Staff 03 explained that poor metadata management practices could negatively impact the usefulness of a repository for its users, "The devil's in the details. You can maintain preservation metadata and do it well. Or you could do it poorly. And so risks, I guess, implicit there are if it's not normalized, if it's not taking advantage of controlled vocabularies or authority, things like that, then the quality of the preservation metadata, if it's poor, could present a risk to the usefulness of the repository." In addition to maintaining metadata over time, Repository Staff 07 emphasized that metadata objects change over time and it is important for repositories to keep pace with the changes to digital objects and their metadata in order to preserve digital content: “In terms of the actual content itself what we’re finding is that it all changes, and in particular the metadata about objects changes a lot more than the underlying objects themselves. Both in terms of being enriched and enhanced over time, but also in terms of just being corrected.” Repository staff agreed with the standard developers that the work of maintaining file formats over time could pose a potential risk to repositories because of the amount of time and resources required.

However, repository staff disagreed that file format obsolescence or lack of expertise would be a problem for repositories. They argued instead that as long as there was sufficient interest and knowledge in the repository or its Designated Community they would be able to make sense of the digital content. For example, Repository Staff 04 pointed to current successes with outdated formats as an example, “You know, we’ve worried a lot in the preservation community about Word Perfect is gone. We can’t read WordPerfect anymore or these weird file formats are gone and it’s actually never been the case. We’ve never not been able to figure out what we’ve got, as long as we’ve still got it.”

Repository Staff 08, 12, and 15 spoke at length about processes to ingest content as costly and time-consuming. “Ingest of content is the most expensive piece, and it is where almost all the resources are spent. And unfortunately,…the content that is most at risk is the most expensive to ingest” (Repository Staff 12). Similarly, Repository Staff 08 stated it was costly to ingest digital content in a way that would support her repository’s mission of long-term preservation, “More often, however, the data would come to [repository] that had not been very rigorously produced or managed, and so it was expensive and time-consuming for us to process it in a way that allowed us to be confident of our preservation commitment.”

Repository staff painted a picture of digital object management processes as ongoing, time-consuming activities that required regular actions with no guarantee of long-term success. Repository Staff 07 explained that digital content requires regular attention in order to ensure the integrity of each item and make it usable for the Designated Community, “There’s so many items that can simply become obsolete as well as physically degrade and long-term digital preservation requires handling the data on a regular basis, so that you actually are continually testing your assumptions that it’s not only still there but still usable and fit for a particular purpose.” On the other hand, Repository Staff 11 argued that in practice digital object management processes required making compromises in order to balance this with other repository priorities, “One of the interesting things about being a preservation organization is that on the one hand you often have very high lofty ideals, but you have to balance that. There’s a risk to meeting them. You have to balance that with the practical decisions.”

These attitudes were in contrast to the attitudes expressed by standard developers and auditors, that it was difficult for repository staff to meet the criteria set forth in the TRAC standard for digital object management, and that the discrepancy between the ideal and what repositories was likely to be able to accomplish presented a potential threat to repositories and content. Repository Staff 07 explained that this was an area of risk because best practices for managing digital objects for long-term preservation have yet to be established, “It quickly gets mind numbingly complex and [we] have not come to any really good future-proof answers that we're comfortable with in terms of identifying objects uniquely, and perpetually, and persistently."

This disagreement between repository staff and standard developers, and auditors about whether meeting the criteria described in the standard would ensure the longevity of digital content surfaced during the audit of Repository Staff 04's organization, "there were a lot of revisions we had to do in our technical section because of that. I don't mean this as an insult, but they wanted clean, formulaic answers, and there just weren't any." He emphasized that the auditors, following the TRAC standard, wanted his repository to provide clear responses to the criteria in Section 4, but the actual work of managing digital objects was complicated and messy. Indeed, several repository staff members identified this area as one where they disagreed with auditors, or where auditors required a substantial amount of additional information before they would agree to certify the repository.

Standard developers, auditors, and repository staff members all described processes for digital object management as a potential source of risk for repositories. While standard developers and auditors characterized digital object management as relatively straightforward and held that clear documentation of digital object management processes would mitigate risks in this area, repository staff argued that the actual work of managing digital content over time was not as straightforward as the TRAC standard implies. This was the section of the TRAC standard that repository staff reported as the most contentious during the audit process, because auditors wanted clear documentation communicating repository processes, and repository staff members viewed their processes for digital object management as complex and difficult to communicate via documentation in the way that the audit process demanded.

Technical infrastructure

Interviewees identified threats to the technical infrastructure of digital repositories as a potential source of risk. Standard developers and auditors both viewed threats to technical infrastructure as identifiable and manageable, and argued that repositories that engaged in the environmental monitoring required by the TRAC standard would be able to understand and respond to these threats. While some repository staff members agreed with this perspective, others questioned whether their repositories would be able to identify actual threats, and thought that even if they did identify them they might not have the resources to respond.

Among standard developers, threats to the technological infrastructure of repositories were described as a significant but manageable source of risk for repositories and their content. These interviewees identified aging hardware and software, costliness of maintenance, and the ongoing work required to sustain trustworthy infrastructure over time as potential sources of risk and posed straightforward solutions, such as equipment replacement, software upgrades, content migration, and up-front investment in infrastructure.

Standard developers argued that the technical infrastructure of a repository was both complex and continually evolving as new digital preservation solutions emerged. "The already complex world of hardware and software platforms. The concept of the virtual computer has not proved to be very successful yet. We're stuck right now in, really, taking baby steps in terms of our hardware and our software approaches to digital preservation. We've got to get some kind of more universal, more virtual approach, to how we can preserve all formats of digital materials" (Standard Developer 06). This complexity, they explained, required continual monitoring in order to keep abreast of changes in the environment. "For example, one of the areas of the audit and certification standard is concerned with regular monitoring of changes in the environment, and that's complex because it can mean hardware obsolescence" (Standard Developer 09).

Section 5, "Infrastructure and Security Risk Management" of the TRAC standard echoes this belief in the importance of ongoing monitoring in order to maintain up-to-date hardware and software and cites the importance of tracking "when hardware or software components will become obsolete and migration is needed to new infrastructure" (Consultative Committee for Space Data Systems, 2012, p. 65). Through this document, the standard developers frame threats to technical infrastructure as identifiable, often predictable, and as something that can be addressed before it becomes a problem.

While standard developers framed threats to technical infrastructure as manageable, they did point out that people were one of the biggest challenges in mitigating these threats, "The difficulty is always people. The hardware and software is always going to be much easier" (Standard Developer 07). For example, while it might be relatively simple to set a timeframe for hardware replacement, it may be difficult to secure the necessary funding to follow that replacement schedule, "You can't tell a resource allocator … that you're going to basically wipe out everything and replace it all in three years. That what is brand new and spiffy and perfect now will all be gone in three years because it will be inadequate. Resource allocators don't like to hear that" (Standard Developer 06).

In contrast, when asked what he considered to be the greatest risk or threat that digital repositories face, another standard developer argued that the cost of storage decreases exponentially over time, and that securing funding for long-term preservation was more about the ongoing work of digital object management rather than infrastructure:

> *"So whereas initially [a] petabyte may be on one or two, maybe it's two tapes, in three years time it'll be on a small part of one tape. In another three years, it'll be on a tiny part of one tape, and in another three years it'll be next to nothing on a tape, and so the management of it will be negligible from then on because it's just this much of a tape and that's nothing in terms of the cost of the tape and the processing to check these things. So all of that is significant in terms of the costs, so then the costs come to actually making sure the data is usable." (Standard Developer 07)*

Standard developers framed threats to the technical infrastructure as ongoing and manageable. They articulated a view of long-term preservation in which digital content is expected to survive but the technologies used to store, preserve, and access it are not. Through the text of the TRAC standard, they communicated to both auditors and repository staff that a TDR should be able to demonstrate a firm understanding of the limitations of its infrastructure, and an ability to preserve digital content beyond the lifespan of any given part of that infrastructure.

Auditors agreed with standard developers about the importance of technical infrastructure and the notion that threats were significant but manageable for digital repositories, "A technical infrastructure is not difficult. It may cost you a bunch of money, but it's a solvable problem and you kind of assume it's robust given that there are processes and checks and all sort of things in place to verify that it's robust" (Auditor 09). The expectation that money could solve problems relating to technical infrastructure was shared by several auditors, "Everything else from a, comes down to the challenge of technological change, but a lot of the technological change can be mitigated with sufficient resources" (Auditor 05). Similarly, auditors argued that in addition to having sufficient resources, having appropriate staffing with the right kinds of expertise was also important for mitigating threats to the technical infrastructure of a repository, "The biggest thing I learned is that the human factors are more important than the technology factors. Because the technology factors, as long as you have good people and support for the technology, you can do that" (Auditor 08). Auditor 08 went on to explain that both the hardware and software of a repository require specialized knowledge and expertise, but that in general technologies for digital repositories are well known.

Implicit in this perspective is the assumption that with enough resources and the right kind of expertise, potential sources of risk to a repository's technical infrastructure can be ameliorated. In the context of a TRAC audit, one auditor explained that an important goal of the site visit is to inspect the physical infrastructure, including equipment, software, and facilities in order to confirm that the documentation provided by repository staff accurately represents the repository, "You're there to gather evidence of facts, so yes, there is a data center and its doors are locked and under alarm. There is earthquake monitoring. So you know, one responsibility was to see things, okay? And I think that's really important. 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).

Overall, auditors agreed with the view communicated by standard developers that although threats to the technical infrastructure of a repository were serious, they were also knowable and manageable. Both standard developers and auditors developed a view of potential sources of risk in this area as issues that repositories seeking TRAC certification should be able to identify and mitigate. While repository staff members agreed with standard developers and auditors that threats to technical infrastructure were potential sources of risk for digital repositories, repository staff expressed mixed attitudes about the manageability of those threats. Some repository staff members agreed with the view of technical infrastructure as a potential source of risk that was manageable while others argued that technical issues could not be separated from other aspects of repository management, such as funding and staffing, and that problems in those areas had the potential to make threats to technical infrastructure intractable.

Several repository staff members described examples from their own experience in which staffing issues compounded potential sources of risk relating to the technical infrastructure. For example, one interviewee explained that staffing issues, including turnover, created instances where repository software was not understood by repository staff. "[We have] various generations of software and they've been developed by different people. We're not a huge organization, obviously, so it's not that big a deal, but we certainly have pieces of software that people are like, I have no idea what that is. Or, I know what that is, but I didn't write it. So I think that's really where most of our complexity lies" (Repository Staff 04). The stakes of not understanding repository software can be particularly high in instances where repository staff think that they understand their infrastructure and fail to catch problems until it is too late, "So that's a vulnerability. Especially software. You think it's doing one thing. Everybody thinks it's doing one thing, and then you find out if it's doing something else, and then maybe it's too late" (Repository Staff 05). When asked how his role and experience influenced his understanding of the risks that his repository faced at the time of their audit Repository Staff 03, an IT manager, described his approach to managing technical infrastructure as being driven by a desire to prevent the repository from being affected by a failure:

> *"As far as the technical infrastructure too, I never wanted us to be impacted by failures. I never wanted to say, 'We had some sort of system failure but, we think everything's okay.' Or 'Service was down for this time because of some unplanned thing that we didn't understand.' I really tried to keep everything to a high bar in terms of those kinds of technical considerations. Redundancy for all of the – Also, I didn't want to respond to crisis. I didn't want my staff to have to respond to crises. You know?"*

In addition to questioning whether breakdowns in technical infrastructure would be identified, repository staff also argued that repositories could not assume that they would always have the staffing levels to support their infrastructure and respond to potential threats, "We have three now. But we're still doing the work that we did when we were seven. So there's things that are not happening that I wish were happening. You know, even on a systems side" (Repository Staff 16).

Interviewees largely identified threats to the technical infrastructure of repositories as a potential source of risk that was straightforward and within the power of repository staff to address. While repository staff shared the understanding of this potential source of risk as communicated through the TRAC standard, they disagreed about whether responding to threats in this area would be as clear-cut for their repositories as the standard developers and auditors assumed it would be. While some repository staff members agreed with standard developers and auditors in their characterization of technical infrastructure as manageable, other repository staff members argued that other areas of repository management such as funding and staffing would prevent their repository from maintaining the level of expertise needed to identify and mitigate threats to their technical infrastructure.

Discussion

Risk is a foundational concept in digital preservation and the TRAC audit process (Consultative Committee for Space Data Systems 2012b; Conway 1996). In this article I have characterized the classical definition of risk as one that included two elements that were common throughout the literature: (1) the probability, and (2) the magnitude of consequences of an event (e.g., Gardoni & Murphy 2013; Hilgartner 1992; Kaplan & Garrick 1981; Leveson et al. 2009; Rowe 1977; Slovic 1987). This understanding of risk relies upon the concept of a rational actor and assumes that different individuals will understand risk in a similar manner and respond to risk information in predictable ways. In this study, I found that the TRAC standard developers assumed that auditors and repository staff would interpret the TRAC standard in the same way, and that both groups would understand the risks facing a repository in a consistent manner and agree on mitigation strategies and actions.

Standard developers, auditors, and repository staff discussed the concept of risk in ways that demonstrated an understanding that reflected this classical definition. Yet, the results of this research have shown that this understanding of risk was not reflected in their experiences. Instead, I found that individuals across those three groups did not share the same understanding of risk and did not agree about the risk mitigation strategies that were required for TRAC certification.

While standard developers, auditors, and repository staff tended to agree on the major categories of potential risk for digital repositories (i.e., finance, legal, organizational governance, legal, repository processes, and technical infrastructure), repository staff often held different perspectives than the standard developers and auditors about whether the audit process could accurately assess their ability to mitigate those risks and ensure the long-term preservation of digital content. For example, repository staff, with their varied educational and professional experiences, tended to be less senior than the standard developers or auditors, and were more likely to be in professional roles where they were directly carrying out the work of preserving digital content. They expressed greater skepticism about the effectiveness of succession plans as mitigation tools for financial risk and their discussion about this topic tended to focus on the immediacy of the threat to their organization, their role, and the digital content that they were preserving.

My findings indicate that digital repositories can meet the requirements from the TRAC standard without the repository staff believing that those requirements will, in fact, ensure the longevity of their digital content. Standard developers and auditors agreed about the types of evidence that would demonstrate trustworthiness with regard to long-term preservation for digital repositories, but repository staff members disagreed about whether documentation, such as a succession plan, was in fact evidence of repository trustworthiness.

The OAIS and TRAC standard developers, a group consisting largely of individuals with graduate degrees in highly technical fields, such as physics and engineering, established guidelines for repository certification that assumed identifying risks and describing policies and processes to address them could demonstrate a repository's ability to preserve digital content for the long-term. This approach to risk typified the shared epistemic culture among standard developers that emphasized discoverable, calculable phenomena rather than socially constructed phenomena and assumed that different people would behave rationally and predictably when presented with risk information. Similarly, the auditors enforced this understanding of how to determine repository trustworthiness. Their acceptance of the requirements set forth in the TRAC standard, and the underlying assumptions about risk identification and policy documents as sufficient evidence of repository trustworthiness, reflects the culture and expectations of this group of academic library administrators with library and information science backgrounds.

In contrast, repository staff members did not believe that documentation about repository missions, policies, and processes was evidence of trustworthiness with regard to long-term preservation of digital content. The majority of the repository staff members had master's degrees in library and information science, a few had a bachelor's degree, one had a Ph.D., and one had completed some coursework but did not have a college degree. This group included people in a range of professional roles within their repositories. Repository staff questioned (1) whether documentation would translate into action, and (2) if it did, whether those actions would produce consistent results. Repository staff, responsible for enacting the policies and processes described in TRAC documentation, did not believe that documentation was evidence of a repository's ability to preserve digital content long-term. They saw it as performative rather than demonstrative of trustworthiness.

In the future, repository staff should consider what measures, and corollary evidence, they think would increase their perception of the trustworthiness of their repository with regard to long-term digital preservation and whether/how those measures complement or conflict with the accepted best practices for digital preservation and repository management. Rather than proceeding with certification under an evidential regime in a standard that they disagree with, the results of this research suggest that repository staff should take a more active part in the development of the standards themselves and that standard developers and auditors would benefit from including the perspectives of this group, which have so far been missing from the conversation.

Conclusion

In this qualitative study of TDR certification, I found that standard developers, auditors, and repository staff members identified risk in the TRAC audit and certification process in terms of specific potential threats or sources of risk, which I have organized into five main categories: finance, legal, organizational governance, repository processes, and technical infrastructure.

I have argued that although digital preservation has been examined as a technical, economic, and organizational phenomenon, it is also social. While the digital preservation community has regarded the concept of risk as a discoverable, calculable value, it is in fact socially constructed, and as such research that seeks to understand risk in digital preservation must consider the social context in which repositories exist and the ways in which social factors may influence how participants understand and behave in response to risk information.

My findings demonstrate that while standard developers, auditors, and repository staff generally shared an understanding of the major sources of potential risk that face digital repositories, they disagreed about whether and how these risks can be mitigated and how mitigation can be proved. Individuals who were more removed from the day-to-day work of the repositories undergoing an audit were more likely to accept well-documented risk identification and mitigation strategies as sufficient evidence of a repository's ability to preserve digital content long-term, while repository staff were skeptical that the documentation required for TRAC certification was sufficient evidence of risk assessment and mitigation and thus questioned whether it would translate to actual trustworthiness for long-term digital preservation.

Acknowledgements 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 their feedback and guidance on the development of this project. I would also like to thank Megh Marathe and Carl Haynes for their assistance with data analysis. This research was funded in part by a University of Michigan Rackham Graduate Student Research Grant.

Funding Open Access funding enabled and organized by Projekt DEAL.

Declarations

Conflict of interest The author has no conflicts of interest to report. Research materials, including the interview protocol and code set used for analysis, are available via Deep Blue, the institutional repository at the University of Michigan: http://hdl.handle.net/2027.42/147539.

References

About Chronopolis. (2021) UC San Diego: The Library. https://libraries.ucsd.edu/chronopolis/about/index.html. Accessed 5 May 2021

Barateiro J, Antune G, Freitas F, Borbinha J (2010) Designing digital preservation solutions: a risk management-based approach. Int J Digit Curation 5(1):4–17. https://doi.org/10.2218/ijdc.v5i1.140

Barateiro J, Antunes G, Borbinha J (2011) Long-term security of digital information: assessment through risk management and enterprise architecture. 2011 IEEE EUROCON-International Conference on Computer as a Tool (EUROCON), 1–4. https://doi.org/10.1109/EUROCON.2011.5929270

Beck U (1992) Risk society: towards a new modernity. Sage Publications

Becker C, Rauber A (2011) Decision criteria in digital preservation: what to measure and how. J Am Soc Inform Sci Technol 62(6):1009–1028. https://doi.org/10.1002/asi.21527

Berman F (2008) Got Data? A guide to data preservation in the information age. Commun ACM-Surv Data Deluge 51(12):50–56. https://doi.org/10.1145/1409360.1409376

Bernard H R (2012) Social research methods: qualitative and quantitative approaches. Sage Publications Incorporated

Burgess A (2015) Social construction of risk. In: Cho H, Reimer T, McComas K (eds) The sage handbook of risk communication. SAGE Publications, Thousand Oaks, CA, pp 56–68

Canadian Research Knowledge Network (2021) Heritage content. Canadian Research Knowledge Network. https://www.crkn-rcdr.ca/en/heritage-content

Canadiana.org (2015) About Canadiana.org | Canadiana. In: Canadiana.org. http://www.canadiana.ca/en/about. Accessed 30 Mar 2016

Center for Research Libraries (2010) CRL certification report on Portico audit findings. Center for Research Libraries. 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. 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. 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. http://www.crl.edu/sites/default/files/attachments/pages/ScholarsPortal_Report_2013_%C6%92.pdf

Center for Research Libraries (2014) CRL certification report on CLOCKSS audit findings. Center for Research Libraries. http://www.crl.edu/archiving-preservation/digital-archives/certification-and-assessment-digital-repositories/clockss-report

Center for Research Libraries (2015) CRL certification report on the Canadiana.org Digital Repository. Center for Research Libraries. https://www.crl.edu/sites/default/files/reports/CANADIANA_AUDIT%20REPORT_2015.pdf

Consultative Committee for Space Data Systems (2012a) Reference model for an Open Archival Information System (OAIS) (Magenta Book CCSDS 650.0-M-2). Consultative Committee for Space Data Systems

Consultative Committee for Space Data Systems (2012b) Space data and information transfer systems—audit and certification of trustworthy digital repositories (Standard ISO 16363:2012 (CCSDS 652-R-1)). Consultative Committee for Space Data Systems. http://www.iso.org/iso/catalogue_detail.htm?csnumber=56510

Conway P (1996) Preservation in the digital world. Commission on Preservation and Access

Dale R, Gore E (2010) Process models and the development of trustworthy digital repositories. Information Standards Quarterly 22(2):14. https://doi.org/10.3789/isqv22n2.2010.02

Dappert A, Farquhar A (2009) Modelling organizational preservation goals to guide digital preservation. Int J Digit Curation 4(2):119–134. https://doi.org/10.2218/ijdc.v4i2.102

Day M (2008) Toward distributed infrastructures for digital preservation: the roles of collaboration and trust. Int J Digit Curation 3(1):15–28. https://doi.org/10.2218/ijdc.v3i1.39

Dillo I, De Leeuw L (2018) CoreTrustSeal. Mitteilungen Der Vereinigung Österreichischer Bibliothekarinnen Und Bibliothekare, 71(1), 162. https://doi.org/10.31263/voebm.v71i1.1981

Frank RD (2020) The social construction of risk in digital preservation. J Assoc Inf Sci Technol 71(4):–484. https://doi.org/10.1002/asi.24247

Frank RD, Yakel E (2013) Disaster planning for digital repositories. Proc Am Soc Inf Sci Technol 50:1–10. https://doi.org/10.1002/meet.14505001058

Gardoni P, Murphy C (2013) A scale of risk. Risk Anal. https://doi.org/10.1111/risa.12150

Garrett J, Waters D J (1996) Preserving digital information: report of the Task Force on Archiving of Digital Information (9781887334501 1887334505; p. 68). The Commission on Preservation and Access & Research Libraries Group. https://www.clir.org/wp-content/uploads/sites/6/pub63watersgarrett.pdf

Gubrium JF, Holstein JA (2001) Handbook of interview research. SAGE Publications, Inc., Thousand Oaks

Hart PE, Liu Z (2003) Trust in the preservation of digital information. Commun ACM 46(6):93–97. https://doi.org/10.1145/777313.777319

Hilgartner S (1992) The Social Construction of Risk Objects. In: Short JF, Clarke L (eds) Organizations, Uncertainties, and Risk. Westview Press, Boulder, pp 39–53

Hughes R (2004) Vignette technique. In M. Lewis-Beck, A. Bryman, & T. F. Liao (eds), The SAGE Encyclopedia of social science research methods. (Vol. 1). SAGE Publications, Inc., Thousand Oaks, pp 1184–1184 http://sk.sagepub.com/reference/socialscience/n1078.xml, pp 1184–1184

International Organization for Standardization Technical Committee (2018) Risk management—guidelines (Standard ISO 31000:2018). International Organization for Standardization. https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:en

ITHAKA (2021) Why Portico. Portico. https://www.portico.org/why-portico/. Accessed 5 May 2021

Jantz R, Giarlo M (2007) Digital archiving and preservation: technologies and processes for a trusted repository. J Arch Organ 4(1–2):193–213. https://doi.org/10.1300/J201v04n01_10

Kaplan S, Garrick BJ (1981) On the quantitative definition of risk. Risk Anal 1(1):11–27. https://doi.org/10.1111/j.1539-6924.1981.tb01350.x

Lachlan KA, Burke J, Spence PR, Griffin D (2009) Risk perceptions, race, and Hurricane Katrina. Howard J Commun 20(3):295–309. https://doi.org/10.1080/10646170903070035

Lazorchak B (2011, August 23) Digital preservation, digital curation, digital stewardship: what's in (some) names? The Signal: Digital Preservation. http://blogs.loc.gov/digitalpreservation/2011/08/digital-preservation-digital-curation-digital-stewardship-what%E2%80%99s-in-some-names/

Leveson D, N, Marais K, Carroll J, (2009) Moving beyond normal accidents and high reliability organizations: a systems approach to safety in complex systems. Organ Stud 30(2–3):227–249. https://doi.org/10.1177/0170840608101478

McHugh A, Ross S, Innocenti P, Ruusalepp R, Hoffman H (2008) Bringing self-assessment home: repository profiling and key lines of enquiry within DRAMBORA. Int J Digital Curation 3(2):130–142. https://doi.org/10.2218/ijdc.v3i2.64

National Science Foundation (2011) Grant proposal guide (NSF 11–1). National Science Foundation. http://www.nsf.gov/pubs/policydocs/pappguide/nsf11001/gpg_index.jsp

Nelkin D (1989) Communicating technological risk: the social construction of risk perception. Annu Rev Public Health 10(1):95–113. https://doi.org/10.1146/annurev.pu.10.050189.000523

Nickel PJ, Vaesen K (2012) Risk and Trust. In: Roeser S, Hillerbrand R, Sandin P, Peterson M (eds) Handbook of Risk Theory: Epistemology, Decision Theory, Ethics, and Social Implications of Risk. Springer Netherlands, Dordrecht, pp 857–876, https://doi.org/10.1007/978-94-007-1433-5_34

Ontario Council of University Libraries (2021) Scholars Portal homepage. Scholars Portal. https://scholarsportal.info/. Accessed 5 May 2021

Porsdam Mann S, Donders Y, Mitchell C, Bradley VJ, Chou MF, Mann M, Church G, Porsdam H (2018) Opinion: advocating for science progress as a human right. Proc Natl Acad Sci 115(43):10820–10823. https://doi.org/10.1073/pnas.1816320115

Prior L (2003) Chapter one: Basic themes: use, production and content. In Using documents in social research (pp. 1–29) SAGE

Renn, O (2008) White paper on risk governance: Toward an integrative framework. In O. Renn & K. D. Walker (Eds.), *Global Risk Governance: Concept and Practice Using the IRGC Framework*. Springer, Netherlands. https://doi.org/10.1007/978-1-4020-6799-0_1, pp. 3–73

RLG-NARA Digital Repository Certification Task Force (2007) Trustworthy repositories audit & certification: criteria and checklist, Version 1.0. http://www.crl.edu/sites/default/files/attachments/pages/trac_0.pdf

RLG-OCLC Working Group on Digital Archive Attributes (2002) Trusted digital repositories: attributes and responsibilities. Research Libraries Group (RLG). https://www.oclc.org/content/dam/research/activities/trustedrep/repositories.pdf

Ross, & McHugh A, (2006) The role of evidence in establishing trust in repositories. D-Lib Magazine. https://doi.org/10.1045/july2006-ross

Rowe WD (1977) An anatomy of risk. Wiley

Royal Society (Great Britain) & Study Group on Risk (1983) Risk assessment: report of a Royal Society Study Group. Royal Society

Saffady W (2020) Managing information risks: threats, vulnerabilities, and responses. Rowman & Littlefield

Scott WA (1955) Reliability of content analysis: the case of nominal scale coding. Public Opin Q 19(3):321. https://doi.org/10.1086/266577

Slovic P (1987) Perception of risk. Science 236(4799):280–285. https://doi.org/10.1126/science.3563507

Smith Rumsey A (2016) When we are no more: how digital memory is shaping our future (Kindle Edition). Bloomsbury Press

Strodl S, Becker C, Neumayer R, Rauber (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, 29–38. https://doi.org/10.1145/1255175.1255181

Sudman S, Bradburn N M, Schwarz N (1996) Thinking about answers: the application of cognitive processes to survey methodology. Jossey-Bass Publishers

The National Science Foundation (2021a) National Science Foundation FY 2020 performance and financial highlights. The National Science Foundation. https://www.nsf.gov/pubs/2021/nsf21003/nsf21003.pdf

The National Science Foundation (2021b) United States National Science Foundation FY 2020 agency financial report. The National Science Foundation. https://www.nsf.gov/pubs/2021/nsf21002/pdf/nsf21002.pdf

United Nations Office of the High Commissioner (1966) International covenant on economic, social and cultural rights. https://www.ohchr.org/Documents/ProfessionalInterest/cescr.pdf

van Est R, Walhout B, 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 Netherlands, Dordrecht, pp 1067–1091, https://doi.org/10.1007/978-94-007-1433-5_43

Vermaaten S, Lavoie B, Caplan P (2012) Identifying threats to successful digital preservation: the SPOT model for risk assessment. D-Lib Magazine. https://doi.org/10.1045/september2012-vermaaten

Welcome to HathiTrust! (n.d.). HathiTrust Digital Library. https://www.hathitrust.org/about. Accessed 5 May 2021

Why CLOCKSS? (2021) CLOCKSS. https://clockss.org/about/. Accessed 5 May 2021

Wildavsky A, Dake K (1990) Theories of risk perception: who fears what and why? Daedalus 119(4):41–60

Yakel E (2007) Digital curation. OCLC Syst Services: Int Digital Library Perspect 23(4):335–340. https://doi.org/10.1108/10650750710831466

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Rebecca D. Frank Ph.D. is an Assistant Professor at the Berlin School of Library and Information Science at Humboldt-Universität zu Berlin, and the Einstein Center Digital Future (ECDF). Her research examines the social construction of risk in trustworthy digital repository audit and certification. She also conducts research in the areas of digital preservation, digital curation, data reuse, and open data, focusing on social and ethical barriers that limit or prevent the preservation, sharing, and reuse of digital information. She has a Ph.D. from the University of Michigan School of Information, an MSI from the University of Michigan School of Information with a specialization in Preservation of Information, and a BA in Organizational Studies from the University of Michigan. Her work has been supported by the National Science Foundation in the United States and the Australian Academy of Science.