



2023

Audit Team Communication and Risk in Trustworthy Digital Repository Certification

Rebecca D. Frank

University of Tennessee, Knoxville, rfrank7@utk.edu

Jessica Wylie

University of Tennessee, Knoxville, jwylie6@vols.utk.edu

Follow this and additional works at: https://trace.tennessee.edu/utk_infosciepubs



Part of the [Library and Information Science Commons](#)

Recommended Citation

Frank, Rebecca D. and Wylie, Jessica, "Audit Team Communication and Risk in Trustworthy Digital Repository Certification" (2023). *School of Information Sciences – Faculty Publications and Other Works*. https://trace.tennessee.edu/utk_infosciepubs/474

This Conference Proceeding is brought to you for free and open access by the School of Information Sciences at TRACE: Tennessee Research and Creative Exchange. It has been accepted for inclusion in School of Information Sciences – Faculty Publications and Other Works by an authorized administrator of TRACE: Tennessee Research and Creative Exchange. For more information, please contact trace@utk.edu.

Audit Team Communication and Risk in Trustworthy Digital Repository Certification

Frank, Rebecca D.

University of Tennessee, USA; Einstein Center
Digital Future, Germany | rfrank7@utk.edu

Wylie, Jessica

University of Tennessee, USA | jwylie6@vols.utk.edu

ABSTRACT

This paper aims to investigate the Trustworthy Repositories Audit & Certification (TRAC) process by examining the communication practices and risk communication dynamics among auditors during the audit. Through an in-depth, qualitative analysis of the audit process and the interactions between auditors, this paper provides valuable insights into the importance of diverse backgrounds, effective communication, and consensus building in the assessment of TRAC checklist requirements. Furthermore, the paper highlights potential areas of improvement within the audit process, addressing concerns related to disagreements, reliance on leadership, and the comprehensiveness of risk identification and communication.

KEYWORDS

Risk, Communication, Digital Preservation, Trustworthy Digital Repositories, Trustworthy Repositories Audit and Certification (ISO 16363).

INTRODUCTION

Much has been written about the essential role that digital repositories play in the curation and preservation of valuable information (e.g., Boyd, 2021; Kriesberg & Kowall, 2020; Thomer et al., 2022). Repositories carry out the vital work of preserving and providing access to a wide array of information, including research data, government information, and cultural heritage information. Processes have been established to evaluate whether the organizations entrusted with this uniquely valuable information are indeed up to the task (e.g., Consultative Committee for Space Data Systems, 2012a; CoreTrustSeal Standards and Certification Board, 2022; nestor Certification Working Group, 2013).

These processes evaluate whether repositories can be considered trustworthy for long-term preservation through a process of risk assessment that asks auditors to review and evaluate evidence submitted by repository staff members against a set of formal criteria (e.g., Consultative Committee for Space Data Systems, 2012a; CoreTrustSeal Standards and Certification Board, 2022; RLG-NARA Digital Repository Certification Task Force, 2007). When an audit process determines that a repository is indeed trustworthy in this regard, they are deemed a Trustworthy Digital Repository (TDR), and may receive certification confirming this status (e.g., Center for Research Libraries, 2010, 2011, 2012, 2013, 2014, 2015, 2018).

The Trustworthy Repositories Audit & Certification (TRAC) process is one such certification system (Center for Research Libraries, n.d.). In this system, auditors play a key role in interpreting the requirements and evaluating documentation of repository policies and practices against those requirements. Despite the central role that auditors play in this process, scholarship about TRAC and other TDR certification systems has not focused on this group.

In this paper we ask the following research questions about the auditors who were involved in conducting TRAC certification audits for the Center for Research Libraries (CRL):

1. In what ways do members of the audit team communicate during a TRAC audit?
2. How do their communication processes influence their perceptions of risk in the context of a TRAC audit?

Our findings indicate that diverse expertise and open communication using a variety of tools were essential elements of the TRAC certification process. Disagreements among audit team members were resolved through iterative discussions, allowing auditors to reach a consensus and achieve a shared understanding of the risks facing repositories in the context of the audit process. And finally, interviewees were confident in the accuracy of risk information communicated during an audit, but were aware that the process did not surface all of the risks facing the repositories that they reviewed.

LITERATURE REVIEW

Trustworthy Digital Repository Audit and Certification

Repositories can be certified as trustworthy for long-term digital preservation via several different systems, such as CoreTrustSeal, nestor, and TRAC (Center for Research Libraries, n.d.; CoreTrustSeal Standards and Certification Board, 2022; nestor Certification Working Group, 2013). All of these certification systems evaluate repositories against a set of criteria that are informed by the Open Archival Information System (OAIS) Model (Consultative

Committee for Space Data Systems, 2012b). In this paper, we focus on the TRAC certification process as administered by CRL (Center for Research Libraries, n.d.).

In 1994, the digital preservation community identified a need for trusted organizations to manage, curate, and preserve digital information, and called for a process to certify those organizations as trustworthy (Garrett & Waters, 1996; RLG-NARA Digital Repository Certification Task Force, 2007). The TRAC certification process was developed as a joint effort between CRL, the Research Libraries Group (RLG), the National Archives and Records Administration (NARA), and the Consultative Committee for Space Data Systems (CCSDS) (Yakel, 2007). The checklist for TRAC was published in 2007 (RLG-NARA Digital Repository Certification Task Force, 2007). The ISO 16363 standard formalizing repository certification criteria was approved in 2012, and the ISO 16919 standard creating a process of accreditation for auditors was approved in 2014 (Consultative Committee for Space Data Systems, 2012a, 2014).

CRL conducted TRAC audits between 2010 and 2015, and worked to update and maintain those certifications through at least 2018 (Center for Research Libraries, 2010, 2011, 2012, 2013, 2014, 2015, 2018). Subsequent certifications have been conducted by the Primary Trustworthy Digital Repository Authorisation Body (PTAB), the only group currently (as of April 2023) accredited to administer audits using the ISO 16363 standard (PTAB - Primary Trustworthy Digital Repository Authorisation Body Ltd., 2021).

Research about TDRs has been critical of various aspects of the certification process such as the Designated Community (e.g., Bettivia, 2016; Frank & Rothfritz, 2023; Moles, 2022), but overall has emphasized the importance of understanding the value proposition of certification (e.g., Donaldson & Russell, 2021). However, scholarship has not yet established whether TDRs are more effective at long-term preservation than other repositories, meaning that the primary goal of certification – to identify and label repositories as trustworthy for long-term preservation – remains an open question (Bak, 2016; Donaldson, 2020; Maemura et al., 2017). Despite these challenges, several benefits of TDR certification have been identified, including increased stakeholder confidence, transparency in documentation, and improvements in repository processes (Donaldson & Russell, 2023; Lindlar & Schwab, 2018).

Much of the literature about TDR certification has consisted of self-reports from organizations about their experiences with certification, both through formal audit processes and self-audits (e.g., CLOCKSS, 2014; Houghton, 2015; Kirchhoff et al., 2010; Krahmer et al., 2017). Literature also describes the work of groups who develop standards for TDR certifications (e.g., Dillo & De Leeuw, 2018; Giaretta et al., 2019; L'Hours et al., 2019). Missing from scholarship about TDR certification, and especially about TRAC certification, is empirical research that focuses on the experiences of the individuals and/or groups who carry out the work of the audit and make decisions about whether to award certification to repositories. Understanding their perspectives and experiences is essential for developing a well-rounded understanding of the audit and certification of TDRs.

Risk and Communication

Risk is fundamental to digital preservation (e.g., Barons et al., 2021; Conway, 1996; Vermaaten et al., 2012), and repository certification is largely an exercise in risk assessment (e.g., Frank, 2022). Research about TDR certification has tended to emphasize trust rather than risk (e.g., Bak, 2016; Berman et al., 2008; Donaldson & Conway, 2015; Dryden, 2011; Faundeen, 2017), a focus which emphasizes the goal of certification rather than the process or audit outcomes.

Communication influences the ways in which people construct their understanding of risk (e.g., Lachlan et al., 2009; Nelkin, 1989; Renn, 1991). Scholarship about risk communication has argued that perceptions of risk can be amplified or attenuated depending on factors such as the source, audience, and method of communication (Arvai, 2007; Kasperson & Kasperson, 1996; Lachlan et al., 2009). Communicating risk information requires an understanding of the audience (Konheim, 1988). Risk communication has been examined in the context of many different groups and types of actors, taking into consideration both the source and the recipient of information. For example, the involvement of media, government, political actors, scientists, and/or other types of experts can amplify or attenuate messages about risk (Arvai, 2007; Kasperson & Kasperson, 1996; Lachlan et al., 2009).

Different people, if presented with the same risk information, will not necessarily share the same perception of risk. In addition to the source and the audience, it is also important to consider the mode of delivery any time risk information is communicated (Arvai, 2007). For example, relevance of the information source to the recipient of the communication is an important factor influencing risk perception (Lachlan et al., 2009). The social amplification of risk, a theory about the "social experience of risk, behavioral responses, and secondary consequences relating to economic, legal, social, or institutional changes" argues that risk is a social construct and that hazards can interact with social processes to amplify risk and create secondary effects (Renn, 1991, p. 288).

Research has shown that formal risk assessment processes conducted by groups of experts do not necessarily address the questions or concerns that the general public (i.e., non-experts) have – when it comes to risk

information, the two groups are often talking past one another (Konheim, 1988). Indeed, Konheim (1988) argues that people tend to trust, for example, their neighbors, more than experts when it comes to risk assessments. This is relevant for TDR certification, a process in which the expert/non-expert dynamic emerges between stakeholder groups: standard developers and auditors, who are experts in the certification processes, and repository staff members, who are experts in the policies, procedures, and technologies used by their organizations. The expert/non-expert dynamic also emerges within each of these three groups. Members of the audit team during a TDR audit are selected for their particular knowledge and expertise in order to conduct the most thorough audit possible, but they do not have expertise in *all* aspects of repository management and thus are both experts and non-experts at the same time during their work as audit team members. Rather than TDR certification only being an example of experts communicating risk information about digital repositories to the public, it is also a process in which the stakeholders are both experts and non-experts and must communicate with one another in order to reach a consensus.

The process of TDR certification is one of risk identification and assessment. The goal of this process is for repository staff members to effectively communicate information to a team of auditors, who in turn evaluate that information and communicate their findings to the repository and the general public. Certification is a social process that has the potential to amplify risk information and create secondary effects in the context of digital preservation. Theories of risk perception that emphasize communication help us to understand that it is not only the identification of risk that influences digital preservation outcomes, but also the ways in which that information is communicated and received, and the actions that people take in response to this information.

In the context of a TRAC audit, an area in which communication about risks is particularly salient is the interactions among auditors who are evaluating repositories for certification. Auditors receive information from repository staff members, discuss and share additional information among themselves, and communicate information out to repositories and to broad audiences who may seek out the results of their audits. Communication about risk information between and among members of these different group may amplify or attenuate risks depending on the mode of communication, the way in which the risk message is communicated, and the relationship between the source and recipient of the message. This has the potential to influence the outcome of TDR audits, and also repository practices if staff members rely on and trust in the expertise of the auditors (e.g., Bostrom, 1997; Wynne, 1992). Professional discourse around digital preservation and TDRs may also influence perceptions of risk for different types of stakeholders depending on their connections to the digital preservation community, and the ways in which the communication norms of this community either match or diverge from the communication norms of their own professional communities.

RESEARCH METHODS

This qualitative paper is part of a research project which investigates the social construction risk in digital preservation, focusing on the TRAC audit and certification process. The study involved 42 interviews with standard developers (n = 11), auditors (n = 10), and repository staff members (n = 21). In this paper we draw upon the 10 interviews with auditors who administered TRAC audits via CRL.

Data Collection

In-depth, semi-structured interviews were conducted with developers of the ISO 16363 standard, members of the audit team from CRL, and staff members from TRAC certified repositories. At the time of data collection in 2016, there were six TRAC certified repositories, and all audits had been conducted by CRL, as shown below in Table 1 (Center for Research Libraries, 2010, 2011, 2012, 2013, 2014, 2015).

Repositories	Initial Certification Date	TRAC Score	Full or Partial Repository Certification	Repository Focus
Canadiana.org	2015	11	full	digital resources documenting Canada's national heritage
Chronopolis	2012	11	full	digital preservation network
CLOCKSS	2014 (updated in 2018)	14	partial	e-journals
HathiTrust	2011	9	full	digitized books
Portico	2010	11	full	e-journals
ScholarsPortal	2013	13	partial	shared digital information and collections

Table 1. TRAC Certified Repositories

Previous research has demonstrated that the work of digital preservation involves collaboration across three main functional areas: digital preservation, IT, and repository administration (Frank & Yakel, 2013). The auditors who were interviewed held professional roles in digital preservation (n = 4) and repository administration (n = 6). The audit team for TRAC audits consisted of official auditors, as well as an advisory board who reviewed documentation and prepared an assessment. For the purposes of this paper, members of both groups are referred to as auditors and/or audit team members, terms which are meant to encompass the range of individuals who were involved in reviewing and auditing repository documentation during the course of a TRAC audit for the six repositories in Table 1 above.

Interviews asked participants to reflect on their experiences with the TRAC certification process and to identify potential sources of risk for digital repositories. They lasted for one to two hours, depending on the role and experiences of the interviewee. All interviews were recorded and transcribed for analysis.

Data Analysis

Interview transcripts were coded in NVivo using a set of codes that included descriptive, analytic, and thematic codes. The code set addressed several themes, including: potential sources of risk for digital repositories, factors that influence the social construction of risk, the TRAC audit process, attitudes about TDR certification, and communication during the audit process. Coding began with a code set that was developed prior to analysis, and additional codes were added during the analysis process as needed. Transcripts were analyzed by a pair of coders working together to achieve an acceptable interrater reliability score. We achieved a Scott's pi of 0.719 for the subset of interviews with auditors (Craig, 1981; Scott, 1955). Additional analysis focusing on discussions about interaction among members of the audit team was conducted by a single researcher.

Limitations

In this research we encountered problems with memory and recall (Sudman et al., 1996). Interviewees were asked to recall details about events that took place anywhere from three to eight years in the past. As such, we sent copies of the audit reports ahead of the interviews and suggested that interviewees review their own records, calendars, communications, and documentation before, during, and after each interview. Due to the small population of this community, social desirability and expectancy effects were also likely present, as well as inaccuracy in self reporting and deference effects (Bernard, 2013).

FINDINGS

Our findings are organized into four sub-sections. First, we examine the audit process, the composition of the audit team, and modes of communication among auditors, including tools and platforms used during the audit process. Second, we examine communication processes during an audit, including communication among audit team members, and between the audit team and the staff members of repositories. Third, we explore how disagreements were managed among the audit team. And fourth, we end with an examination of risk communication among audit team members during a TRAC audit.

Audit Process, Team Composition, and Modes of Communication

Interviewees described an audit process in which repository staff members would prepare and submit documentation to meet the requirements in the TRAC checklist. The audit team would review the documentation, asking for additional information when necessary, which happened frequently:

“Always, 100%. I mean, if you ask how often, it always happens. And it’s a question of how much really. There are some repositories that do, have done a really stellar job. Like the [repository] people at [location]. [Full name of organization] did really a spectacular job of generating documentation and having it really very clearly written and addressing really all of the issues. But even in that case there were instances where we needed more information or explanation or something. So it’s always the case that there will be back and forth and the organization will need to add more documentation or better or new versions of documentation to better explain what is happening” (Auditor 06).

The extended audit team (i.e., audit panel members) would prepare recommendations for the auditors who would then conduct a site visit, investigating repository practices and confirming the accuracy of documentation. After the site visit, the full audit team would reconvene to prepare a final assessment and audit report: “It really depends on what kinds of responses we get from the self-audit and the documentation what we decide to look at at the site visit, but we need to confirm all the things that we had questions about and talk to the right people to help clarify other questions. Then we go back to the panel and talk to them about what we found, and then we come out with the report” (Auditor 03).

Interviewees discussed the importance of having a team of auditors with diverse knowledge and expertise, in order to ensure that all areas of the TRAC checklist could be assessed accurately. Several interviewees described

situations in which someone with a particular expertise was able to ask questions, or identify a gap in repository documentation, which resulted in a more responsible audit, “Yes, because everything is not black and white. You know, there’s some areas where you need to rely upon the group expertise, to do an analysis of a component of the metric. So it may be that someone is more familiar with something than somebody else, and they want to double check on something. Or if we want to double check to make sure that we’ve received all the documentation that one would like to have about a certain thing. So there’s a lot of backing each other up, and making sure that we’re right on target. And I think that makes it a more community-based and responsible effort, ‘cause it isn’t just one person coming in, and making a judgment call, exclusively, on their own” (Auditor 10).

The process described was one which required the contributions of multiple individuals with different types of expertise, communicating with one another around a set of documentation in order to evaluate repositories against a checklist of requirements. Multiple points in the process involved written and verbal communication among audit team members with different types of expertise, and the final result was one in which they needed to reach a consensus in order to determine the final outcome of each audit.

Interviewees described a variety of tools and methods that were used in the context of their work as audit team members to communicate with one another. The auditors used a mix of tools and platforms for communication and collaboration, including Google Docs, Excel, email, and various content management systems (CMS). These tools focused on document-centric collaboration, as the goal of the process for most of the audit team was to analyze repository documentation and write a report summarizing their assessment of that documentation.

While simplicity and accessibility were described as important, interviewees acknowledged challenges in finding a system that would work well for everyone. As a result, various communication methods were used, including both synchronous (e.g., group calls) and asynchronous (e.g., collaborative document editing, email, etc.) methods:

“If memory serves me, there were a lot of email ... They produced documents and the documents, we could comment on them. There was a CMS that CRL provided that we had to access, you logged into a member’s area and you could leave comments and that sort of thing. I kind of forget, a lot of organizations or a lot of, sorry, distributed groups at that time we were still using Microsoft Word and Excel. I say still, because they’re never really good at collaborative editing. You had to pass it around via email attachments or you had to upload it to a CMS. Google Docs became ascendant then. People realized that they could do real, real-time collaboration on documents. I recall lots of emails where we had discussions via email. We had regular, or not regular but a number of meetings, phone calls like teleconferences. And I do recall uploading documents to a CMS after we commented on them” (Auditor 09).

The general theme among interviewees was a pragmatic approach to collaborative tools that facilitated communication between audit team members without boxing them in to any one system or platform.

Communication Processes

We found that communication processes among audit team members were open, with regular synchronous and asynchronous interactions. In contrast, communication between auditors and the staff members of repositories under review were highly controlled, with one person managing all communications between the two groups.

Among Auditors

When discussing their experiences and interaction with one another, interviewees discussed the importance of communication and interaction to share knowledge across diverse areas of expertise. An open and supportive environment among auditors allowed them to ask questions and engage in collective decision-making. Most said that they were in regular communication through the process, and that this allowed them to divide tasks amongst themselves in order to distribute the workload and allow each auditor to contribute in areas relevant to their own expertise.

For each TRAC audit the team of auditors was broken down into smaller groups, depending on their areas of expertise. Different subgroups chose to communicate in different ways and with varying frequency. For example, Auditor 04 explained a process in which the team was in regular communication via email, with meetings as needed: “I don’t remember but it would seem like it would be monthly or every six weeks. Sometimes it depends on how quickly we get responses back from the repository as questions come up and we put them to the repository. Within the subgroups there is often just a steady low-level email conversation going on.”

In contrast, Auditor 06 described a process of regular conference calls, “during that process we generally break up into smaller groups and focus on a particular section of the three main sections of the audit. And meet via conference call, usually, to discuss issues or questions and then write up a summary report for the auditors and give it to them. And then there are regular calls of the whole group to discuss them.”

Auditor 08 said that the frequency of communication depended on the quality of documentation submitted by each repository, and the amount of additional documentation that auditors would need to request:

“We would have calls every couple months. Within a given audit, the work of that might in a really tight and well-constructed package, you may be able to wrap up the whole process in about six months from the time that you initially get their self-study. Other ones where there’s a lot more remediation that needs to be done, it can take at least a year. Depending on the strength of the initial self-study, it can just be a matter of dividing up roles. You typically would have two people look at each section who were not the core CRL team but other members of the audit team. I did most of my work in [section number]. The core CRL team would be knowledgeable in the entire package, so they would look at three, four and five and be conversing with all of that, but then they relied on that extended team to look specifically at the other three sections and ask questions from their perspectives to ... They tried to have both a mixture of administrative and technical folks as part of the team, so you try and bring together a spectrum of perspectives and experience because that adds to a richer conversation around those things.”

One interviewee, however, expressed uncertainty about the communication among the audit team. Auditor 09 explained that the process was opaque, and that he had the impression that decisions were being made behind the scenes which influenced her work but to which she was not privy:

“There were times when I distinctly recall that I thought there was a lot of things had gone on between communication cycles. I didn’t really think too much of it at the time, because I thought, we’re just giving our input. The people at CRL are, they’re actually doing the work of collecting all this information and putting it into their, kind of, their packages and their envelopes and templates. There were honestly, there were times and it may just have been an artifact of me having a busy schedule and not paying attention or something, but there were times when I felt like there was a lot of, there were side discussions going on that had shaped the questions that I was not being asked” (Auditor 09).

Interviewees described adaptable communication processes that varied depending on the conditions of each repository audit and on the preferences of the sub-groups within the audit team. Some interviewees spoke with confidence about these processes, while others found them to be opaque. The lack of standardization was helpful for a process that needed to adapt to the conditions of each individual audit. However, we argue that it also had the potential to be problematic in light of the fact that the certification process was meant to assess repositories based on a clear set of criteria in order to produce results that could be compared across audits.

Between Auditors and Repository Staff

A feature of the TRAC audit process is the limited interaction between members of the audit team and staff members from the repositories being audited, “The panel never really talks to the repository” (Auditor 03). Interviewees explained that communication with repository staff was typically channeled through a single point of contact in order to streamline the process and ensure consistency. This separation had the benefit of maintaining a degree of separation between auditors and the staff members of the repositories under review, as it was likely that members of the two groups would know – or at least be familiar with – one another: “No, I think we were over to the side. CRL dealt with them and us, even though these are people that I work with all the time, the staff at [repository], but we didn’t go to them directly, no” (Auditor 07).

Interviewees explained that the initial documentation provided by the repositories was not sufficiently clear or comprehensive enough for their needs, necessitating clarification and/or additional documentation. The additional back-and-forth required to meet this need was channeled through the single point of contact described above. While this simplified the process in some ways, limiting the number of requests that repository staff members would receive, it also created opportunities for miscommunication by having information travel across multiple people, like a game of telephone:

“[T]here’s usually some more back and forth because it invariably happens, they’ll mention something. I’ll remember it, and then I’ll be like, “Wait a minute. I need to see that. They talked about it, but I didn’t see it,” or something along those lines, so I need to do that sort of thing. Then sometimes, we’ll go back to the panel, and they’ll be like, “Wait a minute. What about this?” We’ll have to go back and talk to them about that. Then sometimes if there’s deficits or there’s something that needs to be fixed, there’s a lot of back and forth about that. If we found out that they didn’t have some sort of system for checking their files or something along those lines, we’d want to see them doing that before we could certify them, so there would be all of that hand holding, too” (Auditor 03).

Communication between auditors and repository staff members was channeled through one representative from each side of the audit process. This served to streamline communication and shield auditors from potential conflicts of interest although people with connections to the repositories, and/or staff members of those repositories, were still able to participate in the process. The streamlining did not always save time or make the process more efficient, however, because the specific people handling communication between the audit team and the repository staff did not necessarily have expertise in areas relevant to the discussion.

Managing Disagreements Among Auditors

Interviewees described instances of mild disagreement among members of the audit team. When disagreements would arise, they were addressed through iterative rounds of discussion and deliberation. Auditors would work together to resolve disagreements, reaching a shared understanding and consensus in order to ensure that the final result was one that they could all support.

In some cases, disagreements were resolved through discussion and negotiation: “There's certainly disagreement about, as we're discussing, as we move through each of the sections when talking about the individual items and the documentation provided by the organizations there are disagreements. There have been disagreements about, as we talk about any particular item, about the significance of how serious somebody felt a problem might be, or just a range of opinion about how to assess any particular item. But we talk through them and come to an agreement that's in the process. And I think that by the end of the process everybody agrees with, and is ready to sign off on, the assessment that CRL comes to” (Auditor 06).

In other cases, interviewees deferred to the opinions of CRL leadership in resolving disagreements. Auditor 08 explained that when the audit team had trouble resolving a disagreement, they would rely on the opinion of a particular high-ranking staff member at CRL, “When we had questions, we would defer to [name] at CRL, who was the most experienced person with all of this, with more than [number of years] of doing this kind of thing.” This practice seems to run counter to the design of the audit process, in which people were brought in to the team for their particular expertise in order to inform and advise CRL staff.

Auditors also recognized that there was a balance between seeking more information and the diminishing returns of excess detail. They were able to achieve consensus about how much information was needed to resolve disagreements, in order to assess each repository for TRAC certification. Auditor 08 explained that through the process, auditors came to see that there was a point at which more information did not necessarily help the team make a determination about the repository being evaluated, “You could always ask for more and more information, and at a certain point, the additive piece of what you get out of a certain piece of information becomes less and less” (Auditor 08).

Interviewees characterized disagreements as opportunities for communication amongst audit team members, and to request additional information from repository staff members. Some found that there were limits to how much conflict could be resolved with additional documentation. Others were over-reliant on the opinions of CRL leadership, a group of people who were themselves relying on the audit team members for their expert assessments.

Communicating Risk

Interviewees were confident that information about risks was communicated accurately among audit team members. When asked directly, Auditor 07 was unequivocally confident in the accuracy of risk information shared among audit team members, “Yeah, I felt confident in that, as well.” However, some were less confident that the process could surface *all* the relevant risks facing the repositories being audited: “I'm pretty confident about that because of the way those risks are shared, because of the report on the site visits that come up in discussions that follow. There's usually a conference call discussion that's part of the ... there's always a conference call discussion that's part of the process. The folks who are involved in the site visit are giving their perspective and addressing questions which spawn more questions. Through that I think all the risks identified come up. Obviously, have we identified all the risks? Probably not” (Auditor 04).

It was important for members of the audit team to have diverse backgrounds and different types of expertise, in order to inform all of the aspects of the TRAC requirements. Auditor 06 explained that in addition to needing sufficient expertise, it was also important for diverse perspectives in order to prevent over-emphasis on any one aspect of the repository in a process whose goal was a comprehensive analysis of each digital repository:

“And the importance of having people from organizations on this advisory committee helped shape that more consistently so that there weren't people with particular hobby horses always insisting on certain ways of doing things. You could have a multiplicity and heterogeneity of backgrounds to temper ... Because the standard doesn't prescribe any particular, doesn't prescribe a whole lot really. It really asks, for the most part whether what the repository is doing meets the expectation and understandings of its members. And so that's what we're trying to

assess is whether they can, first explain what they're doing, and then second whether this meets what they've told their members they're doing and the members have agreed."

Besides recognizing the significance of diverse viewpoints for assessing a repository against all TRAC criteria, which evaluate a repository's risk assessment, interviewees were at ease discussing risk-related matters with each other. Auditor 04 expressed confidence about discussing risk, and asking for input from other audit team members, "I felt very free to contact my colleagues and say, 'I don't understand this, or this seems like a risk to me. Am I reading this correctly?' Or to check in on things that I didn't feel comfortable with before we went to the larger group" (Auditor 04).

In the context of a TRAC audit, a process that evaluates trustworthiness for digital preservation through a process of risk assessment, audit team members were confident that communication about risk information was accurate but were aware that the risk information communicated was not comprehensive. They relied on the varied types of expertise of their audit team members to reach accurate conclusions about the risks facing each repository.

DISCUSSION

Auditors play a central role in TDR certification as the people responsible for interpreting the checklist requirements and applying them to information provided by repositories. Despite their position as key players in the audit and certification process, the experiences and attitudes of auditors have been understudied in digital preservation research. This paper extends discussions about TDR certification to include an investigation into the communication practices of auditors across all of the TRAC audits administered by CRL.

While much has been written about the experiences of repositories going through TDR certification processes, and about the development of TDR standards, the experiences of those conducting the audits have received comparatively little attention. Indeed, one of the interviewees in this study identified communication among auditors in TDR certification as an understudied and opaque, part of the audit process:

"It would be interesting to think about how the communication amongst certification panel members works and what role that plays. I wouldn't say that it's a terribly important flaw in the certification process, but let me put it this way, it was probably one of the least well understood aspects of it, from my perspective. One of the more opaque parts of the process. But I'm having difficulty expressing why" (Auditor 09).

Interviewees expressed confidence in the audit process and the resulting certifications. While they did describe challenges in communication during the audit process, their overall attitudes toward the process were positive and indicated that they were able to effectively communicate with one another to reach a consensus. This aligns with previous research about TRAC, which found that auditors as a group shared consistent understandings of the risks facing repositories and the effectiveness of TRAC certification for demonstrating trustworthiness for long-term preservation (Frank, 2022).

We have established that communication influences the ways in which people perceive and construct their understandings of risk (e.g., Arvai, 2007; Cho et al., 2015; Kasperson & Kasperson, 1996; Konheim, 1988). Communication among audit team members during the TRAC audits was pragmatic, allowing sub-groups of auditors to self-organize and use a variety of synchronous and asynchronous modes of communication. Interviewees expressed positive attitudes toward, and deference to the expertise of, CRL leadership and their fellow audit team members. As the organization coordinating the TRAC audits, CRL leadership also selected the members of the audit team for their expert knowledge. This appears to have facilitated a process in which auditors trusted the expertise of their team members in part because they trusted the judgment of those managing the process. This created conditions that allowed them to be confident in the accuracy of risk information that was communicated during the audit process, while also understanding that the risk information was likely not exhaustive.

The relatively smooth communication about risk information among members of the audit team reflected their shared view of the audit team as consisting of people with expertise in digital preservation. It is likely that the selection process, regular communication, and emphasis on the audit team as a group of experts with a shared goal reinforced this perspective while minimizing the differences in their expertise and areas in which audit team members may have lacked a shared understanding of risk. Research seeking to further examine the social amplification of risk in relation to TDR certification should examine perceptions of risk outside of the direct stakeholders in the certification processes (i.e., standard developers, auditors, and repository staff members), in order to investigate secondary effects as described by scholars such as Renn (1991).

Our findings describe a collaborative, multi-disciplinary process for evaluating digital repositories against the TRAC checklist of requirements. The process involved adaptable communication methods and tools, with the audit team tailoring their approach based on specific conditions and preferences. Although the lack of standardization allowed

flexibility, it is possible that pragmatic approaches to communication and consensus-building could also lead to concerns about comparability across audits. Communication between auditors and repository staff was channeled through one person, which had the potential to both prevent and create opportunities for miscommunication (e.g., Fischhoff et al., 1990). Disagreements were seen as opportunities for further communication, but some interviewees noted that there were limits to the amount of additional information that could be gathered to help resolve those disagreements. We have also identified instances of over-reliance on the opinions of people who were looking to the audit team for expertise and advice. While audit team members were confident in the accuracy of risk information communicated during the TRAC audit process, they were also aware that the information they had could be accurate without being comprehensive.

The high cost of certification, particularly for certification via processes with formal audit teams, brings urgency to the need to understand the inner workings of audit teams in the context of TDR certification processes (e.g., CoreTrustSeal, 2023; PTAB – Primary Trustworthy Digital Repository Authorisation Body Ltd, 2023). Scholarship about risk and audit processes has demonstrated the importance of understanding those who are responsible for interpreting and applying standards to real world organizations (e.g., Vaughan, 1996). The role of auditors in TDR certification is an aspect of certification that has not been the primary focus of empirical research in digital preservation thus far. This paper contributes to the growing body of research about TDR certification by examining communication among auditors during the TRAC certification process.

CONCLUSION

This paper investigates the TRAC audit and certification process, focusing on communication among auditors. The study, based on 10 interviews with audit team members, explores the audit process, communication, disagreements, and risk in TRAC. Findings show that auditors communicated regularly and openly, resolved disagreements through iterative discussions, and recognized the importance of diverse backgrounds for comprehensive analysis. However, they were also aware that the process did not surface all the relevant risks for the repositories being reviewed, and we argue that deference to CRL leadership may have contradicted the TRAC process, in which a team of auditors – selected for their expertise – evaluate a repository in order to determine whether to award certification. Overall, these findings produce a picture of the audit process that inspires confidence in the ability of auditors to work together to evaluate repositories for certification.

Future research should continue to investigate the role that auditors play in TDR certification processes, as this group represents a key component of certification. We also suggest that standards and processes for TDR certification would be strengthened by a stronger focus on the selection of auditors, and by making their work more visible and transparent.

ACKNOWLEDGMENTS

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

REFERENCES

- Arvai, J. L. (2007). Rethinking of Risk Communication: Lessons from the Decision Sciences. *Tree Genetics & Genomes*, 3(2), 173–185. <https://doi.org/10.1007/s11295-006-0068-7>
- Bak, G. (2016). Trusted by Whom? TDRs, Standards Culture and the Nature of Trust. *Archival Science*, 16(4), 373–402. <https://doi.org/10.1007/s10502-015-9257-1>
- Barons, M., Bhatia, S., Double, J., Fonseca, T., Green, A., Krol, S., Merwood, H., Mulinder, A., Ranade, S., Smith, J. Q., Thornhill, T., & Underdown, D. H. (2021). Safeguarding the nation’s digital memory: Towards a Bayesian model of digital preservation risk. *Archives and Records*, 42(1), 58–78. <https://doi.org/10.1080/23257962.2021.1873121>
- Berman, F., Kozbial, A., McDonald, R. H., & Schottlaender, B. E. C. (2008). The Need to Formalize Trust Relationships in Digital Repositories. *Educause Review*, 43(3), 11–12.
- Bernard, H. R. (2013). *Social Research Methods: Qualitative and Quantitative Approaches* (2nd ed). SAGE Publications.

- Bettivia, R. S. (2016). The Power of Imaginary Users: Designated Communities in the OAIS Reference Model. *Proceedings of the Association for Information Science and Technology*, 53(1), 1–9. <https://doi.org/10.1002/pr2.2016.14505301038>
- Bostrom, A. (1997). Risk Perceptions: Experts vs. Lay People. *Duke Environmental Law & Policy Forum*, 8, 101.
- Boyd, C. (2021). Understanding Research Data Repositories as Infrastructures. *Proceedings of the Association for Information Science and Technology*, 58(1), 25–35. <https://doi.org/10.1002/pr2.433>
- Center for Research Libraries. (n.d.). *TRAC Metrics*. CRL: Center for Research Libraries Global Resources Network. Retrieved March 7, 2023, from <https://www.crl.edu/archiving-preservation/digital-archives/metrics-assessing-and-certifying/trac>
- 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
- Center for Research Libraries. (2018). *2018 Updated Certification Report on CLOCKSS*. Center for Research Libraries. https://www.crl.edu/sites/default/files/reports/CLOCKSS_Report_2018_0.pdf
- Cho, H., Reimer, T., & McComas, K. (Eds.). (2015). *The Sage Handbook of Risk Communication*. SAGE.
- CLOCKSS. (2014, July 28). CLOCKSS Archive Certified as Trusted Digital Repository; Earns top score in Technologies... [Nonprofit]. *CLOCKSS News*. <https://www.clockss.org/clockss/News>
- Consultative Committee for Space Data Systems. (2012a). *Audit and Certification of Trustworthy Digital Repositories* (Standard ISO 16363:2012 (CCSDS 652-R-1); Space Data and Information Transfer Systems). Consultative Committee for Space Data Systems.
- Consultative Committee for Space Data Systems. (2012b). *Reference Model for an Open Archival Information System (OAIS)* (Magenta Book CCSDS 650.0-M-2; p. 135). Consultative Committee for Space Data Systems.
- Consultative Committee for Space Data Systems. (2014). *Requirement for Bodies Providing Audit and Certification of Candidate Trustworthy Digital Repositories* (Standard ISO/DIS 16919; Space Data and Information Transfer Systems). Consultative Committee for Space Data Systems.
- Conway, P. (1996). *Preservation in the Digital World*. Commission on Preservation and Access.
- CoreTrustSeal. (2023). *Administrative Fee*. CoreTrustSeal. <https://www.coretrustseal.org/apply/administrative-fee/>

- CoreTrustSeal Standards and Certification Board. (2022). *CoreTrustSeal Requirements 2023-2025*.
<https://doi.org/10.5281/zenodo.7051012>
- Craig, R. T. (1981). Generalization of Scott's Index of Intercoder Agreement. *Public Opinion Quarterly*, 45(2), 260–264. <https://doi.org/10.1086/268657>
- Dillo, I., & De Leeuw, L. (2018). CoreTrustSeal. *Mitteilungen Der Vereinigung Österreichischer Bibliothekarinnen Und Bibliothekare*, 71(1), 162–170. <https://doi.org/10.31263/voebm.v71i1.1981>
- Donaldson, D. R. (2020). Certification Information on Trustworthy Digital Repository Websites: A Content Analysis. *PLoS ONE*, 15(12), e0242525. <https://doi.org/10.1371/journal.pone.0242525>
- Donaldson, D. R., & Conway, P. (2015). User Conceptions of Trustworthiness for Digital Archival Documents. *Journal of the Association for Information Science & Technology*, 66(12), 2427–2444. <https://doi.org/10.1002/asi.23330>
- Donaldson, D. R., & Russell, S. V. (2021). Towards a Taxonomy of Trustworthy Digital Repository Impacts. *Proceedings of the Association for Information Science and Technology*, 58(1), 430–434. <https://doi.org/10.1002/pr2.473>
- Donaldson, D. R., & Russell, S. V. (2023). Trustworthy Digital Repository Certification: A Longitudinal Study. In I. Sserwanga, A. Goulding, H. Moulaison-Sandy, J. T. Du, A. L. Soares, V. Hessami, & R. D. Frank (Eds.), *Information for a Better World: Normality, Virtuality, Physicality, Inclusivity* (Vol. 13972, pp. 552–562). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-28032-0_42
- Dryden, J. (2011). Measuring Trust: Standards for Trusted Digital Repositories. *Journal of Archival Organization*, 9(2), 127–130.
- Faundeen, J. (2017). Developing Criteria to Establish Trusted Digital Repositories. *Data Science Journal*, 16, 22. <https://doi.org/10.5334/dsj-2017-022>
- Fischhoff, B., Hope, C., & Watson, S. R. (1990). Defining Risk. In T. S. Glickman & M. Gough (Eds.), *Readings in Risk*. Resources for the Future.
- Frank, R. D. (2022). Risk in Trustworthy Digital Repository Audit and Certification. *Archival Science*, 22(1), 43–73. <https://doi.org/10.1007/s10502-021-09366-z>
- Frank, R. D., & Rothfritz, L. (2023). Designated Community: Uncertainty and risk. *Journal of Documentation*, 79(4), 880–897. <https://doi.org/10.1108/JD-07-2022-0161>
- Frank, R. D., & Yakel, E. (2013). Disaster Planning for Digital Repositories. *Proceedings of the American Society for Information Science and Technology*, 50, 1–10. <https://doi.org/10.1002/meet.14505001058>
- 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>
- Giarretta, D., LaPlant, L., Shiers, J., Tieman, J., Pennock, M., & Zuberi, I. (2019). Dawn of Digital Repositories Certification under ISO 16363 Exploring the Horizon and Beyond. *Proceedings of IPRES 2019*. iPRES 2019, Amsterdam, The Netherlands. <https://doi.org/doi.org/10.17605/osf.io/py5ah>
- Houghton, B. (2015). Trustworthiness: Self-assessment of an Institutional Repository against ISO 16363-2012. *D-Lib Magazine*, 21(3/4). <https://doi.org/10.1045/march2015-houghton>
- Kasperson, R. E., & Kasperson, J. X. (1996). The Social Amplification and Attenuation of Risk. *Annals of the American Academy of Political and Social Science*, 545, 95–105.

- Kirchhoff, A., Fenton, E., Orphan, S., & Morrissey, S. (2010). Becoming a Certified Trustworthy Digital Repository: The Portico Experience. *Proceedings of the 7th International Conference on Preservation of Digital Objects*, 87–94. <https://phaidra.univie.ac.at/o:185497>
- Konheim, C. S. (1988). Risk Communication in the Real World. *Risk Analysis*, 8(3), 367–373. <https://doi.org/10.1111/j.1539-6924.1988.tb00499.x>
- Krahmer, A., Andrews, P., Tarver, H., Phillips, M. E., & Alemneh, D. (2017). Documenting Institutional Knowledge Through TRAC Self-Audit: A Case Study. *Knowledge Discovery and Data Design Innovation*, 335–348. https://doi.org/10.1142/9789813234482_0018
- Kriesberg, A., & Kowall, J. (2020). Scientific data management in the federal government: A case study of NOAA and responsibility for preserving digital data. *Proceedings of the Association for Information Science and Technology*, 57(1). <https://doi.org/10.1002/pra2.266>
- Lachlan, K. A., Burke, J., Spence, P. R., & Griffin, D. (2009). Risk Perceptions, Race, and Hurricane Katrina. *Howard Journal of Communications*, 20(3), 295–309. <https://doi.org/10.1080/10646170903070035>
- L'Hours, H., Kleemola, M., & De Leeuw, L. (2019). CoreTrustSeal: From Academic Collaboration to Sustainable Services. *IASSIST Quarterly*, 43(1), 1–17. <https://doi.org/10.29173/iq936>
- Lindlar, M., & Schwab, F. (2018, September 24). All that Work... For What? Return on Investment for Trustworthy Archive Certification Processes – a Case Study. *Proceedings of the 15th International Conference of Digital Preservation*. iPres, Boston, MA. <https://doi.org/10.17605/OSF.IO/8A3SC>
- Maemura, E., Moles, N., & Becker, C. (2017). Organizational assessment frameworks for digital preservation: A literature review and mapping. *Journal of the Association for Information Science and Technology*, 68(7), 1619–1637. <https://doi.org/10.1002/asi.23807>
- Moles, N. (2022). Preservation for Diverse Users: Digital Preservation and the “Designated Community” at the Ontario Jewish Archives. *Journal of Documentation*, 78(3), 613–630. <https://doi.org/10.1108/JD-02-2021-0041>
- Nelkin, D. (1989). Communicating Technological Risk: The Social Construction of Risk Perception. *Annual Review of Public Health*, 10(1), 95–113. <https://doi.org/10.1146/annurev.pu.10.050189.000523>
- nestor Certification Working Group. (2013). *Explanatory Notes on the nestor Seal for Trustworthy Digital Archives* (nestor-materials 17). Deutsche Nationalbibliothek. http://files.d-nb.de/nestor/materialien/nestor_mat_17_eng.pdf
- PTAB - Primary Trustworthy Digital Repository Authorisation Body Ltd. (2021). *Certified clients*. PTAB - Primary Trustworthy Digital Repository Authorisation Body Ltd. <http://www.iso16363.org/iso-certification/certified-clients/>
- PTAB – Primary Trustworthy Digital Repository Authorisation Body Ltd. (2023). *Audit Costs*. PTAB - Primary Trustworthy Digital Repository Authorisation Body Ltd. <http://www.iso16363.org/iso-certification/audit-costs/>
- Renn, O. (1991). Risk Communication and the Social Amplification of Risk. In R. E. Kasperson & P. J. M. Stallen (Eds.), *Communicating Risks to the Public* (Vol. 4, pp. 287–324). Springer Netherlands. https://doi.org/10.1007/978-94-009-1952-5_14
- 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
- Scott, W. A. (1955). Reliability of Content Analysis: The Case of Nominal Scale Coding. *Public Opinion Quarterly*, 19(3), 321. <https://doi.org/10.1086/266577>

- Sudman, S., Bradburn, N. M., & Schwarz, N. (1996). *Thinking About Answers: The Application of Cognitive Processes to Survey Methodology*. Jossey-Bass Publishers.
- Thomer, A. K., Starks, J. R., Rayburn, A., & Lenard, M. C. (2022). Maintaining Repositories, Databases, and Digital Collections in Memory Institutions: An Integrative Review. *Proceedings of the Association for Information Science and Technology*, 59(1), 310–323. <https://doi.org/10.1002/pra2.755>
- Vaughan, D. (1996). *The Challenger Launch Decision: Risky Technology, Culture, and Deviance at NASA*. University of Chicago Press.
- Vermaaten, S., Lavoie, B., & Caplan, P. (2012). Identifying Threats to Successful Digital Preservation: The SPOT Model for Risk Assessment. *D-Lib Magazine*, 18(9/10). <https://doi.org/10.1045/september2012-vermaaten>
- Wynne, B. (1992). Misunderstood Misunderstanding: Social Identities and Public Uptake of Science. *Public Understanding of Science*, 1(3), 281–304. <https://doi.org/10.1088/0963-6625/1/3/004>
- Yakel, E. (2007). Digital Curation. *OCLC Systems & Services: International Digital Library Perspectives*, 23(4), 335–340. <https://doi.org/10.1108/10650750710831466>