Arch Sci (2017) 17:349–370
DOI 10.1007/s10502-017-9280-5

ORIGINAL PAPER

Using the cloud for records storage: issues of trust

Julie McLeod[1] · **Brianna Gormly**[2]

Published online: 1 September 2017

Abstract Organisations cannot avoid working in the cloud and therefore records are being stored in the cloud either by design or by default. This raises important issues of trust in using third-party cloud service providers for storing records and digital archival collections. What factors contribute to trust in the decision-making process? What are the implications that archives and records (ARM) professionals need to understand and assess? This article discusses findings from an international research project that explored issues of trust in the context of the economics of cloud storage services. The most significant issues of trust to emerge were trust in the sustainability and continued economic viability of cloud storage services. Whilst anticipated costs savings (software, hardware, human) was the most frequently cited reason for adopting a cloud storage service, the research revealed that very few organisations or ARM professionals had actually estimated the costs, suggesting decision-making processes are inadequate. A basis for trust in cloud storage solutions might be found in the enhancement of checklists and other guidance documents for ARM professionals to address economic considerations.

Keywords Cloud computing · Records storage · Trust

✉ Julie McLeod
julie.mcleod@northumbria.ac.uk

Brianna Gormly
brianna.gormly@fandm.edu

[1] Department of Computer and Information Sciences, iSchool, Northumbria University, Room 117, Pandon Building, Camden Street, Newcastle upon Tyne NE2 1XE, UK

[2] Archives and Special Collections Martin Library of the Sciences, Franklin & Marshall College, P.O. Box 3003, Lancaster, PA 17604-3003, USA

Introduction

Organisations cannot avoid working in the cloud; in fact International Data Corporation (IDC 2016) estimates that worldwide sales of cloud related IT infrastructure for the top five vendors in the market grew by over 20% to $29 billion in 2015, representing almost one-third of their total revenue from IT infrastructure sales. For archivists and records managers, the issue of using cloud services to store records and archive collections is particularly important. As more data and information is generated and stored in the cloud, either by design or default, they need to be confident they can trust cloud service providers for storing their organisation's records. If cloud service providers are to be used, their viability, sustainability and trustworthiness are paramount. What are the issues of trust in using the cloud for records/archives storage and what factors contribute to trust in the decision-making process?

This article reports on part of a larger study exploring economic models for storing records in the cloud and archives' use of these models in the cloud decision-making process. Such models can be helpful in forecasting the medium to longer-term financial implications of cloud storage to enable greater confidence in the decision (McLeod and Gormly 2015). The study included a literature review to identify existing models and an empirical study of their use in practice, the full details of which have been reported elsewhere (McLeod and Gormly 2015, 2016). It also examined issues of trust in third-party cloud service providers in order to contextualise the economic decision-making process. This part of the study revealed insights into issues of trust in cloud storage that went beyond the study's original focus on economic aspects and warranted further analysis.

This article presents the specific issues and themes identified from that analysis. It first provides background on the push towards cloud storage for records, followed by a literature review discussing trust in the context of storing records in the cloud. It then presents the findings of the study related to issues of trust and a discussion of the themes that emerged from these findings. Finally, it concludes with implications for archives and records management (ARM) professionals.

Context

Third-party cloud services include public cloud, community cloud, or hybrid cloud as well as private clouds managed by a third party. It is important to study their adoption for records/archives storage because they can improve access to and sharing of digital collections, increase potential for their long-term preservation, increase security, take advantage of economies of scale and potentially save money. Early drivers towards cloud storage were the economic benefits, highlighted in literature from service providers and consultancy companies (Forrester Research 2011; Gartner 2011), though more recent literature has brought the financial benefits into question (e.g. Gartner 2015). There is evidence that ARM professionals are increasingly using the cloud for the storage of digital collections (e.g. Brown and

Fryer 2014; Oliver 2014; Oliver and Knight 2015; Zander 2014). However, decisions about using in-house versus cloud storage are complex; there are implications if the wrong decision is made. In particular, a move to the cloud can mean a loss of control where interruptions in the service may make data inaccessible and there may be a lack of clarity about where data is stored (Duranti and Rogers 2012, pp. 529–530). Can we trust in cloud service providers to store our records?

For records and archives collections, these questions are particularly significant because of the inherent uniqueness, special characteristics and role of records and archives as evidence of "business" activities and as information assets (ISO 15489:1 2016). Archival records support accountability, protect rights, aid decision-making and can create value. However, storing records in such a way that they can remain authentic over time proves a complicated question as research projects have explored (see for example InterPARES 1998–2012; Strodl et al. 2011).

Literature on trust

Existing work on trust and digital records in the archives and information studies disciplines largely falls into two categories: examining the trustworthiness of digital records themselves and exploring users' trust in digital information and information systems. Reporting on the first InterPARES project, MacNeil (2000) discusses the requirements for authentic digital records, specifically, verification of their identity and integrity. Here, trust is presented in the context of trust that the record is authentic (MacNeil 2000, p. 53). Whilst the record preserver can perform the appropriate checks to ensure a record is authentic, as the title of MacNeil's article suggests, this is the "grounds" for trust, but it is the future user who decides if the record is trustworthy (MacNeil 2000, p. 74).

MacNeil's conception of trust, as trust in the record to be authentic, appears elsewhere in archival scholarship (see Meijer 2003, p. 289). In fact, in an overview of the formulation of trust from a recordkeeping perspective, Sundqvist (2011) sees "a conflation of the concepts of trust and reliance, and of trustworthiness and reliability" (p. 289). In this view, "[t]rustworthiness" is "an objective property" of the record (Sundqvist 2011, p. 289). More recent work by the InterPARES project also situates trust in the context of trustworthy records. Duranti and Rogers (2012) apply this view directly to cloud computing and situate "trust in records" as based on what can be known about the parties responsible for the records over time (particularly the records' custodian) (p. 522). However, writing about trust in the context of cyberspace, Yeo (2013) notes that trust in archivists, archival institutions (custodians), governments and private corporations (specifically banks in the context of financial crises) is "in decline" (p. 215).

As noted above, MacNeil also views trust as a property understood through the perspective of the user, and other scholars of information studies focus on trust in terms of users' views of digital information. Kelton et al. (2008, p. 363) explore trust in order to address a gap in the information studies field (citing Hertzum et al. 2002 as an exception). They present their Integrated Model of Trust in Information, which illustrates how users trust (or not) digital information (Kelton et al. 2008,

pp. 368–370). Donaldson and Conway (2015, p. 2441) further apply and interrogate Kelton, Fleischmann and Wallace's model in an archival context.

Additionally, a few studies have looked at the trust between parties involved with digital archives. Price and Smith (2011) respond to the limited discussion of trust within archival scholarship (p. 254) and look to trust "between groups within society" rather than trust in objects (p. 255). Specifically, they examine trust between archives and users of archives (pp. 265–266) and between archives and record creators (pp. 259–260). Oliver et al. (2011) explore the trust that information and communication technology (ICT) professionals have in archivists to preserve and provide access to digital records (pp. 312–313). In fact, trust in the context of trust between different involved parties appears in the conclusion of Duranti and Rogers' (2012) article when they bring their discussion of trusting records, based on knowledge of the custodian, to "the [cloud service] providers to whom we trust our records and data" (p. 530).

More recent studies have examined trust in the context of the cloud. Franks et al. (2015) look at the specific issue of retention and disposition, exploring how the use of cloud services affects the ability to retain and dispose of records in accordance with the law and other applicable guidelines, as well as how any resultant risks might be mitigated. Through a survey of ARMA International members, they identified both internal and external obstacles that require trust and understanding of cloud services and also assessment of risk related factors. In essence their recommendations are about cloud service providers offering fit-for-purpose services and ARM professionals trusting those services based on a risk assessment.

Stancic et al.'s (2015) comparative analysis of the security policies of selected cloud infrastructure service providers in Croatia sought to identify the information needed for potential customers to view the company as a trusted service provider. With only three responses from 10 service providers, it is difficult to draw firm conclusions. However, the study demonstrates that not all cloud service providers perceive the concept of trust in their service as their concern. Some use disclaimers to place responsibility on the user, whilst others do not understand the special attention required to become a trusted provider. The authors concluded that trust between customers and cloud service providers should be based on providers communicating adequate information and customers negotiating the functionality required. Trust should therefore be seen as a combined socio-technical set of requirements, roles and responsibilities, and responsible governance (including rules, policies, procedures and best practices).

Specifically addressing the perspective of information professionals, Borglund (2015) and Oliver and Knight (2015) provide relevant discussions of these professionals' trust in cloud solutions and service providers, respectively. Borglund (2015, p. 116) interviewed Swedish archivists, whilst Oliver and Knight (2015) use the National Library of New Zealand's National Digital Heritage Archive as a case study. Both studies touch on the financial dimension of using the cloud for archives. Congruent with other research, Borglund (2015) notes that half the archivists interviewed stated that the move to cloud storage was for cost reasons. However, the interviews provided a "more nuanced picture" when interviewees indicated that they could be more certain about the costs of their contract with the cloud service

provider as opposed to in-house costs, which tended to be unclear (Borglund 2015, p. 123). Similarly, one benefit noted in Oliver and Knight's (2015) study was "greater transparency about the costs involved in digital preservation activities" (para. 16). Trust plays a role here because, as the in-house costs were not clear, making the economic decision to move to cloud storage involved "a leap of faith" (para. 26).

These studies consider issues of trust in selecting a cloud service provider but, for existing users who lose trust in a service provider they use, what are the reasons why they lost trust? Looking beyond the archives, Leverich, Nalliah and Suderman explore the experiences of individuals using "mainstream services" (e.g. Facebook) "to determine how trust-related issues changed the nature of users' trust in the service" (Leverich et al. 2015, p. 3). Based on the trust literature and a case study they argue that "trust in the service provider is a far greater consideration than trust in the technology" (Leverich et al. 2015, p. 4). In the course of their study, they review many trust typologies and identify three types of trust particularly applicable in the context of cloud services—cognition, relational and calculated trust. Cognition-based trust is based on judgments about, for example, responsibility and reliability (McAllister 1995; Lewicki et al. 2006). In a cloud context, these might include (first) impressions of a service, a provider or technology interface (Leverich et al. 2015, pp. 4, 8). Relational trust is based on direct experience "from repeated interactions over time between trustor and trustee" i.e. information "from within the relationship itself" (Rousseau et al. 1998, p. 399). Finally, calculated (or calculus-based) trust is a rational economic choice (Rousseau et al. 1998, p. 399) i.e. a cost–benefit decision at a given time.

In this way, the archival and information studies literature has touched on issues of trust in digital records and cloud services, directly and indirectly related to archives' use of the cloud. This article further explores issues of trust for information professionals and their organisations when considering the cloud for records storage and the nature of the trust relationships involved.

Research investigation

Overall, our study aimed to more directly explore economic considerations in the choice and sustainability of cloud storage, which had been touched upon in the studies by Borglund and Oliver and Knight, as well as to extend coverage into the international arena. As part of the larger InterPARES Trust project (www.interparestrust.org) on public trust in digital evidence on the Internet, issues of trust in third-party cloud service providers were examined in order to contextualise the economic decision-making process. The study was conducted through an online survey and follow-up interviews with a small number of respondents.

The survey design was influenced by another InterPARES Trust project (The Use of Cloud Services for Records Management in International Organizations) which the authors had access to and was ongoing at the time of this research. It was subsequently reported by Goh and Sengsavang (2016) and was helpful in terms of the structure for gathering demographic information on respondents and their

organisations, as well as their experience in disseminating their survey (Goh and Sengsavang 2016). The development of the survey questions was informed by the study's research questions (McLeod and Gormly 2016, p. 4). The questions fell into three main themes: use of the cloud for records storage; trust in adopting cloud services; and use of economic models in the decision-making process for records storage. The initial survey was piloted with other InterPARES Trust researchers and their contacts, and revised based on feedback. It also was split into two parts: The first asked about the organisations' use of cloud storage and the second asked questions from the respondents' perspectives in their specific roles. This structure was designed to capture any differences between respondents' views and those of their organisations, irrespective of the extent to which the respondents were involved in the decision-making process. In December 2015, the survey was disseminated online through a purposively selected global set of archives, records and information management listservs, and by international research colleagues to contacts and relevant stakeholders in their organisations. Due to low response, it was disseminated again in February 2016. McLeod and Gormly (2016) provide full details of the survey tool (Appendix A pp. 22–38) and dissemination channels (Appendix B, p. 39).

Ultimately, 61 completed survey responses and 115 incomplete responses were received. Only the complete responses were analysed. Perhaps unsurprisingly, over half the respondents (54%) were ARM practitioners and 13% ARM educators or researchers. 11% were IT professionals, 10% in administration and the other 12% had a role that combined ARM with another area (e.g., administration, IT, risk, Freedom of Information, and e-government). Respondents were based in 17 different countries; however, the majority were in English-speaking countries (66% from Australia, Canada, the United Kingdom, and the United States). The majority of respondents were from governmental and educational organisations (33 and 23% respectively). In terms of their involvement in decision-making about the adoption (or not) of cloud services for storing some or all of their organisation's records, 28% were largely involved, 49% partly involved and 23% not involved. Whilst the response rate and demographics limit the generalisability of the results to the international records and archives community, and preclude any meaningful comparison of the perspectives of respondents according to their role, the results can be viewed as a snapshot of current perceptions of cloud storage in the information profession.

At the end of the survey, respondents indicated whether or not they would be willing to be contacted for an interview to provide a case example and more detail about issues of trust. Potential interviewees were necessarily self-selected because the survey was anonymous, making it impossible to purposively select from the pool of respondents. Of 16 respondents who answered "yes" to this question, seven were not relevant for follow-up, either because they did not know if their organisation used the cloud or economic models, or because their organisation neither used the cloud nor an economic model. Of the remaining nine respondents, five were ultimately available to be interviewed. All interviewees were either ARM professionals or had a role that combined ARM with something else. Their organisations all use the cloud to some extent and represent a global spread of

different sectors and different sizes (100–3000 staff). From smallest to largest, they were a Spanish city council, a Canadian religious organisation, a New Zealand state owned body, a Canadian university and a UK public sector body. They are diverse in terms of their use of the cloud for storing records, with one using it specifically for its digital archives, three using it for business systems (therefore storing records by default), and one using it for a specific business function (teaching) but not for its organisational records. Table 1 provides a summary of the case example contexts. As stated in the introduction, whilst the overall study explored economic aspects of cloud storage, this article reports on insights pertaining to issues of trust, which have broader implications. The following sections report on the relevant data from this part of the project, which was directly addressed in four survey questions and discussed more extensively in the interviews.

Survey findings

Reasons for use (or not) of cloud storage for records

Just over half (32) of the survey respondents said their organisations used the cloud for records storage; 43% did not, and the rest did not know. 47% of the organisations stored some of their records in the short term (defined in the survey as 1–9 years) and 35% stored some of them in the longer term (defined as 10 + years). Only 10% stored all of their records in the cloud in the short term and no organisation used the cloud for longer-term storage of all of its records.

The top two factors their organisations had considered in making the decision were operating costs (41 of 61) and technology suitability (37 of 61); this was followed by risks (31 of 61), which relates to trust. For respondents who indicated that their organisation did or did not use cloud storage, the survey asked why or why not. Respondents in organisations using cloud storage indicated that the decision to use the cloud was based on anticipated cost savings in hardware and software, and in human resources (25 and 14 of the 32 respondents respectively), which supports the observations that cloud storage has been promoted for financial reasons. Some of these respondents cited (positive) trust in cloud computing deployment models (6) and trust in cloud service providers (8) as factors for adopting cloud storage services, but these were less important than service-related factors (e.g. increased flexibility and energy savings, enhanced availability, improved scalability of IT infrastructure and business continuity). In contrast, half of respondents in organisations not using cloud storage (13 of 26) cited lack of trust in cloud service providers as the reason for their choice followed closely by legal/regulatory requirements (10 of 26).

Issues of trust

All respondents in organisations both using and not using cloud storage were asked to rate the importance of a list of issues of trust from not important to extremely important, with the option "don't know". The issues were grouped into four themes

Table 1 Summary of the case example contexts

Case 1: Large UK public sector body
Developed its first digital repository in 2013, making use of cloud services for storing low usage archival records that have no security classification. Includes records of some core business functions but primarily archived websites and digitised archival records (public access is to other copies). Present volume ~17 Terabytes. Archives Department's decision to use cloud services motivated by the organisation's adoption of a 'cloud first' IT strategy in alignment with UK Government's 'Cloud First' policy. An in-house digital repository storage centre would then bear a disproportionate level of inherent overheads, substantially increasing costs
Case 2: Large 100-year-old Canadian technical college, satellite campuses around the world
Has a records management team and an archives unit. No formal records management programme until 2015. Many hard copy records are stored with a commercial service provider, large percentage of born-digital records being created and stored in digital form only. Organisation looked at the cloud for digital records storage and cost savings in human resources. Began using Apple's iCloud to store some records in 2015 through a time-limited introductory offer. Though not a solution to the lack of a fully developed records management programme, in conjunction with a new retention schedule and development of records classification, the cloud offered an alternative storage solution for inactive digital records. However, senior management put its adoption on hold
Case 3: Large New Zealand state owned enterprise, many contractors
Has a well-established records management service and is one of Microsoft's early adopters worldwide. Decided to move to an evergreen platform when Microsoft offered a big discount to move to its new cloud platform and services suite. Microsoft was looking to trial its new platform. Organisation was in a good position in terms of IT lifecycle management; offer showed a substantial monetary advantage against its 3–5 year budget, though the organisation recognised there would be risks. Cost was not the only driver for moving to the cloud; increased flexibility, access to specialised services, evergreen technical support, avoiding shadow IT (i.e. individual staff or business units "doing their own thing") and gaining centralised control, ability to work collaboratively with third parties, better remote/home working support, 24/7 access and use of portable devices (part of business transformation) were other drivers. A strategic decision for organisational benefit but providing an excellent opportunity to move its records management to the cutting edge (e.g. implementing ontology driven records management with front end auto-classification)
Case 4: Large Spanish City Council responsible for governing the city, providing public services administration and fostering socio-economic development of the area
Well-established ARM departments with records management processes/requirements well integrated into management and business systems. Has used cloud-type platforms to provide and manage public services and projects for a long time. Now uses the cloud for Software as a Service (e.g. to maintain public street lighting, to manage incidents in collaboration with the Police Service). Using these cloud services means records are created, used and therefore implicitly stored within those systems. Present volume ~2 Terabytes. Started to use a cloud service to manage its own records in 2005. In principle does not use the cloud for storing its 60 Terabytes of digital archival records, these are managed in its own system. There is no driver to do so though if a cloud provider offered software of interest for this collection it could be an option; not currently on the agenda
Case 5: Medium Canadian religious organisation formed by an amalgamation of four related organisations, with staff spread across four different geographical locations
Organisation does not have a records management programme but has used public cloud services to store some records since 2014. Main driver for using the cloud was to solve problems of file sharing between different locations, provide access to files and email for leadership members and staff travelling on business, and connect everyone. Uses the cloud for generic office software and a professional association archives catalogue database. Administration, finance, personnel and facilities management records are stored in the cloud but firm decision not to store archival records in the cloud

relating to: concerns about the service, including economic viability and sustainability; potential savings; lack of trust in cloud computing and cloud service providers; and the decision-making process. Figure 1a, b shows the respondents' assessment of their organisations' perspectives, as users and non-users of the cloud for records storage, respectively. Figure 2a, b shows the respondents' own perspectives, again filtered by organisations using and not using the cloud for records storage, respectively.

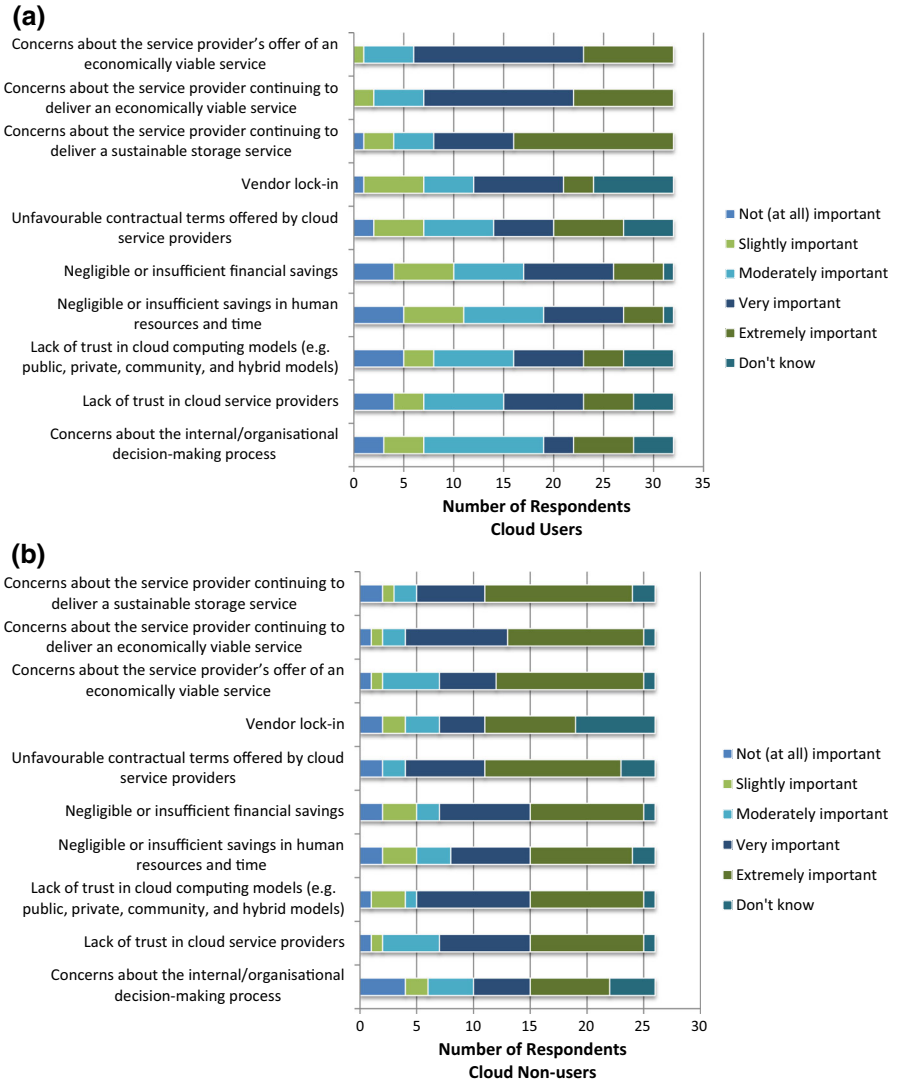

Fig. 1 **a** Importance of trust issues in adopting a third-party cloud service for records storage—perspective of organisations using the cloud. **b** Importance of trust issues in adopting a third-party cloud service for records storage—perspective of organisations not using the cloud

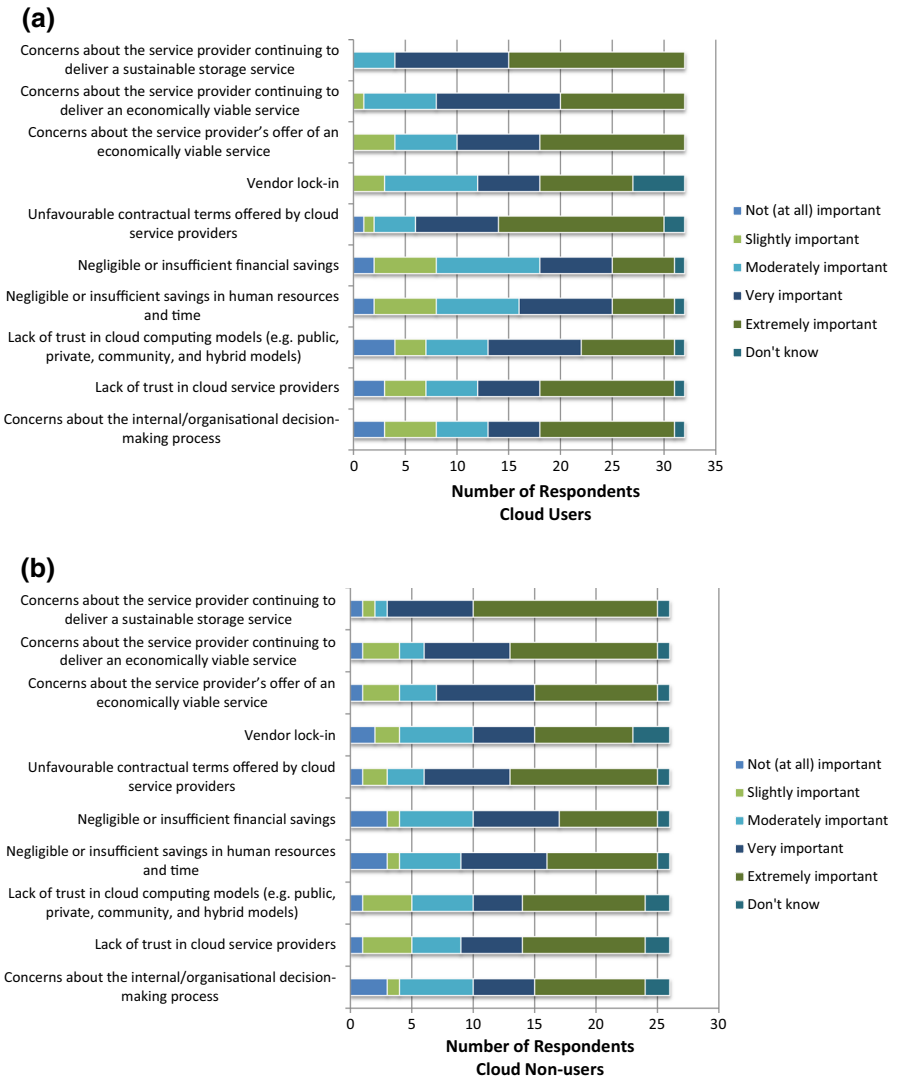

Fig. 2 **a** Importance of trust issues in adopting a third-party cloud service for records storage—perspective of respondents using the cloud. **b** Importance of trust issues in adopting a third-party cloud service for records storage—perspective of respondents not using the cloud

For organisations, the areas of greatest concern (ranked very or extremely important) were about the service provider offering a financially viable service, continuing to deliver an economically viable service, and also continuing to deliver a sustainable service. Segmenting the data by organisations that had chosen versus had not chosen to use the cloud shows that cloud users tended to be somewhat less concerned with trust issues (Fig. 1a), suggesting they had satisfied any concerns or were managing them. Those who had chosen not to use the cloud tended to rank

issues of trust as extremely important (Fig. 1b) and perhaps were non-users because their concerns were not adequately addressed or their risk appetite was less. However, as reflected in the overall data, cloud users are still concerned about issues of viability and sustainability of the service.

In general, respondents considered trust issues more important than their organisations. Respondents were particularly concerned about unfavourable contractual terms offered by the provider and the sustainability of the service in the future (see Fig. 2a, b). Given the overwhelming majority had an ARM role, it is unsurprising that service sustainability emerged as a major concern. Well over half indicated that concerns about the provider's offer of an economically viable service, and the service continuing to be economically viable in the future, were either extremely or very important. Sorting the data by respondents in organisations using and not using the cloud did not reveal substantially different views as Fig. 2a, b shows. However, respondents in organisations not using cloud storage were slightly more likely to rank issues of trust as extremely important (Fig. 2b). This follows the same trend as responses at the organisational level (Fig. 1b). Overall, the respondents' greater concern about issues of trust as compared to their organisations may reflect their greater awareness of these issues in their professional roles (ARM practitioner/researcher, IT, etc.). Respondents were invited to share any other issues of trust they had considered. There were very few and they related to security, legal and specific service issues, with one respondent noting a lack of trust in staff having the skills to make informed decisions (see McLeod and Gormly 2016, pp. 73–74).

Though there was a difference in degree between how respondents ranked issues of trust for themselves and for their organisations, there were similarities in which issues were considered to be of greater or lesser importance as careful comparison of Figs. 1a, b and 2a, b shows. For both the respondents and their organisations, irrespective of their use of the cloud for records storage, the most important issues of trust were the service-related ones (i.e. economic viability, sustainability, contractual terms or vendor lock-in), although there were some variations in the relative importance of the different aspects. Similarities in relative importance are evident for the other trust issues, with one notable exception. More respondents indicated that concerns about the internal organisational decision-making process were extremely important for them (23 respondents), whereas only 15 respondents indicated that this issue was extremely important for their organisations, with slightly more indicating that it was only moderately important (16 respondents). This might suggest that respondents in their professional roles encounter issues in the decision-making process which are going unnoticed by their organisations, or it might reflect the exclusion of their concerns from the decision-making process, as 23% were not involved in the process.

Trust in the organisation's decision-making

To better understand the issue of trust in the internal or organisational decision-making process, the survey included a question asking what factors contributed to trust in the process. The options were slightly different for the organisation's perspective versus the respondent's own perspective (see Fig. 3 caption).

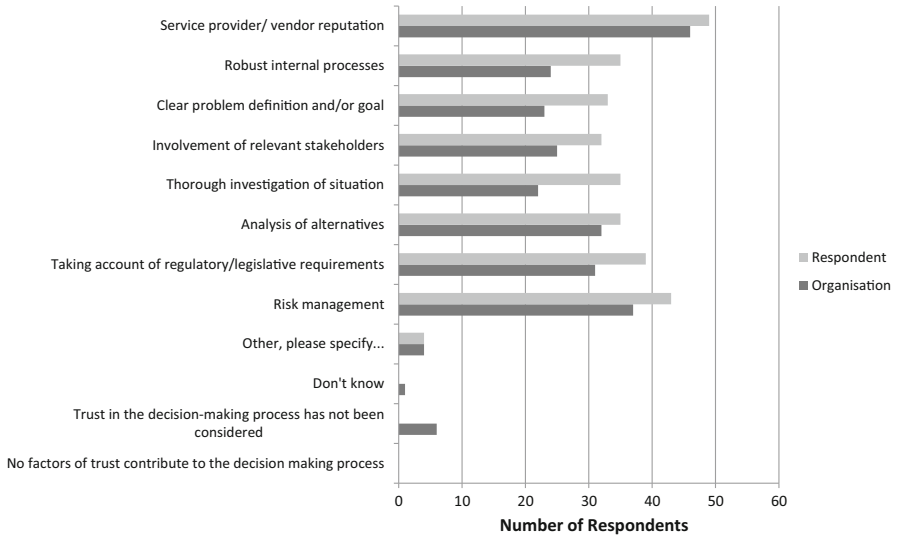

Fig. 3 Factors contributing to trust in the decision-making process—all respondents. *Note*: The first nine options were the same for both the organisation's and respondent's perspectives. The options "don't know" and "trust in decision-making process has not been considered" were only for the organisation's perspective to account for the respondent not knowing. The option "no factors of trust contribute to the decision-making process" was for the respondent's perspective only

Respondents could select as many factors as they felt were relevant. From the organisations' perspective, the most important factor (46 of 61 responses) was the service provider/vendor's reputation, followed by risk management (37 of 61 responses) (Fig. 3). This was the case irrespective of whether the organisation was or was not using cloud storage. Several respondents who chose "other" noted factors related to the contract with the service provider. Two specifically referred to "delivery capacity" and "clarity about durability levels provided"; a third noted that "solutions often meet business needs", however, future business needs were not necessarily being adequately considered which was "contributing potentially to a false sense of trust". From the respondents' perspective, the top two factors contributing to trust in the organisation's decision-making process were the same; however, taking account of regulatory/legislative requirements was also very important. In fact, this factor ranked slightly above risk management for respondents in organisations using cloud storage. In contrast, non-users most frequently considered internal rather than external factors (e.g. thorough investigation of the situation, analysis of alternatives and robust internal processes).

Case examples: issues of trust

Whilst the survey data provided a snapshot of what issues of trust were of concern to information professionals, the interviews provided context for why these factors were problems for archives. Each organisation had considered a range of factors in

reaching the decision to use cloud services for records storage, some of which related directly or indirectly to trust. It is important to note that, with one exception, the interviewees did not always know what their organisation's perspective of trust issues were and were sharing their view or interpretation of it. The exception was Case 1 whose organisation saw it as being the Archives Department's responsibility to consider and be satisfied about issues of trust and hence the perspectives were the same.

Cloud service providers

The cases mirror the importance of trust in cloud service providers that emerged from the survey. For Case 2, lack of trust was based on the information professionals' negative past experience with one particular provider. For Case 1 trust in cloud computing deployment models and in service providers were factors in deciding to use the cloud for records storage. Allied to this, they had considered risks, responsibilities and stakeholder impact. Case 3, which was in the process of business transformation, had considered the ability to work collaboratively with third parties and the socio-political benefits of using the cloud "to meet changes in expectations brought about by the digital world". The desire to better support remote/home working as well as meet the need to access information anywhere, anytime, from any device implies trust in the platforms to deliver these services.

In case 5, whilst the organisation trusted in cloud computing models and the service provider's reputation, the archivist and administrative assistant had serious concerns which they voiced in meetings and in briefing papers to its leaders. Concerns centred around maintaining the records' authenticity, reliability and integrity. Further, they noted concerns about: (1) records subject to discovery, even though their service provider Microsoft stated it was able to place holds on records for discovery; (2) that Microsoft states it can access data to improve service or to troubleshoot; and (3) the potential for records to be lost or deleted, surveilled, or hacked. "Microsoft does have good security and encrypts data in transit and storage, and does not mine data; however, [it] states that it may disclose data without prior consent. The inability to do an external audit with a large corporate provider like Microsoft is a concern". These factors led to their decision not to store born-digital or digitised records, transferred to the archives, on the cloud server.

Adding further context to this issue, Case 3 interviewee (a senior manager in the IT Department with an ARM education) pointed out that the importance of trust in the cloud as a platform and for software can be lowered by the choice of content for which an organisation uses the cloud. Their organisation planned to store only administrative records and records of some core business functions (e.g. manufacturing, sales, research) that were classified as "public" or internal/confidential. By exempting its critical services from moving content to the cloud, the organisation had effectively lowered its trust threshold. This was similar in Case 1, which stored only records that were open to the public, and Case 4 where only "non-official records" were stored and only if the information does not contain personal data subject to data protection legislation. This aspect of trust is only partially reflected in the survey results where, of 20 respondents, just over half (11) said records

classified as "public" were stored with third-party cloud services, half were storing internal/confidential records, 9 were storing restricted/sensitive/secret records and only one was storing highly confidential/top secret ones. Interestingly, Case 3's IT Department viewed the risks of using the cloud as not significantly different to those faced on premises, although the magnitude of the consequences should a risk materialise are likely to be significantly greater depending on the risk, since they are not wholly in the organisation's control.

Vendor lock-in

Vendor lock-in was a significant issue of trust in two of the cases but less so for others. For Case 1, this was related to the "durability of service", i.e. the ability of the service provider to retain and return the data with its integrity intact at any point. Their strategy for addressing the issue was to add resilience by using two service providers, identified from a sector recommended list, and duplicating all content to both. This proved to be a cost-effective approach as the level of resilience required of each service provider could be reduced, meaning procurement of a cheaper service from each one and a lower overall cost. This reflects the view expressed by Case 4 interviewee that concerns about the service provider and vendor lock-in can be summarised as "being careful" in a market that is still developing, with a lot of new companies offering products, and not yet considered "safe". These views contrast with the survey findings where vendor lock-in was not one of the top concerns; however, vendor lock-in relates to issues of sustainability, which were large concerns for a majority of respondents.

Service viability and sustainability

A series of issues emerged related to the offer of an economically viable storage service, and trust in the continued delivery of both an economically viable and sustainable service. All of the interviewees and their organisations considered the offer of an economically viable service to be highly important. However, some were less concerned about its continued economic viability. For Case 1, the context of storing low usage archival records used only by relatively few staff, together with the UK Government's Cloud First policy for public sector IT procurement, contributed to this view. In 2013 the UK Government announced that "purchases through the cloud should be the first option considered by public sector buyers of IT products and services" in an attempt to make savings and efficiencies, for example by ceasing to operate in-house data centres, and improve competitiveness (Great Britain. Cabinet Office 2013). For Case 3, their strong relationship with Microsoft was a factor; and for Case 5, the focus was on using the cloud to solve the immediate problems of information access and sharing rather than taking a longer-term view.

With the exception of Case 1, which had contracts with two service providers running at staggered dates, the interviewees were particularly concerned about sustainability. This is not surprising given the nature of records as information assets and the responsibility of ARM professionals to ensure their availability over time,

however long. Again, the interviews reflect the survey results in which roughly half of respondents (30) indicated that sustainability of the cloud storage service was extremely important. Further, the case examples highlight a complicating factor viz. a gap in understanding between ARM professionals and their organisations that do not fully understand the implications of ensuring that the storage service is sustainable in a recordkeeping context.

Cost savings

Each organisation had considered the capital and/or operating cost in deciding whether to use cloud services for records storage, and were split in their view of the importance of cost factors. In this way, they did not reflect the survey data in which cost saving was the most frequently cited reason why organisations had chosen to use cloud storage. Three interviewees indicated that cost was important to some degree. Having evaluated the overall costs of in-house versus cloud storage to the organisation over time, the economics of using the cloud was a deciding factor for Case 1. It was anticipated that, in the context of the cloud first strategy, there would be no or few in-house data centre services in the future. In such an event, an in-house digital repository would have to bear a disproportionate level of inherent overheads, thereby substantially increasing the cost. Case 2, which had developed a formal records management programme only the previous year, was moving away from paper storage and looking at the cloud for digital records storage and cost savings in human resources. Although cost was not the only driver to move to the cloud for Case 3, Microsoft approached them with a heavily discounted offer if they moved to the new Microsoft cloud platform with its suite of services. The organisation was in a good position in terms of IT lifecycle management and a review of its IT budget for the next 3–5 years showed a substantial monetary advantage, though the organisation recognised there would be risks.

Cost can be particularly important in cases where the use of cloud software as a service offers (e.g. email, office, and other standard systems) means that records are created, used and, therefore, implicitly stored within those systems. This "records storage by default" scenario is more complicated than known archival collections whose size, growth rate and use can be relatively accurately estimated, as exemplified in Case 1. Indeed Case 4 interviewee recognised that the cost was not known. Failure to consider costs is particularly worrying in such a scenario, especially if ARM professionals are not involved, as Case 3 interviewee highlighted. Since their IT Department is responsible for monitoring costs, if costs increase and the increase cannot be borne, they will probably discuss how to reduce them with the individual business units. A likely approach is to reduce storage costs by cutting content but without considering what content to cut and hence making arbitrary decisions. This is a disconnection between IT and ARM.

With one exception, the interviewees shared the same perspective as their organisations. This is perhaps unsurprising, given all of the organisations had considered cost in reaching their decision, and reflects trust and/or agreement in the cost factor. However, only Cases 1 and 3 were actively monitoring costs and in both instances this was the responsibility of the IT Department.

Contractual terms

Issues of trust also emerged about contractual terms with all five interviewees considering unfavourable contractual terms to be moderately to extremely important. In Cases 2 and 5, the ARM professionals were much more concerned about contractual terms than their organisation. For Case 2 this was due to poor past experience elsewhere. For Case 5 ownership of records was a concern. Although their provider (Microsoft) "states it will delete data once a contract is finished it is not clear if the data is zeroed out". Portability of records, migration or refreshing to ensure long-term preservation, the retention of embedded metadata and the potential addition of metadata by the cloud provider were other concerns, all of which need to be addressed in a contract. An additional concern for Case 5 was compliance with Canadian legislation, given that Microsoft servers were not located in Canada when the service contract was signed. Microsoft (2016) later announced they would open two data centres in Canada in 2016. Even though, as a religious organisation, the archives is not subject to federal or provincial privacy laws, the archivist wanted to follow best practice and comply with existing legislation, resulting in a decision not to store archival records in the cloud at the time. The cases reflect the survey data in which respondents ranked unfavourable contractual terms as very or extremely important from their perspective but did not indicate that it was as important from the perspective of their organisation. However, Cases 1 and 3 were less concerned with contractual terms since they were, respectively, aligning with their sector's cloud first strategy and had a strong relationship with Microsoft. Both situations contributed to greater trust.

Internal decision-making process

Trust in the internal decision-making process varied. The organisations' perspectives spanned the entire range, from not at all important, reflecting complete trust in the process, to extremely important reflecting the need to have complete trust. Most of the interviewees shared the view that this was an extremely important trust issue. However, in Case 1 the Director of Archives viewed it as less important since there were robust internal processes in place which ensured the situation was thoroughly investigated, requirements taken into account, risks assessed and managed, and relevant stakeholders involved. The involvement of relevant stakeholders was also the one factor that contributed to trust in the decision-making process in Case 2, whose aim was to manage any potential distrust in moving to the cloud for staff who could be very protective of information.

In Case 4, internal factors contributing to trust were the organisation's management of risk through, for example, the development of requirements and assessment of the systems. The IT Department was only concerned about the technology and was unaware of the risks and confidentiality issues of using the cloud from a records perspective. It was the role of the Records Management Department to make the organisation aware of the recordkeeping requirements. The Department was completing a set of scalable requirements for contracting cloud services. Depending on the risk and criticality of the content, as well as the business actions and access restrictions necessary, some cloud services could be used (or not)

under specific requirements. In Case 4 the organisation listens to the ARM professionals. This was not the same for Case 5 where the archivist and administrative assistant had voiced concerns, which included lack of involvement of all relevant stakeholders, not taking account of regulatory/legislative requirements and not conducting any form of risk management, to the organisation's leaders, but they had not been addressed.

Discussion

The findings from the survey and follow-up interviews revealed three main themes. Overall, the primary concerns of our respondents might be summarised as concerns about the sustainability of the service, the ability of the service to meet records requirements, and the economic viability of the service. Our study also provides some reflections on the existing scholarship on records and trust.

Sustainability of the service

Overall, the most significant issues of trust revealed in our study were trust in the sustainability of a cloud storage service together with the offer and continued delivery of an economically viable service. Perhaps this focus on sustainability is unsurprising considering that archivists have a primary concern regarding preservation and access to records over time. Further, the survey respondents' high level of concern about the continued economic viability of a service also belies issues of trust in the sustainability of the service in addition to the organisation's responsibility for sound financial management. The case examples also reflect on the importance of a sustainable storage service and their discussions connected this concern to issues around contractual terms and vendor lock-in. They speak to a nexus of trust issues around establishing a records solution that can be managed effectively over time.

The case examples also point to how issues of trust in the sustainability of the storage service might be addressed by managing and assessing risk. Risk management was most evident in Case 4, which developed a set of requirements and a method for assessing new systems in the organisation's internal decision-making process. Moreover, Cases 1, 3 and 4 chose to store only particular classes of records, which presents another approach to determining acceptable risk in cloud storage. This strategy follows the conclusions of Stuart and Bromage (2010) who describe cloud adoption as a "risk-based decision" in which the risks differ between organisations and between records of different values (pp. 223–224).

Ability of the service to meet records requirements

A second theme that emerged from the study was the need for records requirements to be considered in the selection of a cloud storage service. As Case 4 demonstrates, establishing requirements informs service procurement and is crucial for contractual requirements. Checklists and guidance documents developed by government archives

and archival scholarship can help ARM professionals determine the requirements to consider in establishing cloud service contracts for storing digital assets of any kind (e.g. ADRI 2010; Bushey et al. 2016; National Archives of Australia n.d.; New Zealand Government 2015; State Records of South Australia 2015). Bushey et al. (2015) list the specific areas these should cover, including many issues of trust that emerged from our study (e.g. ownership; availability, retrieval and use; data retention and disposition; data storage and preservation; security, confidentiality and privacy; data location and cross-border data flows; and contract termination). Clearly defining requirements also can help cloud service providers to understand recordkeeping requirements, such as retention and disposition, to know how these functions can be accomplished, and to develop appropriate products and services, as Franks et al. (2015) recommend. Finally, a requirements list "could be used within an organization to communicate the needs of records mangers and archivists to administration and IT support" (Bushey et al. 2015, p. 131).

Economic viability of the service

Though the survey data indicated a high level of concern about cost among respondents, with cost savings the most frequently cited reason for using cloud storage, interviewees indicated that whilst cost was important, it was less so than other issues (e.g. the ability to move data easily out of an unsustainable service). However, data from the interviews and survey responses also suggest that current assessments of the cost of moving to the cloud are inadequate. This follows the previous work by Borglund (2015) and Oliver and Knight (2015) which demonstrated that in-house costs of archival storage tended to be unknown and unmeasured. It also suggests the "leap of faith" revealed by Oliver and Knight (2015) is more widespread.

If ARM professionals and organisations are to trust in the economic viability and sustainability of cloud storage, then costs need to be modelled and actively monitored. This requires familiarity with the range of costing models available and use of the appropriate one(s) to estimate the economic implications of cloud storage over time. It also means quantifying current storage costs, including hidden, nontechnical costs, and not a nominal future state as the Case 3 interviewee indicated. Their organisation was still investigating the cost but thought it may be higher. For ARM professionals, modelling costs will not only support their trust in service providers to give a fair deal and continue to uphold their agreement in the future, but will also facilitate dialogue with IT colleagues and senior managers, as Case 1 exemplifies.

Framework for trust

In contrast to information and archival studies literature on trust, which primarily focus on trusted content and user trust in that content, the findings of our study are best framed in terms of Leverich et al.'s (2015) work on trust in cloud-based services and the relevant trust typologies they identified. Specifically, information professionals' perspectives on cloud storage might be understood as a balance

between cognitive and calculated trust. The issues of trust that emerged relating to cloud service providers, vendor lock-in and cloud computing models, are all cognitive types of trust—judgments based on first impressions or experience, be that direct or indirect, positive or negative, current or past (McAllister 1995; Lewicki et al. 2006). Cost savings and the economic viability of a cloud storage service, on the other hand, are calculated trust issues (Rousseau et al. 1998), which are the outcome of a more or less rigorous cost–benefit analysis as part of a (trusted) decision-making process that is situational and context specific. Relational trust (Rousseau et al. 1998), based on direct experience through interactions between the user and cloud service provider in this case over time, featured less prominently in the findings. This is perhaps partly because most of the case examples did not have the experience over time and partly because it was not explicitly investigated in the survey. However, trust in contractual terms and service sustainability might be considered to be relational trust issues. Case 4's repeated interactions with cloud-type platforms to exchange information with other government bodies worked well and implies trust in the systems. Though Leverich et al.'s (2015) study applies this framework for trust in the context of cloud-based social media platforms, defining trust in this way is useful for understanding information professionals' perspectives on adopting (or not adopting) cloud storage for records.

Furthermore, our findings reflect (Leverich et al. 2015, p. 4) suggestion that "trust in the service provider is a far greater consideration than trust in the technology", and our study offers some nuance to this idea. Whilst the survey confirmed the importance of trust in the service provider, this trust does not necessarily directly translate into trust in the service being provided. A user may trust an organisation based on the experience of using them for other services and/or technology but, if they do not have a positive track record in cloud-based records storage specifically, a user (potential or actual) may still have concerns about the viability, sustainability etc. of such a service. These are subtly different but clearly related issues that are perhaps attributable to the current stage of development and delivery of cloud services.

Conclusions

Increasingly records are being stored in the cloud, either by design or default. This raises questions about trust in using the cloud for the storage of an organisation's records. Our study sought to explore issues of trust in this context and to identify factors that contribute to trust in the decision-making process. Whilst it is important to acknowledge the limitations of the research, in terms of the survey response and the necessary self-selection of the case examples, this study does provide a snapshot that may act as a benchmark for future research.

The study demonstrates that trust in cloud service providers is an important issue and lack of trust in them adversely affects the cloud adoption decision. Whilst this supports Leverich et al.'s (2015) suggestion about the relative importance of trust in the service provider over technology, it nuances this notion, since such trust does

not necessarily translate into trust in the service being provided. Implicit in this is trust in the service meeting both organisational and recordkeeping requirements.

The key issues of trust to emerge were concerns about the sustainability and economic viability of cloud-based records storage. The study also highlights some notable differences in the perspectives of our respondents and their organisations (albeit to the extent that they were confident about their understanding of the broader organisational perspective). These findings point to an inadequately informed decision-making process and, in many cases, a lack of or limited involvement of ARM professionals in that process. The use of cloud computing checklists and guidance, developed specifically for the profession, can help alleviate these concerns. They can also enable archivists and records managers, who are well equipped with their professional knowledge to consider records storage over time, to play a bigger role in a more informed decision-making process leading to greater trust. Existing checklists do not explicitly address the economic issue and, given the study revealed limited use of costing models, there is an opportunity to add this issue. This would support ARM professionals to ensure they and/or other colleagues fully address the economics as part of the decision-making process and, hence, minimise concerns about long-term sustainability.

The case examples, unlike the survey results, expressed only low levels of concern about the cloud, irrespective of their use or not of the cloud for records storage (either deliberately or by default in business systems). In fact all of the case organisations suggested that the cloud is here, should not be viewed as wholly different and needs to be considered carefully and proactively both in terms of potential benefits and risks. This speaks to technology acceptance (Davis 1989), for which trust is a contributing factor in the cloud context (Sharma et al. 2016).

Trust is only needed in a situation that is risky (Wang and Emurian p. 111) or less well understood and, as Leverich et al. (2015, p. 4) suggest, trust is dynamic. Whilst sustainability and viability are the current concerns in using the cloud for records storage, over time issues of trust may change. Gartner (2016) for example predicts that increased security will become the main motivation for using cloud services. ARM professionals will need to be alert to this shift and guidance will need to reflect it.

Funding This research was partially supported by funding from the Social Sciences and Humanities Research Council (SSHRC-CRSH Grant No: 895-2013-1004 - Trust in digital records in an increasingly networked society).

References

ADRI (Australasian Digital Recordkeeping Initiative) (2010) Advice on managing the recordkeeping risks associated with cloud computing. http://www.adri.gov.au/content/products/cloud-computing.aspx

Borglund E (2015) What about trust in the cloud? Archivists' views on trust. Can J Inf Library Sci 39(2):114–127
Brown A, Fryer C (2014) Achieving sustainable digital preservation in the cloud. 2nd annual conference of the international council on archives, Girona, Spain, 11–15 Oct, 2014. http://www.girona.cat/web/ica2014/ponents/textos/id87.pdf. Accessed 17 May 2017
Bushey J, Demoulin M, McLelland R (2015) Cloud service contracts: an issue of trust. Can J Inf Library Sci 29(2):128–153
Bushey J, Demoulin M, How E, McLelland R (2016) Checklist for cloud service contracts. Final version. InterPARES Trust. http://interparestrust.org/assets/public/dissemination/NA14_20160226_CloudServiceProviderContracts_Checklist_Final.pdf. Accessed 17 May 2017
Davis FD (1989) Usefulness, perceived ease of use, and user acceptance of information technology. MIS Q 13(3):319–340
Donaldson D, Conway P (2015) User conceptions of trustworthiness for digital archival documents. J Assoc Inf Sci Technol 66(12):2427–2444
Duranti L, Rogers C (2012) Trust in digital records. An increasingly cloudy legal area. Comput Law Secur Rep 28(5):522–531
Forrester Research (2011) File storage costs less in the cloud than in-house. Authors: A Reichman with R Whiteley and E Chi. http://media.amazonwebservices.com/Forrester_File_Storage_Costs_Less_In_The_Cloud.pdf. Accessed 19 July 2017
Franks PC, Poloney K, Weck A (2015) Retention and disposition in the cloud executive summary of survey distributed to members of ARMA International February-March 2015 (NA06). InterPARES Trust Research Project
Gartner (2011) Case studies in cloud computing. Analyst: David W. Cearley. http://www.gartner.com/doc/1761616/case-studies-cloud-computing. Accessed 17 May 2017
Gartner (2015) Government CIOs see expected cloud cost savings evaporate. 20 Feb 2015, refreshed 2 Jun 2016 Analysts: N Cannon & G Archer. http://www.gartner.com/doc/2989120/government-cios-expected-cloud-cost. Accessed 17 May 2017
Gartner (2016) Gartner says security will displace costs and agility as primary reason government agencies move to cloud. Press release. http://www.gartner.com/newsroom/id/3187517
Goh E, Sengsavang E (2016) Survey results on the use of cloud services for records management purposes by international organizations. InterPARES Trust Project. http://interparestrust.org/assets/public/dissemination/TR01_20160928_RMinIOs_TRWorkshop7_SurveyReport_Final.pdf. Accessed 19 July 2017
Great Britain. Cabinet Office (2013) Government adopts 'Cloud First' policy for public sector IT. http://www.gov.uk/government/news/government-adopts-cloud-first-policy-for-public-sector-it. Accessed 19 July 2017
Hertzum M et al (2002) Trust in information sources: seeking information from people, documents, and virtual agents. Interact Comput 15(4):575–599
International Data Corporation (2016) Worldwide cloud IT infrastructure spend grew 21.9% to $29.0 Billion in 2015. Press release 8 April 2016. http://www.idc.com/getdoc.jsp?containerId=prUS41176716. Accessed 17 May 2017
InterPARES (1998–2012) International research on permanent authentic records in electronic systems. http://www.interpares.org/. Accessed 17 May 2017
ISO 15489:1 (2016) Information and documentation—records management. Part 1: concepts and principles. International Organisation for Standardisation
Kelton K et al (2008) Trust in digital information. J Am Soc Inf Sci Technol 59(3):363–374
Leverich M, Nalliah K, Suderman J (2015) Historical study of cloud-based services (NA11). InterPARES Trust Research Project. http://interparestrust.org/assets/public/dissemination/NA11_20150109_HistoricalStudyCloudServices_InternationalPlenary2_Report_Final.pdf. Accessed 17 May 2017
Lewicki RJ, Tomlinson EC, Gillespie N (2006) Models of interpersonal trust development: theoretical approaches, empirical evidence, and future directions. J Manag 32:991–1022
MacNeil H (2000) Providing grounds for trust: developing conceptual requirements for long-term preservation of authentic electronic records. Archivaria 50(Fall):52–78
McAllister DJ (1995) Affect- and cognition-based trust as foundations for interpersonal cooperation in organizations. Acad Manag J 38(1):24–59
McLeod J, Gormly B (2015) Economic models for storage of records in the cloud (StaaS)—a critical review of the literature (EU18). InterPARES Trust Project. http://interparestrust.org/assets/public/

dissemination/EU18_20150713_CloudEconomicsLitReview_FinalReport.pdf. Accessed 17 May 2017
McLeod J, Gormly B (2016) Economic models for cloud storage decision-making: an investigation into the use of economic models for making decisions about using the cloud for records storage (EU20). InterPARES Trust Project. http://interparestrust.org/assets/public/dissemination/EU20_20160609_CloudEconomicModels_EUWorkshop8_FinalReport.pdf. Accessed 17 May 2017
Meijer A (2003) Trust this document! ICTs, authentic records and accountability. Arch Sci 3:275–290
Microsoft (2016) Introducing Canada's enterprise-grade hyper-scale public cloud. http://www.microsoft.com/en-ca/web/datacentre/default.aspx. Accessed 7 Aug 2017
National Archives of Australia (n.d.) Cloud computing and information management. http://www.naa.gov.au/records-management/agency/secure-and-store/cloud-computing/index.aspx#section3. Accessed 17 May 2017
New Zealand (2015) Records management and the cloud. Verson 1. http://records.archives.govt.nz/assets/Archives-ResourcesandGuides-Quick-Guides/QUICK-GUIDE-Records-Management-and-the-Cloud-June-2015-final.docx. Accessed 17 May 2017
Oliver G (2014) Digital preservation in the cloud (AA01). InterPARES Trust project. 2nd Annual Conference of the International Council on Archives, Girona, Spain, 11–15 Oct, 2014. http://www.girona.cat/web/ica2014/ponents/ponents/id16.htm. Accessed 17 May 2017
Oliver G, Knight S (2015) Storage is a strategic issue: digital preservation in the cloud. D-Lib 21(3/4). doi:10.1045/march2015-oliver. Accessed 17 May 2017
Oliver G, Chawner B, Liu HP (2011) Implementing digital archives: issues of trust. Arch Sci 11:311–327
Price D, Smith J (2011) The trust continuum in the information age: a Canadian perspective. Arch Sci 11:253–276
Rousseau DM, Sitkin SB, Burt RS, Camerer C (1998) Not so different after all: a cross-discipline view of trust. Acad Manag Rev 23(3):393–404. doi:10.5465/AMR.1998.926617
Sharma SK, Al-Badi AHb, Govindaluri SM, Al-Kharusi MH (2016) Predicting motivators of cloud computing adoption: a developing country perspective. Comput Hum Behav 62:61–69
Stancic H, Bursic E, Al-Hariri A (2015) Ensuring trust in storage in Infrastructure-as-a-Service (IaaS) (EU08). InterPARES Trust Research Project
State Records of South Australia (2015) Cloud computing and records management. Guideline Version 1. http://government.archives.sa.gov.au/sites/default/files/20150706%20Cloud%20Computing%20and%20Records%20Management%20Final%20V1.pdf
Strodl S, Petrov P, Rauber A (2011) Research on digital preservation within projects co-funded by the European Union in the ICT programme. http://cordis.europa.eu/fp7/ict/telearn-digicult/report-research-digital-preservation_en.pdf
Stuart K, Bromage D (2010) Current state of play: records management and the cloud. Rec Manag J 20(2):217–225
Sundqvist A (2011) Documentation practices and recordkeeping: a matter of trust or distrust. Arch Sci 11(3):277–291
Yeo G (2013) Trust and context in cyberspace. Arch Rec 34(2):214–234. doi:10.1080/23257962.2013.825207
Zander O (2014) Preserving 40 terabytes per day. On-premises, cloud … or both? 2nd annual conference of the international council on archives, Girona, Spain, 11–15 Oct 2014

Julie McLeod is Professor in Records Management at the iSchool, Northumbria University, UK. She leads research in the management of digital records and is a member of InterPARES Trust. She teaches postgraduate courses in records management and information governance and received the Emmett Leahy Award for outstanding contribution to the field of information and records management in 2014.

Brianna Gormly is the Digital Initiatives Librarian at Franklin and Marshall College, primarily working in the creation of digital collections, management of the digital repository, and digital preservation. She received a dual Master of Archival Studies/Master of Library and Information Studies (2016) from the University of British Columbia, where she worked as a Graduate Research Assistant for InterPARES Trust.