2017

Core elements in information security accountability in the cloud

Zahir Al-Rashdi
RMIT University

Martin Dick
RMIT University

Ian Storey
RMIT University

DOI: 10.4225/75/5a84e30d95b41
Al-Rashdi, Z., Dick, M., & Storey, I. (2017). Core elements in information security accountability in the cloud. In Valli, C. (Ed.). (2017). The Proceedings of 15th Australian Information Security Management Conference, 5-6 December, 2017, Edith Cowan University, Perth, Western Australia. (pp.125-131).

CORE ELEMENTS IN INFORMATION SECURITY ACCOUNTABILITY IN THE CLOUD

Zahir Al-Rashdi, Dr Martin Dick, Dr Ian Storey
School of Business Information Technology and Logistics, RMIT University, Melbourne, Australia
zahir.al-rashdi@rmit.edu.au, martin.dick@rmit.edu.au, ian.storey@rmit.edu.au

Abstract

This paper proposes 9 core elements of information security accountability in the area of cloud computing. The core elements were determined via a series of 18 case studies with Omani government organisations that were actively using and/or providing cloud computing. 36 interviews were conducted and then analysed using a grounded theory methodology As a result of the analysis, responsibility, transparency, assurance, remediation, accountability support environment, flexible change process, collaboration, mechanisms and commitment to external criteria. The research also found that the emphasis on specific core elements is context-dependent and that there was considerable variation in emphasis amongst the case study organisations.

Keywords: Accountability, Cloud Computing, Information Security, Case Study, Grounded Theory

INTRODUCTION

Cloud computing is growing at a dramatic rate (Weins 2017). Such rapid growth over the past decade, combined with the changes cloud computing can cause in the structure and operations of an organisation means information security needs to be more closely examined. Accountability is a core concern for information security in cloud computing, representing most importantly the trust in service relationships between clients and cloud service providers (CSPs). Without evidence of accountability, there will be a lack of trust and confidence in cloud computing by decision makers and it will be considered as an added level of risk, since a client's essential services will be controlled and managed by a third party. The combination of the two factors of significantly increased usage of cloud computing in the last decade and that this involves an outsourcing arrangement raises the need for improved understanding by organisations of many aspects of the cloud computing relationship. Accountability in information security is an important aspect that needs to be examined in a serious manner. Research in this area of information security for the cloud has also been largely technical in nature and management issues such as accountability have not been examined extensively.

When information security accountability is not present, a lack of trust and confidence in cloud computing often develops among business management (Ko et al. 2011; Muppala, Shukla & Patil 2012; Pearson 2013; Rashidi & Movahhedinia 2012), which is then considered an added level of risk (Cayirci 2013; Gellman 2012; Guitart et al. 2013; Morin, Aubert & Gateau 2012; Rajani, Nagasindhu & Saikrishna 2013). Cloud outsourcing renders the process of maintaining data security and privacy, supporting data and service availability, and demonstrating compliance far less transparent (Rajani, Nagasindhu & Saikrishna 2013).

This paper presents a model of the core conceptual elements that determine information security accountability in cloud computing – a primary concern that represents the trust in service relationships between clients and cloud service providers (CSPs) (Pearson & Wainwright 2013).

BACKGROUND

Past research on cloud computing accountability has produced various definitions, embodying different spheres of accountability research. There is a wide variety of views of accountability among academics and practitioners. Accountability in computer science has been referred to as a limited and imprecise requirement met by reporting and auditing mechanisms (Cederquist et al. 2005; Pearson 2011). Yao et al. (2010) considered accountability the way of making the system accountable and trustworthy via the combination of mechanisms. Muppala, Shukla and Patil (2012) defined accountability as accepting ownership and responsibility towards all actions in a standardized manner, regulated by an acknowledged organisation such as the Organisation for Economic Co-operation and Development (OECD) which published privacy guidelines in 1980. In addition, Rush (2010) defined accountability as the reporting and auditing mechanisms that obligate an organisation to be answerable for its actions.

Ko et al. (2011) considered accountability only one component of trust in cloud computing; the others are security mechanisms (e.g. encryption), privacy (protection of confidential data), and auditability. Similarly, the Galway project on privacy regulators and professionals defined accountability as the safeguarding of personal information, acting as a responsible steward and taking responsibility for protecting, managing and appropriately using that information beyond legal requirements, including being held accountable for any misuse (The Centre for Information Policy Leadership 2009).

The Centre for Information Policy Leadership (2011) also identified accountability in relation to privacy as "the acceptance of responsibility for personal information protection. An accountable organisation must have in place appropriate policies and procedures that promote good practices which, taken as a whole, constitute a privacy management program. The outcome is a demonstrable capacity to comply, at a minimum, with applicable privacy laws. Done properly, it should promote trust and confidence on the part of consumers, and thereby enhance competitive and reputational advantages for organisations" (The Centre for Information Policy Leadership 2011, p. 1).

RESEARCH METHODOLOGY

This research builds on earlier work (Al-Rashdi, Dick & Storey 2015), that detailed a comprehensive review of accountability in relation to cloud computing, via two primary literature sources: academic and professional literature; and industrial reports published by high-profile organisations (e.g. Gartner and Microsoft). More than 450 articles, standards and reports were examined, with the literature revealing four core, interrelated elements of accountability: transparency; responsibility; assurance; and remediation. Accountability is not a 'one-size-fits-all' approach, as each organisation has separate needs, such as those with highly sensitive data.

That research was extended using an interpretive qualitative case study approach. This approach was chosen based on the maturity of this research area, as it was felt that a qualitative approach could be used here to obtain an in-depth understanding or 'very rich' picture of information security accountability in cloud computing – a phenomenon common to the qualitative approach (Kvale 1989). Grounded Theory was the chosen research methodology with case studies used for data collection (Eisenhardt 1989). It should be noted that the extended research was carried out independently from the initial research and that only after both research projects had been completed were comparisons of the results made.

This study was conducted via 18 case studies within Omani government organisations that both use and provide cloud computing. 36 staff (senior and middle managers, information security specialists, regulators, and cloud service providers) with over two years of experience in cloud computing were interviewed via open-ended questions. The interviews were conducted during official working hours in the interviewee's offices, with each session lasting about an hour and half. Over 120,000 words were obtained, with all interview transcripts analysed via an inductive and interpretivist qualitative approach. The specific approach was a Grounded Theory (Strauss & Corbin 1998) methodology that was based on Eisenhardt's approach (Eisenhardt 1989) to using Grounded Theory in case studies. This is a highly accepted variant in the area of grounded theory with over 43,000 citations to the relevant paper on Google Scholar. It adapts grounded theory by focusing specifically on case studies and by also incorporating theory in a compatible way. Analysis was conducted using standard grounded theory methods such as open coding, axial coding and constant comparison. This analysis then led to the coding that has been formalised and presented in this paper. NVivo 11 software (QSR_International 2016) was used as the tool for coding the themes that arose.

CORE ELEMENTS OF INFORMATION SECURITY ACCOUNTABILITY

The goal of this research was to understand what an organisation needs to do to achieve information security accountability in a cloud computing context. It should be noted that this is different from achieving information security, as an organisation considered accountable for information security may still have corresponding breaches. Indeed some aspects of information security accountability such as remediation may never come into play if such a breach does not occur.

In order to determine if an organisation is accountable for its information security, the first step is to determine and define the core elements of information security accountability. Previous research (Al-Rashdi, Dick & Storey 2015) used literature analysis to determine the following four core elements of information security accountability – Assurance, Remediation, Responsibility, and Transparency. The case study research undertaken here, independently found that these four elements were considered by respondents to be core elements in achieving information security accountability. The four elements are defined as follows:

- **Assurance** - a well-founded belief that all relevant actors are complying with governance and ethical measurements, and promoting the implementation of practical mechanisms that support them (The Centre for Information Policy Leadership 2010).
- **Remediation** - "the method by which an organisation provides remedies for those whose privacy has been put at risk" (The Centre for Information Policy Leadership 2010, p. 1).
- **Responsibility** - the acknowledgment and assumption of responsibility by relevant actors that they have introduced or have in place appropriate policies and procedures (Ko, Lee & Pearson 2011).
- **Transparency** – the availability and provision of relevant information in a clear and timely manner to the relevant actors (Pearson & Charlesworth 2009).

Figure1 shows the nine core elements and any sub-elements that make up the element. This model arose out of the analysis of the data collected in the 18 case studies.

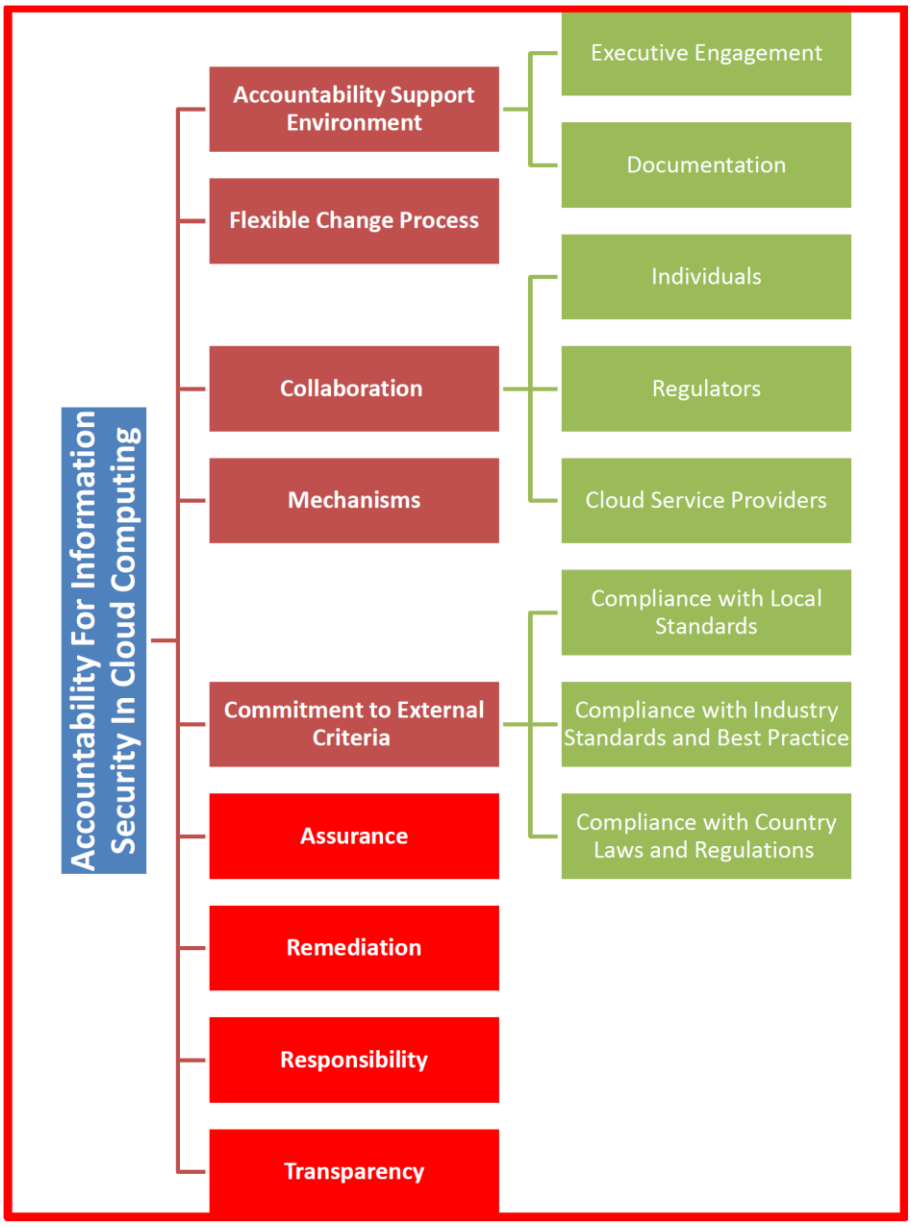

Figure 1: The core elements of information security accountability

As the four core elements of responsibility, transparency, assurance and remediation have been documented individually in the related literature and brought out and described in our earlier work (Al-Rashdi, Dick & Storey 2015) the following sections provide further detail on each of the five new core elements and their sub-elements.

Accountability Support Environment

An Accountability Support Environment in the context of cloud computing is the level of support provided by the organisation in regards to the implementation of accountability and that by providing an environment which supports accounrtability, that the overall level of accountability is increased. The study found that there were two main sub-elements that influenced the level of support of accountability.

- *Executive engagment* is how direct the engagement and follow-up by executives in the development of information security policies. "The executive oversight shows a high level of engagement towards reviewing and re-issuing the implemented policies to match the national or international accepted criteria and country law. This boosts our effort, of information security towards accountability …." Respondents emphasized that fulfilling all of these aspects of compliance, engagement in developing the processes and procedures, and regularly reviewing those policies enhances confidence between CSPs and clients. More confidence then leads to better accountability and minimizes risks.

- *Documentation* is all processes and procedures in information security as a reference for future work, which provides evidence of accountability. A failure to provide documentation leads to significantly reduced accountability according to respondents "It is vital to document all processes and procedures in information security as a reference for future work, which also provides evidence of accountability. Such documentation should keep an up-to-date record of all information security aspects implemented in organizations, with a proper means of implemented solution..".

Flexible Change Process

The respondents were clearly of the opinion that the change process in the context of accountability for cloud computing requires flexibility in relation to altering ICT policies, plans, processes and procedures. The case studies show that the Information Technology Authority supervises the adoption and use of cloud computing by Omani government organisations, but it has worked with them

> *"I can say this terms and conditions applied to change in process, plans and Information Technology Authority policies in the negotiation face within government clients. So overall, that is all based on the outcome revealed from the continued risk assessment used on the customer's site*."

Many respondents emphasized that although ITA policies are comprehensive, plans still need to be tailored to fit specific business needs. Similarly, they pointed out that process changes offered by ITA can allow clients to integrate new protocols that are not addressed by existing ITA policy, e.g. one ministry needing to include health-related security policies into their information security arrangements. An inflexible change policy was considered to not allow organisations to be properly accountable to all their requirements.

A flexible change policy is not without its associated challenges. A typical comment was "*From my experience, there would be some challenges, maybe because of the flexibility in the change process, and there is always conflict between flexibility and security efficiency*."

Collaboration

The third new core element uncovered by the analysis was *Collaboration*. In the context of accountability for information security in the cloud this is primarily about cooperation between the CSP and the organisation. Collaboration ensures that every one of the partners are responsible for their actions and held accountable breaches of regulations. Everything will be transparent and instantly hold a discussion about the non-compliance or breached policies and figure out how to overtake the issue immediately and in cooperation with the client. This ensures the client that the CSP is doing what has been agreed too in the contractual part or assigned SLA. A secondary level of collaboration to achieve accountability is between the organisation and two other entities: regulators and data subjects/and data subjects/individuals.

> *"Compliance and collaboration processes between individuals, business partners and regulators are touching the surface of accountability. In fact, this is part of the selection process that ITA, G-Cloud division is following to filter the government entity according to the list of criteria and standards (local and international) along with applicable law are part of this process."*

By enhancing collaboration, respondents felt that achieving accountability was noticeably easier than situations where collaboration was minimal or non-existent asit built trust between the business partners.

Mechanisms

Mechanisms in the context of information security accountability for cloud computing is the way that cloud service providers assured the clients on how SLA terms and conditions executed in the real world. The assurance on how do the clients trace any breach or non-compliance aspects by ITA as Government Service Provider in Oman. A list of mechanisms has to be established by the organisation and performed in a way that ensures the information security policies and privacy effectively practised and appropriately implemented. The mechanisms might include tools, training and education. The recommended tools might be used to facilitate decision making about appropriate data use and protection, whereas training along with education sessions can be used to identify how to use those tools, and processes. An example of the type of mechanism that needs to be implemented to achieve information security accountability was described by one of the respondents

> *"We do provide the customers with shared service portal. It is a dashboard of the statistics of basically the SLAs and the business process. So it gives the customer that kind of credibility, it tells you very transparently if your SLA and information security policies are right or not. All staff involved in collecting and managing the personal and migrated data is mandatory to commence in training and education session about the use of the portal."*

A failure to put these mechanisms in place undermines information security accountability in the cloud computing context.

Commitment to External Criteria

Commitment to External Criteria in the context of information security accountability for cloud computing is a willingness and capacity to adopt and use organisation-external policies and practices. Such external criteria include local policies (e.g. ITA policies in Oman), industry standards and best practices (e.g. ISO27001, ITIL, CCSK, HIPAA etc.) and government law and regulation (e.g. Oman Electronic Government Architecture Framework (OeGAF) Standard, E-transaction law, privacy law etc.). In the context of information security, failure to commit to these standards indicates a lack of knowledge of the complexity of information security and the inability of any one organisation to be able to deal with the wide and varied threats in the area. As one respondent indicated:

> *"organisations must implement policies connected to appropriate external criteria that can be found in the country law, or industry best practices to protect the information migrated to cloud and privacy of individuals and business partners."*

An organisation that does not adopt and use these external criteria as a reference point is not seen by the respondents as being accountable for information security. Compliance with these external criteria was seen as very important - *"We are not tolerant with vendors/suppliers and individual users for non-compliance."*

THE IMPORTANCE OF CONTEXT

Achieving information security accountability is a complex task for any organisation. The first step is to understand what are the elements that make up information security accountability. It is important to realize that though there are nine elements, the level at which any specific element needs to be driven to is highly context dependent. A level of transparency for one organisation that provides an acceptable level of accountability, may be totally inadequate for another organisation.

It should be noted that the types of organisation that were in the case studies have many similarities. They are all Omani government departments with a high need for data security to protect highly sensitive government data, large complex business processes, and significant infrastructure. This will to some extent hide the requirements for variation in the level of emphasis on specific elements of information security accountability that a more diverse set of case studies might have discovered. But even within this set of case studies, the elements have significant variation. As an example, some of the case studies use private cloud to ensure accountability due to the nature of their requirements, others are able to use private cloud providers while others are satisfied with the government cloud provider.

Overall, it needs to be understood, that the nine element model is not prescriptive and that it must be used in a context-sensitive way that is dependent on the needs of the specific organisation that is attempting to achieve information security accountability.

CONCLUSION

This paper has sought to understand how accountability in cloud computing can be conceptualised. The wide range of existing research into accountability in cloud computing has used a technical approach and has been quantitative, and has generally not addressed the conceptual issues. The enormous growth in moving businesses to cloud computing, mainly due to its flexibility, cost-effectiveness and scalability, and the corresponding absence of a specific cloud computing accountability framework, highlights the growing need for research in this area. Previous research used an extensive analysis of the literature relating to cloud computing and accountability for information security to develop a model of the key conceptual elements (transparency, responsibility, assurance and remediation) relating to this issue. A set of 18 interpretive qualitative case studies were then conducted to examine the situation independently of the literature. A series of interviews were conducted within 38 interviewees from different government entities. Five more key elements were identified from the conducted case studies that are necessary to achieve information security accountability. These were found to be: *accountability support environment*, *flexible change process*, *mechanisms*, *collaboration*, and *commitment to external criteria*.

The findings of this research contribute to the growing awareness of the importance of accountability.It provides an understanding of the importance of the accountability elements that policymakers need to address in cloud computing projects if they wish to be accountable in terms of information security. In future this research is aiming to produce a holistic and heuristic accountability framework that enables a theoretical-based description and analysis of the gap that exists between the ideal and the actuality of the institutional and technical environments of cloud computing implementation in regards to accountability. Finally, this research is seeking to find ways to strengthen the trust and confidence between organisations that have adopted the cloud and CSPs, which in turn strengthen the accountability, which also helps to reduce risks connected to the adoption of cloud computing services.

REFERENCES

Al-Rashdi, Z, Dick, M & Storey, I 2015, 'A Conceptual Framework for Accountability in Cloud Computing Service Provision', *Australasian Conference on Information Systems*.

Cayirci, E 2013, 'A joint trust and risk model for MSaaS mashups', paper presented to Proceedings of the 2013 Winter Simulation Conference: Simulation: Making Decisions in a Complex World.

Cederquist, J, Conn, R, Dekker, M, Etalle, S & den Hartog, J 2005, 'An audit logic for accountability', paper presented to Policies for Distributed Systems and Networks, 2005. Sixth IEEE International Workshop on.

Eisenhardt, KM 1989, 'Building theories from case study research', *Academy of management review*, vol. 14, no. 4, pp. 532-50.

Gellman, R 2012, 'Privacy in the clouds: risks to privacy and confidentiality from cloud computing', paper presented to Proceedings of the World privacy forum.

Guitart, J, Macias, M, Djemame, K, Kirkham, T, Jiang, M & Armstrong, D 2013, 'Risk-driven proactive fault-tolerant operation of iaas providers', paper presented to Cloud Computing Technology and Science (CloudCom), 2013 IEEE 5th International Conference on.

Ko, RK, Jagadpramana, P, Mowbray, M, Pearson, S, Kirchberg, M, Liang, Q & Lee, BS 2011, 'TrustCloud: A framework for accountability and trust in cloud computing', paper presented to Services (SERVICES), 2011 IEEE World Congress on.

Ko, RK, Lee, BS & Pearson, S 2011, 'Towards achieving accountability, auditability and trust in cloud computing', in *Advances in Computing and Communications*, Springer, pp. 432-44.

Kvale, SE 1989, *Issues of validity in qualitative research*, Studentlitteratur.

Morin, J, Aubert, J & Gateau, B 2012, 'Towards cloud computing SLA risk management: issues and challenges', paper presented to System Science (HICSS), 2012 45th Hawaii International Conference on.

Muppala, J, Shukla, D & Patil, S 2012, 'Establishing Trust in Public Clouds', *J Inform Tech Softw Eng*, vol. 2, p. e107.

Pearson, S 2011, 'Towards accountability in the cloud', *Proc. IEEE Internet Computing*, pp. 64-9.

---- 2013, 'Privacy, security and trust in cloud computing', in *Privacy and Security for Cloud Computing*, Springer, pp. 3-42.

Pearson, S & Charlesworth, A 2009, 'Accountability as a way forward for privacy protection in the cloud', in *Cloud computing*, Springer, pp. 131-44.

Pearson, S & Wainwright, N 2013, 'An interdisciplinary approach to accountability for future internet service provision', *International Journal of Trust Management in Computing and Communications*, vol. 1, no. 1, pp. 52-72.

Rajani, B, Nagasindhu, K & Saikrishna, K 2013, 'Integrity Verification & Distributed Accountability in High Performance Distributed Clouds', *International Journal Of Electronics Communication And Computer Engineering*, vol. 4, no. 6.

Rashidi, A & Movahhedinia, N 2012, 'A model for user trust in cloud computing', *International Journal on Cloud Computing: Services and Architecture (IJCCSA)*, vol. 2, no. 2, pp. 1-8.

Rush, B 2010, *The Best Practices Act of 2010 and Other Privacy Legislation,2010*, <https://www.govtrack.us/congress/bills/111/hr5777

Strauss, A & Corbin, J 1998, 'Basics of qualitative research: techniques and procedures for developing grounded theory'.

The Centre for Information Policy Leadership, T 2009, *"Galway Project Plenary session Introduction"* US.

The Centre for Information Policy Leadership , T 2010, *Demonstrating and Measuring Accountability - The Accountability Project – Phase II Paris, France*, France.

---- 2011, *Getting Accountability Right with a Privacy*

Management Program Hunton & Williams LLP, Washington, DC.

Weins, K 2017, 'Cloud Computing Trends: 2017 State of the Cloud Survey'.

Yao, J, Chen, S, Wang, C, Levy, D & Zic, J 2010, 'Accountability as a service for the cloud', paper presented to Services Computing (SCC), 2010 IEEE International Conference on.