Government Information Quarterly xxx (xxxx) xxxx

Contents lists available at ScienceDirect

Government Information Quarterly

journal homepage: www.elsevier.com/locate/govinf

Assessing information security risks in the cloud: A case study of Australian local government authorities

Omar Ali[a,*], Anup Shrestha[b], Akemi Chatfield[c], Peter Murray[b]

[a] American University of the Middle East, Block 6, Street 250, Egaila, Kuwait
[b] University of Southern Queensland, West Street, Toowoomba, Qld 4350, Australia
[c] University of Wollongong, Northfield Ave, Wollongong, NSW 2522, Australia

ARTICLE INFO

Keywords:
Information security requirements
Cloud computing
Structural equation model
Adoption
Local governments

ABSTRACT

Cloud computing enables cost-effective and scalable growth of IT services that can enhance government services. Despite the Australian Federal Government's 'cloud-first' strategy and policies, and the Queensland State Government's 'digital-first' strategy, cloud services adoption at local government level has been limited—largely due to data security concerns. We reviewed the ISO 27002 Information Security standard with extant literature and found that operational security, individual awareness and compliance matters pose more significant government challenges than the often-highlighted technical and process-oriented cloud security requirements. This study identifies and explores the critical factors associated with information security requirements of cloud services within the Australian regional local government context. We conducted 21 field interviews with IT managers, and surveyed 480 IT staff from Australia's 47 regional local governments. We propose a conceptual cloud computing security requirements model with four components – data security; risk assessment; legal & compliance requirements; and business & technical requirements – in order to promote a balanced view on cloud security for governments. Using this model, governments can work together to demand uniform security requirements for adopting cloud services.

1. Introduction

The key purpose of this research paper is to identify and explore the critical factors relating to information security requirements of cloud services within the Australian regional local government context. Companies across disparate sectors are willing to learn about or utilize cloud computing service models if tighter security can be achieved (CSA, 2010). As such, research has been conducted on the probability of privacy threats, the potential effects of security breaches, security resources, data access audits and user trustworthiness (Kresimir & Zeljko, 2010). Three categorizations of threats were noted as a result: security governance; technology; and cloud attributes (Grobauer, Walloschek, & Stöcker, 2010). The realization of these threats to cloud computing advances suggests that tighter security is vital (Atanassov, Gurov, & Karaivanova, 2012; Lagesse, 2011; Poolsappasit, Kumar, Madria, & Chellappan, 2011; Tan & Ai, 2011). To ensure safe availability and greater security, cloud service providers (CSPs) must, inter alia, improve backup implementation and regularity, tighten accessibility and enhance encryption schemes (Harauz, Kauifman, & Potter, 2009).

Despite some breaches in security, CSPs proclaim secure and efficient technology for their cloud infrastructure (Bhagawat & Kumar, 2015). However, breaches of security have often occurred in very large companies. For instance, in 2009 Amazon faced two different cases of security breaches where networks were temporarily terminated (Kanthe & Patel, 2015) while using a simplified storage system. Other high-profile cases include Google Docs in March 2009 where information was compromised and the system faced a 4-h freeze globally. Similarly, an approximate 22-h interruption resulted when Microsoft Azure's cloud computing experienced similar issues. This is in addition to a May 2009 incident when Apple Mac VMware virtualization software was illegally accessed (Kanthe & Patel, 2015).

Very few studies have explored cloud security links at an organizational level (Wang & Mu, 2011). As a result, extant research related to a cloud-based service model has tended to investigate the technical and operational issues (Venters & Whitley, 2012; Yang & Tate, 2012), as distinct from the security issues of cloud computing. Some studies have explored cloud service adoption from an organizational perspective related to security breaches (Grispos, Glisson, & Storer, 2013; Nkhoma

* Corresponding author at: College of Business and Administration, American University of the Middle East, Egaila, Kuwait.
E-mail addresses: Omar.Ali@aum.edu.kw (O. Ali), Anup.Shrestha@usq.edu.au (A. Shrestha), akemi@uow.edu.au (A. Chatfield), Peter.Murray@usq.edu.au (P. Murray).

https://doi.org/10.1016/j.giq.2019.101419
Received 23 January 2019; Received in revised form 30 September 2019; Accepted 1 October 2019
0740-624X/ © 2019 Elsevier Inc. All rights reserved.

& Dang, 2013; Trigueros-preciado, Perez-gonzalez, & Solana-gonzalez, 2013) but these have been relatively few. Here, and consistent with the study's aims, we address the gaps in cloud security within a local government context.

The research team has adopted a case study approach to explore and examine the requirements related to the security of cloud-based solution within a local government context. The main focus of Local governments (represented by regional councils in Australia) is service deliverables for their ratepayers. These include a focus on driving efficiency, improved service delivery and enhancing the end user service experience (LGAQ, 2013). To meet these objectives, local governments can provide critical information related to identifying service-oriented solutions to improve their performance (Scupola, 2003). Cloud computing has the capacity to enhance government services. In 2014, the Australian Government announced a cloud-first focus for the nation through the publication of the Australian Government Cloud Policy (Australian Government Department of Finance, 2014). The stated goal of this specific policy was that "*The Australian Government will be a leader in the use of cloud services to achieve greater efficiency, generate greater value from ICT investment, deliver better services and support a more flexible workforce*" (Australian Government Department of Finance, 2014). Through this policy, the government aimed to strengthen the nation's IT infrastructure through cloud architecture (Vault, 2014). However, the nation's 'cloud first' policy has clear gaps, namely, the lack of a clear plan and specific goals (Foo, 2014). In, 2017, the Queensland Government published its Digital 1st Strategy for, 2017–2021, with its main foci on '*technology*', '*standard operating environments*', and '*software as a service and cloud computing*' (Queensland Government, 2017). Also, through its Digital 1st Strategy, the Queensland Government promoted new developments such as software operating systems that used cloud-based data centres, since this type of software was seen to significantly enhance security, and reduce operating costs.

Cloud-based service has specific potential in Australian regional communities which experience more extreme social and economic pressures compared to cities as a result of government and businesses withdrawing their services (Baxter, Hayes, & Gray, 2011). In many remote areas, certain services such as employment services and telecommunication services (among others) are not available, or are available at significantly higher cost and inferior quality than in urban locations (Asthana, 2003; Baxter et al., 2011). Advanced technologies, and in particular cloud-based solution technology, will help in improving access to services in a cost-effective and timely manner. Also, this advanced technology has enabled government to deliver superior services to its customers (citizens). For example, the US General Services Administration uses cloud computing at the federal, state and local government level (Marston, Li, Bandyopadhyay, Zhang, & Ghalsasi, 2011; Sivarajah, Irani, & Weerakkody, 2015); and cloud application in e-government and e-voting systems (Zissis & Lekkas, 2011).

The shortfall in empirical studies, including a lack of understanding and development of the cloud-based solution model, appears to be the key reason for the lack of cloud-based solution adoption within the local government sector (IT Industry Innovation Council, 2011). Cloud technology has been more widely adopted within urban Australia than regional Australia (IT Industry Innovation Council, 2011), prompting greater investigation into the issues of security that are relevant to local governments in order to guide future decision-making (IT Industry Innovation Council, 2011). Accordingly, the limited studies in this research area have prompted the following research question: *What are the main critical factors required to address the information security requirements of cloud-based solution adoption within the Australian regional local government context?*

This research paper is organized as follows. Firstly, the paper provides in-depth details on the research topic. Secondly, it explores relevant literature related to security, cloud computing, and the international standards organization. Thirdly, the paper outlines the methodology used in the research for the data collection. Fourthly, the paper presents the qualitative study findings, then shows the development of the conceptual framework as a basis for, the quantitative study that includes the findings of structural equation model (SEM) based on the data. Finally, the paper discusses the results and implications for further research, including implications for local governments.

2. Literature review

2.1. Cloud computing

Cloud computing refers to a model of computing where machines in large data centres can be dynamically provisioned, configured and reconfigured to deliver services in a scalable manner (Wyld, 2009). It allows for highly scalable computing applications with CSPs offering a variety of services to individuals, companies, and government organizations. Users employ cloud computing for storing and sharing information, remote access, database management, data mining and deploying web services (Hand, 2007). Cloud computing is seen as revolutionary in terms of its impact on technological innovation and economic growth (Price, 2011).

The U.S. National Institute of Science and Technology (NIST) suggests that the cloud service model promotes availability and is composed of five different essential characteristics: on-demand self-service; resource pooling; broad network access; measured service; and rapid elasticity (NIST, 2009). Cloud-based solutions are typically run as one of three service models: 1) Software as a Service (SaaS); 2) Platform as a Service (PaaS); and 3) Infrastructure as a Service (IaaS) (PopMell & Grance, 2009). According to scholars, there are four major cloud deployment models—public, private, hybrid, and community cloud (Dillon, Wu, & Chang, 2010; Takabi, Joshi, & Ahn, 2010; Zhang, Cheng, & Boutaba, 2010a).

Cloud computing technology has many benefits to organizations such as increasing productivity and effectiveness in business and IT processes, and in the reduction of costs while procuring and maintaining minimal IT infrastructure (Ali, Soar, & Shrestha, 2018; Chen & Zhao, 2012; Liang, Qi, Wei, & Chen, 2017). Organizations that have sensitive data are increasingly confident in managing their applications and data using cloud computing systems (Chen & Zhao, 2012; Pee & Kankanhalli, 2016).

2.2. Security in cloud computing

Security has been defined as "*the quality or state of being secure or to be free from risk*" (Whitman, 2012, p. 12). Security is one of the significant issues for organizations, in particular government agencies that have very sensitive data (Behl, 2011; Jensen, Schwenk, Gruschka, & Iacono, 2009; Julisch & Hall, 2010; Pearson, 2009; Ramgovind, Eloff, & Smith, 2010). Security is tightly linked to legislative and technical components in regards to ensuring data protection (Janssen & Joha, 2011; Paquette, Jaeger, & Wilson, 2010; Subashini & Kavitha, 2011). This comprises many disparate aspects, for example, monitoring user identity, access to software security and security of online data where there may be a merge of stored information (Krumm, 2008; Pearson, 2009; Pearson & Benameur, 2010). Cloud computing is designed to share information, particularly where data is transferred and stored. However, security issues highlighted in previous research (Chen & Zhao, 2012; Janssen & Joha, 2011; Krumm, 2008; Mahmood, 2011; Pearson, 2009; Pearson & Benameur, 2010; Zissis & Lekkas, 2012) hinder cloud adoption, particularly when very sensitive data such as citizen information are being stored. The CIO research conducted in the U.S. by Subashini and Kavitha (2011) has revealed that the loss of rights in controlling data, availability of data, and compliance with IT governance and regulations has led to security issues in cloud computing. Also, a research conducted by Heiser and Nicolett (2008) has reported that issues related to risk management, such as those related to

ARTICLE IN PRESS

compliance with regulations, and audit, need to be resolved. These security issues are the one of the significant barriers to the introduction of cloud computing in public entities (Choi & Lee, 2015).

Previous studies define cloud service security as threats, vulnerabilities and protection of cloud operational services and software as a service application (Cebula & Young, 2010; Liu, Yu, & Mylopoulos, 2003; Mather, Kumaraswamy, & Latif, 2009; Zhang, Cheng, & Boutaba, 2010). A research conducted by Liu et al. (2003), has proposed framework for analyzing security requirements. Mather et al. (2009) provides a detailed definition and description on different cloud security issues. Zhang et al. (2010) provide review of the cloud computing and explain the research challenges associated with security. However, they only provide an overview of important security challenges but do not provide a full detailed solution on cloud security. Cebula and Young (2010) further classify cloud security and its implementation into two major groups: the first group is software acquisition security (which includes the security specifications in all processes to buy, rent, or interchange software to use in an enterprise); the second group is systems and software development security (which include the security specifications in all processes to develop information systems). However, there is no clear framework to be adopted to classify security requirements and then to feed towards implementation.

Although there are many advantages to cloud services (Aljabre, 2012; Marston et al., 2011), security in cloud remains a major concern (Chen & Zhao, 2012; Jansen, 2011; Leuprecht, Skillicorn, & Tait, 2016). Results from a comprehensive industry survey (IDCI, 2009) showed that 74% of participants (e.g. IT managers) highlighted that security is a major reason behind the low level of adoption of the cloud computing service model (Bhagawat & Kumar, 2015). Also, this finding is supported by other survey results conducted by Gartner (2009), where over 70% of CTOs cited security as the major contributing factor for the lack of utilization and adoption of cloud technology (Chen & Zhao, 2011). However, there is no clear framework to follow from security requirements. The significance of a clear framework suggests that a more holistic approach of offering an integrated solution and multi-layered security is required (Chang & Ramachandran, 2016).

2.3. Information security requirements for cloud computing

Cloud-based solutions have been a challenge in terms of security issues (Leuprecht et al., 2016). The International Standards Organization (ISO) published a reference model as the ISO 7498-2 Standard in 1989 (ISO, 1989) that provides a foundation for security architecture needed in information processing systems (Ramgovind et al., 2010). The security services and related mechanisms provided in this standard are still relevant to today's cloud computing technical security challenges (Eloff, Eloff, Dlamini, & Zielinski, 2009). Furthermore, the 2005 release of the ISO27000 family of information security standards formally recognized the need for a holistic view of information security that extends the technology dimension to include people and process dimensions. According to ISO (2013), the ISO 27001 standard includes policies and procedures for legal, physical and technical controls to manage information risks within an organization. An information and security management system encapsulate these procedures. This standard promotes a risk-based management approach that is technology-neutral, but does not enforce specific security controls. The ISO 27002 standard builds on ISO 27001 where a number of information and security control objectives work in tandem with good practice security controls relevant to all organizations.

ISO 27002 (ISO, 2013), for instance, suggests that an organization needs to identify its security requirements from three sources: risk assessments; legal and contractual requirements; and business and technical requirements for information processing (see Fig. 1). While the ISO 27002 standard applied to cloud-based services, a new set of guidelines specific to information security controls for cloud-based solution were then published as ISO/IEC 27017 (ISO/IEC, 2015).



Fig. 1. ISO 27002 standard.

However, ISO/IEC 27017 does not replace the ISO/IEC 27002 controls for cloud-based services, but provides additional controls that specifically relate to cloud computing. We apply these guidelines to the three security requirements (see Fig. 1) underpinning this research.

As represented in Fig. 1, the unique element of risk assessment in cloud-based solution relates to the operational security and monitoring of cloud services. Security assessments are important mechanisms for risk mitigation from cloud security breaches using an information and risk management framework (Zhang, Wuwong, Li, & Zhang, 2010). While there is a good understanding of cloud-associated risks and necessary controls, the risk mitigation practices are not mature enough for wide scale adoption (Brender & Markov, 2013). Similarly, the major difference in legal and contractual security requirements for cloud computing is the agreement of shared responsibility between CSPs and customers. In terms of security control in the cloud, it is a common fallacy that the CSP is in charge of security around the cloud environment. While CSPs have security controls in place, there is little point if the customers who access cloud services do not have adequate protection for their networks, users or applications. In fact, most of the security control issues arise at the client level, thereby prompting cloud providers to look for shared responsibilities for security (Liu, Sun, Ryoo, Rizvi, & Vasilakos, 2015). Several IT compliance models are viable in addressing the security challenges and issues in the cloud. Kalaiprasath, Elankavi, and Udayakumar (2017) presented recommended security compliance models for each recognized type of security threat. For example, compliance models from PCI DSS, ISO 27001, HIPPA, SOX, and NIST 800-61 to ISO 17799 address issues related to denial of services. As shown in Fig. 1, business and technical requirements for information security in cloud computing deal with unique environments in which cloud services deliver value to customers. From the CSP's perspective, key requirements for information security relate to asset management (such as removal of cloud services customer assets), and access control (e.g., segregation of virtual computing environments and virtual machine hardening) (Subashini & Kavitha, 2011). From the cloud service consumer's perspective when using cloud to deliver services to their end customers, there are technical challenges in terms of secure data storage and transmission. Theoretically, recent developments in encryption techniques have confirmed that secure cloud communications are possible. However, there are challenges in practice because of the complexity embedded within cloud environments (Ren, Wang, & Wang, 2012). Another area of concern is trustworthiness between service providers and clients. For example, managing service level agreements that promote continuous monitoring towards adaptive trust management (Li & Du, 2013) are a key feature of efforts to build trust.

Cloud computing growth has slowed due to the challenges

ARTICLE IN PRESS

Table 1
Interviewee details.

Interviewee code	Job title	Experience in Years		Council's classification	Council's size
		IT	Cloud computing		
C25-RTM	IT Network Manager	10	2	Rural remote	Medium
C61-URM	IS Coordinator	9	1.5	Urban regional	Medium
C53-RTL	IT Coordinator	14	3	Rural remote	Large
C18-URS	IT Coordinator	5	6 months	Urban regional	Small
C15-RAL	IT Manager	20	5	Rural agricultural	Large
C52-UFM	IT Manager	21	4	Urban fringe	Medium
C55-URS	Technical Director	7	2	Urban regional	Small
C45-RAV	IT Manager	9	3	Rural agricultural	Very large
C19-RTL	Technical Director	10	1	Rural remote	Large
C68-URL	Manager of the ICT Branch	12	2	Urban regional	Large
C28-URS	ICT Coordinator	10	6 months	Urban regional	Small
C21-RTX	IT Officer	15	4	Rural remote	Very small
C74-RTM	IT Manager	14	3	Rural remote	Medium
C39-URM	Information Services Manager	12	1	Urban regional	Medium
C11-RAV	IT Manager	40	5	Rural agricultural	Very large
C34-UFV	Enterprise Architecture Manager	6	5 months	Urban fringe	Very large
C16-RAL	Information Services Manager	5	9 months	Rural agricultural	Large
C7-RTS	IT Consultant	20	4	Rural remote	Small
C40-UDV	Chief Information Officer	30	5	Urban development	Very large
C42-URL	Team Leader ICT Operation	15	4	Urban regional	Large
C72-URS	IT Manager	10	9 months	Urban regional	Small

surrounding data security and privacy (Fernandes, Soares, & Gomes, 2014). Several security components form the structure of security systems, such as components of confidentiality, integrity, and availability (Algirdas, Jean-Claude, Brian, & Carl, 2004). These security components can be categorized as hardware and software resources and data (Zissis & Lekkas, 2012). Confidential information is contained within company boundaries in conventional models and adheres to security with respect to staffing, access and logistical organization (Knapp et al. 2010). Data is stored externally of company boundaries in cloud computing models at the location of the provider. Therefore, it is the CSP's obligation to confirm security aspects that have been addressed in terms of staff access, leakage and management of security. Consequently, tight encoding and strict authorization to manage information is necessary (Subashini & Kavitha, 2011).

Difficulties and specific risks need to be determined in order to confirm the security of an information system (IS). Once determined, the necessary amendments need to be enforced (Zissis & Lekkas, 2012). As such, privacy requirements and management are applied to the standard systems engineering process so as to assimilate the security measures with IS operational functions and other system aspects such as maintenance (Stine, Kissel, Barker, Fahlsing, & Gulick, 2008). Numerous security benefits are brought about by cloud computing owing to its structure and features. These consist of wide availability, division of information, superfluity and tighter protection (Zissis & Lekkas, 2012).

3. Research methodology

In this research study, we adopted a sequential mixed approach. Mixed research methods are considered more useful than any single research method, and this study will result in significant theoretical contributions (Greene & Caracelli, 1997). Mixed research methods have the capacity to cover exploratory and confirmatory research questions simultaneously (Teddlie & Tashakkori, 2009; Venkatesh, Brown, & Bala, 2013). Using a mixed method requires the researcher to view the research from different sides such as the diversity, variability, and correspondence (Johnson & Onwuegbuzie, 2004). For example, the researcher may use different interview techniques (qualitative approaches) and different survey techniques (quantitative approaches) to collect specific data related to a new ISs adoption. In social sciences, both methods of research have been used as they result in a better assessment and learning of research (Punch, 1998; Walsham, 2006).

The design of a mixed research approach usually begins with a qualitative method followed by quantitative method (Bhattacherjee & Premkumar, 2004; Morgan, 1998; Sale, Lohfeld, & Brazil, 2002; Venkatesh et al., 2013; Walsham, 2006). An exploratory research approach would provide the potential for dynamic adaptation to consider various options for discussion with participants (Teddlie & Tashakkori, 2009; Venkatesh et al., 2013). Quantitative research is the predominant methodology used in management and business research studies (Hanson & Grimmer, 2005). A quantitative method is applied as formal surveys containing planned queries. A quantitative approach generates a large number of participants for statistical significance and generalization of the research findings to the population of interest (Duffy & Chenail, 2008). Accordingly, IS researchers have promoted the use of mixed methods for stronger validity and reliability (Chang, 2006; Dennis & Garfield, 2003; Grimsley & Meehan, 2007; Hackney, Jones, & Losch, 2007; Johnson, Onwuegbuzie, & Turner, 2007; Soffer & Hadar, 2007). Given that the use of mixed research techniques can generate countless approaches for a variety of phenomena, the researchers adopted this approach for this study. Therefore, our study 1 is based on qualitative inquiry from interviews with relevant stakeholders. This data helped develop the conceptual research model. It also guided the development of the study 2 quantitative survey to refine and confirm our research model.

We now turn to Study 1 to explore the broad research question stated earlier. That is, what are the main critical factors required to address the information security requirements of cloud-based solution adoption within the Australian regional local government context?

3.1. Study 1: Qualitative investigation

In-depth interviews were conducted with 24 local government staff members in senior management positions. Table 1 illustrates all details related to the job title of interviewees, their years of experience related to IT in general and in cloud computing specifically, and council's classification and size.

Interviewees were chosen to represent IT decision-makers in Queensland local governments. They also represented regional local governments from a geographical and size classification perspective. Participants were selected from 77 different Queensland local government councils. According to the Local Government Association of

ARTICLE IN PRESS

Table 2
Councils' geographical area and size classification.

Geographical segments	Size classification					Total	%
	Very small	Small	Medium	Large	Very large		
Coastal	0	1	1	2	1	5	23.8%
Resource	0	1	0	2	0	3	14.3%
Indigenous	0	2	1	0	0	3	14.3%
Rural/Remote	1	1	2	1	1	6	28.6%
South East Qld	0	0	1	1	2	4	19.0%
Total						21	100%

Table 3
Councils' cloud adoption stages.

Segments	Cloud-based solution adoption stages		
	Not Adopted	Some Adoption	Full Adoption
Coastal	3	1	1
Resource	1	1	0
Indigenous	4	0	0
Rural/Remote	5	1	0
South East Qld	0	2	2
Total	13	5	3
Percent	62%	24%	14%

Queensland (LGAQ) (2013), the 77 Queensland local governments were classified into five different geographical segments. For more details about geographical areas and size classification of the chosen local governments see Table 2.

The main motivation behind using these specific segments is to investigate those segments that have an effective telecommunication infrastructure base to adopt cloud-based solution and to understand their adoption decision. Table 3 shows the local councils' cloud-based solution adoption stages. The table demonstrates that 62% of participating local councils did not adopt cloud-based solution; while 24% of the research participant councils have some cloud-based solution adoption. Only 14% of the participating councils have full adoption of cloud-based services. This illustrates that most of the participating councils experienced cloud challenges. For more details about cloud-based solution adoption stages of the chosen local governments, see Table 3.

The key purpose of the exploratory stage (study 1) of this research was to investigate gaps in the literature review noted earlier and to measure the information security requirements of cloud computing. This exercise was also useful to refine the conceptual research model (Myers & Avison, 1997; Venkatesh et al., 2013). Finally, this exploratory stage was very helpful in identifying possible measurement items that we used to measure factors for cloud computing security (Zikmund, Babin, Carr, & Griffin, 2012).

3.1.1. Data collection

The data collection in this research included a specific interview protocol. This helped to establish a rapport between the researcher and the interviewees (Gaskell, 2000). Open-ended questions were created in order to allow in-depth answers and clear discussions portraying personal opinions of the research topic (Carson, Gilmore, Perry, & Gronhaug, 2001). The interview protocol involved probing questions that encouraged participants to elaborate on their own areas of interest and expertise during the duration of the interviews—which lasted 30 to 50 min. The total number of probing questions increased as more information was collected (Carson et al., 2001). Five central questions formed the foundation of the interview. Having outlined the duties of their position in the first question, the second question sought to elicit details of their educational background and their skills and comprehension associated with cloud computing. Participants were then questioned to obtain information related to number of years' experience and workforce capacity, along with their understanding of cloud computing. In the fourth question, interviewees were requested to identify the main critical factors for security requirements when considering cloud computing adoption. The fifth question concerned descriptions of specific security impacts on cloud computing adoption. The interview design and approach allowed the interviewer to explore and follow up the responses. Although 24 interviews were conducted for the purpose of this research, 21 interviews were considered sufficient for participant reliability.

3.1.2. Data analysis

Based on each of the research questions listed earlier, manual content analysis was conducted to analyse the data (Miles, Huberman, & Saldana, 2014). Three steps were followed in the analysis: data minimization, data display, and confirmation of results (Hsieh & Shannon, 2005; Miles et al., 2014). Each individual interview was transcribed immediately after completion of the interview; interview data was then used to draw up conclusion tables for each participant (Rao & Perry, 2007). These consisted of central themes consistent with a critical realist approach of lived experiences of the research participants in relation to the security questions under investigation. Data was then organized in to a thematic conceptual analysis similar to that proposed by Miles et al. (2014). By ordering the data into themes, it was then possible to address the main concerns and issues from the responses to each research question. Subsequently, data was then recorded as a final summary (Patton, 2002; Schilling, 2006). Codes for the interview data were then devised, followed by arranging the information categorically and sequentially in order to identify findings and necessary paths of action (Miles et al., 2014).

3.2. ***Study 2***: *Quantitative questionnaire*

The research instrument designed to explore the hypotheses was a questionnaire related to low cost delivery, flexible design options, and shorter time for collecting data (Fan & Yan, 2010; Zikmund et al., 2012; Zikmund, Babin, Carr, & Griffin, 2013). We called this Study 2. The survey is an adaptable instrument (Zikmund et al., 2013) affected by certain traits of the respondents, including qualities, knowledge, inspiration, and disposition (Robson, 2002). The emergent literature gaps and the exploratory data from the qualitative approach (study 1) comprised the development of the questionnaire instrument (Song, Van Der Bij, & Weggeman, 2005). The purpose of the questionnaire was to test the measurement framework and the structural model of the research conceptual framework. Due to its easy access, an online survey was chosen to maximise the likelihood of success in collecting the data.

3.2.1. Data collection

The survey was distributed online to Queensland's 77 councils through the University of Southern Queensland (USQ) Custom Survey System. IT Managers from 47 regional local governments responded to the survey which represented a response rate of 61%. The participating 47 regional local governments had approximately 786 IT staff who were invited to participate and 480 responded. The survey provider ensured 24/7 access to the survey and a link was provided to the respondents over a three-month period.

To identify the main critical factors necessary to measure the information security requirements of cloud computing adoption, a 7-point Likert scale was adopted, with 1 referring to 'strongly disagree' and 7 referring to 'strongly agree'. An essential component in implementing a questionnaire is the process of conducting a pilot study in order to develop its clarity and effectiveness (Shaughnessy, Zechmeister, & Zechmeister, 2012). A pilot study of this research was tested on participants with similar demographic backgrounds and in similar settings to the intended respondents of the final questionnaire (Shaughnessy et al., 2012). The first form of the research questionnaire

ARTICLE IN PRESS

Table 4
Pilot Study Results.

Factors	Total Correlation	Squared Multiple Correlation	Mean	Std. Deviation	Cronbach's Alpha of each Item
Risk Management	0.662	0.502	4.93	1.005	0.743
Security Control	0.872	0.433	5.85	1.216	0.855
Awareness	0.945	0.862	4.12	0.853	0.902
Data Transmission	0.552	0.352	5.44	1.281	0.912
Data Storage	0.790	0.634	5.12	1.033	0.894
Data Privacy	0.823	0.768	5.17	1.029	0.892
Government Regulation	0.746	0.588	4.78	1.378	0.897
Compliance	0.705	0.516	5.11	0.998	0.814
Backup	0.564	0.371	5.83	0.790	0.909
Encryption	0.799	0.756	5.01	0.985	0.813
Trustworthiness	0.535	0.451	5.80	0.759	0.910
Redundancy	0.707	0.735	4.70	1.279	0.900
Service Level Agreement (SLA)	0.645	0.590	4.89	0.906	0.776

was adjusted following feedback from university staff and regional local government managers. The pre-study was effective in highlighting problems and advancing the survey structure (Waters, 2011; Wholey, Hatry, & Newcomer, 2004). The survey was then pilot tested for the purpose of testing the reliability of the conceptual research model instrument items (Shaughnessy et al., 2012; Waters, 2011) by sending the survey to 30 IT managers. Cronbach's alpha is a commonly used pointer of reliability that provided the standard of all feasible split-half reliability co-efficient (Cozby & Bates, 2012). Cronbach's alpha was used to evaluate the reliability of the research instrument items (Field, 2009). The acceptable value required for Cronbach's alpha subsisted on a trustworthy degree between 0.7 and 0.8 (Field, 2009; Stafford & Turan, 2011). The pilot test resulted in 9 of the diminished versions being rejected. Twenty-one surveys were then tested with a response rate of 70%, and the results of the pilot study are shown in Table 4.

3.2.2. Respondents' demographic analysis

The seventy-seven Queensland local governments supply numerous services to their local constituents (citizens) and regional companies. In order to uphold this commitment, these local governments rely heavily on the latest IT research (LGAQ, 2013). The current study therefore identified the IT departments within these regional local governments as the focus population for this research. All 77 regional local governments had access to the online survey. A return rate of 61% correlated with that of IT managers from 47 regional local governments. From these local governments, a total of 480 IT staff participated and returned the survey (see Table 5 for demographics)—which was a particularly strong result.

Table 5
Demographics analysis.

Demographics	Frequency	Percent
Roles in IT		
Management	238	50%
Systems development/Analyst/Programmer	138	28.8%
Systems administrator/Operations/User support	101	21%
Other	3	0.6%
Knowledge related to Cloud		
Little knowledge	111	23.1%
Some knowledge	111	23.1%
Good knowledge	238	49.6%
Excellent knowledge	20	4.2%
Years' of experience in IT		
< 1 year	107	22.3%
2–5 years	250	52.1%
6–10 years	111	23.1%
11–14 years	8	1.7%
> 14 years	4	0.8%
Total	480	100%

The demographics comprised the participants' occupation within the IT department, the level of comprehension surrounding cloud computing and their total length of time working in IT (Table 2). At 49.6%, the majority held authoritative positions; while 28.8% worked as programmers, analysts or developers. Twenty-one percent of participants were either in supporting positions, administration or operators. It is clearly evident that the vast majority of the research respondents held knowledge and experience in managerial positions. 'Good knowledge' was the highest rating and this was attributed to 49.6% of respondents (238); and 'some knowledge' related to 23.1% of respondents (111). These findings point to vast perceived knowledge differences between regional staff.

4. Research Results

4.1. *Study 1:* Results

The themes that emerged from data related to the security requirements of cloud service included: (1) data transmission; (2) trustworthiness; (3) data storage; (4) redundancy; (5) backup; (6) data privacy; and (7) government regulation. Findings related to each of these aspects are explored next.

4.2. Data transmission

Seventy percent of research participants agreed that the cloud provides secure data transfer through the use of sophisticated encryption techniques. Manager C21-RTX suggested that: *"Security of data being paramount and we are being able to trust your provider that the data will be kept secure and of course the ownership with the, to continue to own the data so forth, that they take ownership by holding on this service"* (C21-RTX). Using Amazon Web-Services (AWS), security concerns such as packet sniffing, browsing of ports, IP spoofing and attacks known as MITM (Man-In-The-Middle) may be managed by securing data transmission (Subashini & Kavitha, 2011). Amazon Simple Storage Service (S3) can be accessed by encoded SSL endpoints, which can be reached from Amazon EC2 and the Internet. This ensures that information is moved with full security from location to location outside and inside of AWS (Subashini & Kavitha, 2011). Providers such as Amazon are denied access to customer information and cannot utilize Guest OS through the Elastic Compute Cloud (EC2). However, business administrators need to use their unique cryptographically-strong Secure Shell (SSH) to connect with a host: here, all connections are recorded, reviewed and checked. Information stored in Amazon S3 is not encoded, yet users are able to encode their data prior to uploading to Amazon S3. In this way, it is less likely that tampering can occur (Amazon, 2016).

ARTICLE IN PRESS

4.3. Trustworthiness

Factors related to trustworthiness were supported by eighty-six per percent of participants regarding the idea of a cloud solution being trustworthy. Manager C52-UFM noted that: *"I think that trust and security is raised a lot but the cloud solutions are very secured and trustworthy, if you have to look at Amazon, for example, they hold a number of security specifications that run in properly secured data centres. They have security people looking up after their environment. I think IT people are probably more reliable back in to cloud because they are probably more aware of risks of technology. So, I think those risks in cloud have not blown"* (C52-UFM). Issues within ISs, such as the broad range of privacy concerns and managing access to networks, are not a new phenomenon in trust management (Artz & Gil, 2007). To urge users to be vigilant of these concerns, system security includes the element of trust (Nagarajan & Varadharajan, 2011), which depends largely on the adopted model as authorization of information and how applications are sought externally are at the provider's discretion (Zissis & Lekkas, 2012).

4.4. Data storage

In relation to the secure storage of an organization's data, 77% of participants noted that CSPs and data centres provide greater information security during data storage. Manager C18-URS suggested that: *"Yes, it is much secured. We have full faith it is very safe. We have seen the database centre in Sydney, it is very safe and no one can basically come to our data without prior approval, you know, from the council"* (C18-URS). All sectors of knowledge that are greatly dependent on data analysis and sizes have dramatically increased. Managing a large range of data is beyond the capacity of most local data storage systems. Consequently, storage-as-a-service is common in cloud service (Niehaves, Plattfaut, & Becker, 2013). Our Study 1 results confirm the assurance levels of local governments towards the use of cloud computing for data storage. Attracted by cost-efficient model, almost all organizations opt for outsourcing data to remote CSPs. However, archival storage requires guarantees of availability and redundancy (Islam & Hasan, 2016). This form of storage carries data for a long time, during which it may experience data loss or intentional migration to negative storage. Proof of Retrievability (PoR) (Juels, Kaliski Jr, Bowers, & Oprea, 2013) and Provable Data Possession (PDP) (Ateniese et al., 2007) are two approaches to auditing the data stored on remote servers (Islam & Hasan, 2016). CSPs usually claim multiple replications of data to mitigate data unavailability due to a single point of failure. For instance, Amazon's S3 claims to store data on multiple devices via multiple facilities. Local governments are apparently unaware of these factors associated with data storage (Amazon, 2017). Therefore, these underpinning aspects of data storage must be reviewed to offer full benefits of cloud-based data storage that has high perceived security risks based on our results.

4.5. Redundancy

In relation to redundancy, 46% of participants stated that cloud computing provider data centres have effective redundancy. Managers such as C72-URS and C15-RAL suggested that: *"The best benefits that CSPs have are high quality redundancy, disaster recovery, sharing resources, availability, reduced IT infrastructure, and providing better services"* (C72-URS). Also, *"I am sure that they do have a lot of redundancy built in, but really, we need to satisfy ourselves that the data centres are as strong as they really make out that they are"* (C15-RAL). Redundancy in terms of duplicate data or equipment to design fault-tolerant cloud services is considered a positive factor for cloud computing adoption (Norman, 2012). Consistent with the benefits of cloud service and current literature on the effect of redundancy on cloud adoption, study 1 here found that managers treat redundancy as a significant requirement for cloud security. Interview results show that while redundancy does not offer significant value to cloud services, the absence of redundancy is detrimental to favourable adoption decisions (Islam & Hasan, 2016).

4.6. Backup

For factors related to back-up, 75% of participants pointed out that cloud computing provider data centres had effective back-up systems. Managers such as C61-URM and C19-RTL suggested that: *"The ability of vendor to be able to look after the security side for things such as back-up from disaster recovery from rural and regional area. Back to the supplier, who would carry them out and as a part of the agreement, we need to make sure that they have proper disaster recovery mechanism in place as far as backup and restore"* (C61-URM). Also, *"It would probably be the risk of losing your physical hardware and data through unforeseen circumstances like natural disasters or fires or whatnot where if you have got everything in-house as we do at the moment with nothing going into the cloud and once, we do have the backup measures off site they are only data so it would still be the loss of hardware. I think that would be a factor to drive council at looking at cloud-based computing"* (C19-RTL). The back-up of data is a vital aspect within cloud computing. Due to malicious harm or mistakes, regular back-ups are vital to guarantee recovery (Ali, Khan, & Vasilakos, 2015). Additionally, the provider must ensure periodic back-ups so that data is always accessible. The process of backing up data must adhere to privacy standards to prevent tampering. Furthermore, tight encoding is a necessity so that backed up information is protected and confidential data cannot be leaked (Subashini & Kavitha, 2011). CSPs such as Amazon store data in S3—which is not encoded. Here, users must individually encode the information and carry out backups to ensure no outside individuals can access the data.

4.7. Data privacy

In relation to the privacy of an organization's data, 63% of participants pointed out that CSPs maintain the privacy of an organization's data. Managers such as C15-RAL and C45-RAV suggested that: *"Privacy was a big issue a couple of years ago, when the only real data centres were overseas and Australian law prevented us - or restricted us moving data which is considered to be private, offshore. But those are starting to fade as I say with a lot of major data centres being built in Australia and under our policies and privacy laws"* (C15-RAL). Also, *"It may depend on the type of data we are talking about and the level of privacy requirement for it? A lot of the data we store, there is no privacy requirement so for some of that it would not be an issue. I cannot imagine though the legality data has it all privacy. I cannot imagine that you would get away with that"* (C45-RAV). Each country has legal guidelines to follow when handling confidential data and which all organizations must adhere to (Softlayer, 2009; van Zoonen, 2016). Cloud computing therefore comes with legal obstacles, particularly as data is stored in numerous areas within the cloud, thus increasing security risks. Information is stored with the provider, which may be in an international location rather than internally on the organization's server. This contrasts with some legal requirements, for example, European law states that location and personal possession of confidential data must always be known (Softlayer, 2009). More regulation requirements have been mandated by the introduction of the European Union's General Data Protection Regulation (GDPR) (De Hert & Papakonstantinou, 2016), which came into force in May 2018.

4.8. Government regulation

Regarding government regulation, 83% of participants noted that government regulations can provide better processes and security guidelines for the organization's system and data. Several managers such as C61-URM and C39-URM noted that: *"Government regulation has the potential to drive the use of cloud services as regulations are refined to make it easier for councils to utilize. Government regulation could also force the use of cloud solutions in some circumstances (i.e. government reporting portals)"* (C61-URM), and *"Government regulation, if the regulations*

change and they say you must utilize cloud services for any future software procurement or hardware procurement then you just have to do it. I mean, it is the law if it becomes legislation so the impact would be quite large and it would impact budget and all that staff resourcing" (C39-URM). These participants confirm that government regulation is important and necessary for cloud security solutions, and in the implementation of IS innovations (Kimball, 2011; Kuan & Chau, 2001). Governments have the capacity to promote the implementation of cloud-based solutions through formulating regulations to encourage organizations and businesses to utilize the system (Kuan & Chau, 2001; Misuraca, Broster, & Centeno, 2012).

Despite IS adoption being able to provide various benefits for the public sector and, in particular, local government councils, many instances of failure to realize the value of IS still exist (Anthopoulos, Reddick, Giannakidou, & Mavridis, 2016; Zhu, 2017). This phase of the research that based on the initial literature review, ISO27000 standards and the results from the exploratory stage (Study 1), gave us an improved understanding about the information security requirements of cloud services within the local government context. Consequently, the findings from our qualitative data in Study 1 provided a new set of factors that might not have been discovered with the application of ISO27000 standards alone. Based on Study 1 findings, we proposed a cloud security requirements conceptual framework. According to the four main components and ten factors of the cloud security requirements conceptual framework, we developed research hypotheses which are discussed next.

4.9. Development of the conceptual model and hypothesis

4.9.1. Cloud security requirements conceptual framework

Some studies use IT adoption theories to explore the determinants of cloud service adoption decisions in many different contexts and to analyse the adoption stages (Liu & Kim, 2018). Since this research is based on extant scholarly work noted earlier (e.g., Chen & Zhao, 2012; Kresimir & Zeljko, 2010; Krumm, 2008; Mahmood, 2011; Pearson, 2009; Pearson & Benameur, 2010), it is possible to create a preliminary cloud information security requirements conceptual framework. The standard ISO/IEC 27002 (ISO/IEC, 2013) helped establish the security requirements. Moreover, the findings from the exploratory study (study 1) involving IT managers of regional local governments provide directions for the proposed framework.

As shown in Fig. 2, while various characteristics and dimensions have been identified as the constituents of security of many domains, some underlying common dimensions remain. Based on our review thus far, we conceptualized cloud information security requirements as a multidimensional model consisting of four key groups of constructs: (1) data security; (2) risk assessment; (3) legal and contractual requirements; and (4) business and technical requirements.

Data security refers to the data security requirements in terms of data transmission, storage and also user privacy (Bishop, 2003; Janssen & Joha, 2010). Cloud computing has security implications in terms of data transmission due to high volume data exchange between servers (CSPs) and clients (e.g. light-weight browsers); as well as data storage due to its distributed storage system. In fact, two driving forces behind cloud computing are high speed and omnipresent networking that facilitates data transmission; and falling storage and infrastructure costs that enable scalable remote data storage. Likewise, data privacy concerns continue to restrict users to upload private data into cloud services since the sense of loss of control is lost when cloud computing is adopted (Hashem et al., 2015). Acknowledging these three factors of data transmission, storage and privacy in terms of information security, they are grouped under the category of Data security.

The three other groups of constructs are selected based on the security requirements suggested by ISO 27002 (ISO, 2013), viz. risk assessments; legal and contractual requirements; and business and technical requirements. Finally, we decided on these groups based on the combined efforts from the initial literature review, ISO27000 standards and the results from the exploratory stage (Study 1).

Managing information security using the lens of ***risk assessment*** is a well-accepted principle and this concept has been extended towards applying in cloud computing (Zhang et al., 2010). Risk assessment comprises principles of overall risk management and security control (Zhang et al., 2010). Risk assessments for information security have also considered user awareness as an essential part of overall information security (Kruger & Kearney, 2006). These three factors are therefore considered as part of risk assessment for our conceptual model.

Legal and contractual requirements are essential components of information security since organizations must understand the importance of legal compliance and the obligations that arise from it in terms of information storage and processing (Gerber & Von Solms, 2008). The legal aspects of information security requirements are often mandated by relevant standard and privacy standards and regulations which is therefore the first factor considered in this study. Consequently, compliance is the second factor as it encapsulates the challenges of meeting the obligations from requirements imposed by information security requirements. These factors are significant for organizations irrespective of whether they implement cloud services or not (King & Raja, 2012).

Lastly, the three factors identified from study 1: backup, trustworthiness and redundancy; were grouped as ***business and technical requirements*** as they relate to operational IT activities within the organization. Encryption was added in this group as it is undoubtedly a major technical requirement for cloud security during information transmission and storage. Information security communities continue to develop innovative algorithms for encryption optimized towards cloud services (Stergiou, Psannis, Kim, & Gupta, 2018). Similarly, on the business side, it is important to consider service level agreements (SLAs) as part of essential business requirements for cloud computing. During the keynote address by Buyya, Yeo, and Venugopal (2008) to present a future vision for cloud computing, there was a strong emphasis on market-based resource management strategies for IT service management and risk management for cloud computing using SLAs. Therefore, SLAs were added as the final factor within the business and technical requirements in our conceptual framework, as illustrated in Fig. 2.

4.9.2. Research hypotheses

By employing the information security requirements that were defined in the qualitative interview findings, and by incorporating these with the literature review analysis, four main hypotheses were developed and tested (discussed next). The basis for each hypothesis was to analyse the cloud information security requirements conceptual research framework presented in Fig. 2 and to provide clear answers to the research question.

Data security (H1): In terms of cloud-based solution, data security in cloud service is considered to be more critical in comparison to other services in cloud computing. CSPs state that they have the ability to safeguard organizations' data more effectively than the organizations themselves (Kaufman, 2009). In this research, data security refers to the security of data transmission, storage, and privacy (Subashini & Kavitha, 2011). Greater levels of data security have a positive impact on organizations wishing to adopt cloud computing, leading to the following hypothesis:

H1. Organizations that need secure data transmission, data storage, and data privacy are more likely to adopt cloud-based solution.

Risk assessment (H2): The unique element of risk assessment in cloud computing relates to the operational security and monitoring of cloud services. Security assessments are important mechanisms for risk mitigation from cloud security breaches, which can be undertaken using an information risk management framework (Zhang et al., 2010). While there is a good understanding of cloud-associated risks and

ARTICLE IN PRESS

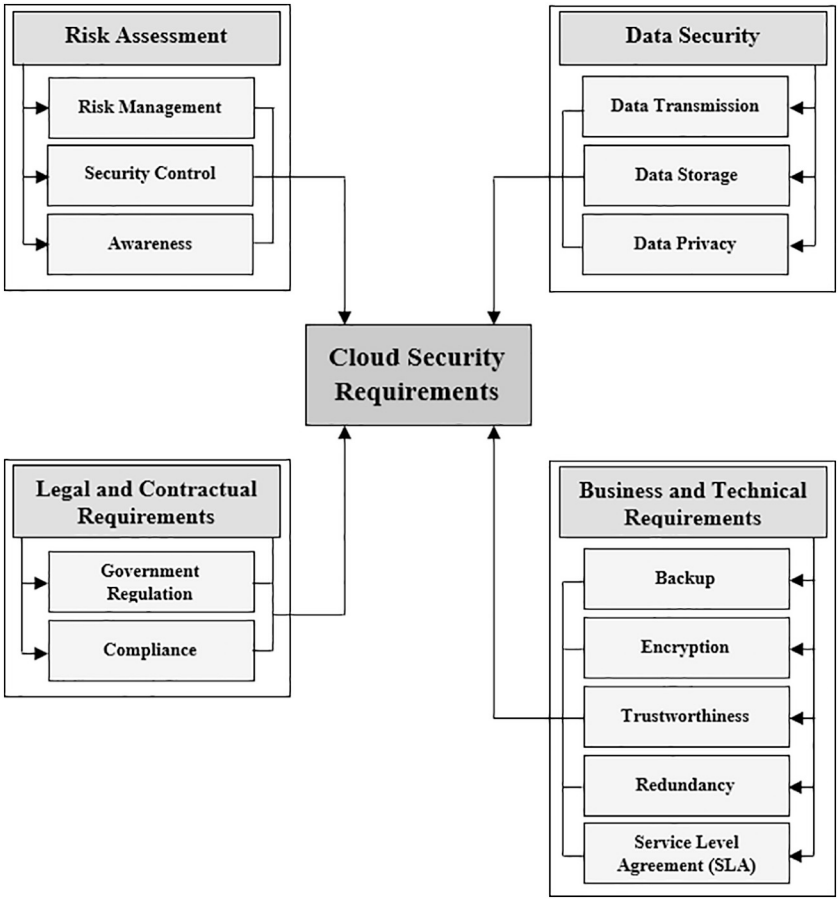


Fig. 2. Cloud security requirements conceptual framework.
(Adapted from ISO/IEC 27002 information security requirements)

necessary controls, the risk mitigation practices are not mature enough for wide scale adoption (Brender & Markov, 2013). This leads to the following hypothesis:

H2. Organizations requiring high risk assessment support in risk management, security control and awareness are more likely to adopt cloud-based solutions.

Legal and contractual requirements (H3): Legal and contractual requirements such as government regulation and compliance can be explained as the support provided by the government for the purpose of encouraging the amplification of organizations' IS innovation capacity (Jaeger, 2007; Jaeger, Lin, & Grimes, 2008). The regulation and policy settings that each organization has, as measured through current laws and regulations, can be evaluated within this requirement. By formulating rules for safeguarding businesses using cloud-based solution, governments can promote the adoption of cloud computing (Best, Kreuger, & Ladewig, 2008; Jaeger, 2007; Carrico & Smalldon, 2004). This leads to the following hypothesis:

H3. Legal and contractual requirements such as government regulation and compliance related to cloud computing security positively influence cloud-based solution adoption.

Business and technical requirements (H4): Business and technical requirements for information security in cloud computing deals with unique environments in which cloud services deliver value to customers (Subashini & Kavitha, 2011). From the cloud service consumer's perspective, there are technical challenges in terms of secure data storage and transmission when using cloud to deliver services to their end customers. Recent developments in encryption techniques have confirmed secure cloud communication is possible in theory; however, there are still challenges in practice due to its complexity in cloud environments (Ren et al., 2012). Another area of concern is trustworthiness between CSPs and clients in the dynamic environment of cloud service, for example, managing service level agreements that promote continuous monitoring towards adaptive trust management (Li & Du, 2013). This leads to the following hypothesis:

H4. Business and technical requirements such as backup, encryption, trustworthiness, redundancy, and service level agreements positively influence cloud computing adoption.

The researchers applied the framework shown in Fig. 2 to test the aforementioned four hypotheses and to measure the security issues surrounding cloud-computing adoption within a quantitative study that encapsulates study 2 of this research (discussed next).

4.10. ***Study 2:*** *Results*

4.10.1. *Measurement model*

The reliability, validity and assessment of information related to the security concerns of cloud computing adoption were tested. Validity was tested by using exploratory factor analysis (EFA) and confirmatory factor analysis (CFA). Secondly, to ascertain how constant the internal factors were, the reliability and validity of the categorizations were also tested.

Factor analysis: It is an important tool which is employed in improvement, assessment of tests, and scales (Williams, Brown, & Onsman, 2010). This technique include exploratory factor analysis (EFA), followed by confirmatory factor analysis (CFA). Each of these factor analysis statistical techniques will be explored next.

Exploratory factor analysis (EFA): It is an extensively utilized

ARTICLE IN PRESS

Table 6
One-factor congeneric measurement results.

Factors	Fit Indices									Items input	Items output
	CMIN	χ2	GFI	AGFI	RMR	IFI	TLI	CFI	RMSEA		
Risk Management	3.937	6.17	0.990	0.936	0.010	0.990	0.967	0.991	0.076	4	4
Security Control	3.998	8.15	0.950	0.908	0.022	0.957	0.945	0.974	0.077	5	4
Awareness	0.858	7.15	0.989	0.990	0.003	1.000	1.001	1.000	0.000	6	5
Data Transmission	0.843	5.90	0.989	0.979	0.002	1.000	1.002	1.000	0.000	4	3
Data Storage	1.189	9.45	0.978	0.967	0.018	0.996	0.994	0.998	0.021	7	5
Data Privacy	2.264	7.25	0.964	0.941	0.015	0.989	0.979	0.971	0.043	5	5
Government Regulation	1.564	7.46	0.973	0.939	0.012	0.967	0.963	0.969	0.037	6	4
Compliance	0.432	6.89	0.989	0.969	0.002	1.002	1.004	1.000	0.000	5	3
Backup	2.150	6.35	0.989	0.964	0.029	0.994	0.988	0.992	0.048	4	3
Encryption	0.529	7.86	1.000	0.994	0.002	1.001	1.003	1.000	0.000	6	4
Trustworthiness	0.716	5.98	0.998	0.990	0.003	1.000	1.001	1.000	0.000	4	4
Redundancy	0.912	7.98	0.972	0.982	0.009	1.000	1.001	1.000	0.000	5	3
Service Level Agreement (SLA)	0.498	8.63	1.000	0.992	0.003	1.001	1.002	1.000	0.000	5	4
Total items										66	51

statistical methodology used in the fields of IS, education, and social science (Williams et al., 2010). In EFA, the investigator has no expectations of the number or nature of the variables and as the title suggests, is exploratory in nature. That is, it allows the researcher to explore the main dimensions to generate a theory, or model from a relatively large set of latent constructs often represented by a set of items (Henson & Roberts, 2006; Swisher, Beckstead, & Bebeau, 2004). So, the main objectives of EFA are; reduce the number of variables; examine the structure or relationship between variables; evaluates the construct validity of a scale, test, or instrument; used to develop theoretical constructs; and used to prove/disprove proposed theories (Thompson, 2007). In this research analysis, we conducted EFA using IBM Statistical Package for Social Science (SPSS) version 22. The results of the analysis revealed that Kaiser-Meyer-Olkin (KMO) factor loadings on each of the 13 factors ranged from 0.783 to 0.981 (Hair, Anderson, Tatham, & Black, 1995). In summary, each factor loading was greater than the suggested 0.50 (Hair, Black, Babin, & Tatham, 2005; Zhang, Waszink, & Wijngaard, 2000), which is considered to be very significant and acceptable.

Confirmatory factor analysis (CFA): It is basically employed to assess a suggested theory and is an arithmetical methodology. CFA is also a type of SEM (Swisher et al., 2004). Contrary to EFA, CFA has suppositions and prospects established on priori theory regarding the number of factors, and which factor theories or models are more appropriate (best fit) (Swisher et al., 2004; Thompson, 2007). In this research, we conducted a CFA using IBM SPSS Amos 22 Graphics. According to Dragovic (2004), we first tested the one-factor congeneric measurement on each factor in the cloud computing security conceptual model. The key purpose of this test is to evaluate the uni-dimensionality and appraisal of the data set through the verification of basic Chi-square ($\chi 2$) with a significance levels at < 0.01, < 0.05, or < 0.10; but any value between 0 and 1 can be used (Hair, Anderson, Tatham, & Black, 1998; Jöreskog & Sörbom, 1993). But, in the literature researchers found out that the $\chi 2$ is not considered to be a very useful fit index by most studies, due to the $\chi 2$ is affected by larger samples, which it is sensitive to a large sample size > 200 and rejects the model (Bentler & Bonett, 1980; Marsh, Balla, & McDonald, 1988; Schermelleh-Engel, Moosbrugger, & Müller, 2003), and it is also no longer relied upon as a basis for acceptance or rejection (Schermelleh-Engel et al., 2003; Vandenberg, 2006). Other fit indices included in this research analysis are; Normed Chi Square (CMIN/DF) with a level of ≤ 5.0 (Hair et al., 1998; Tabachnick & Fidell, 2001). Typically, CMIN/DF is used as an alternative measure to alleviate the effect of larger sample size by dividing the $\chi 2$ by the degrees of freedom, where a value of CMIN/DF < 3 is good, sometimes < 5 is permissible, suggesting acceptable model fit (Kline, 2015). Furthermore, Root Mean Square Residual (RMR) with a level of < 0.06 (Byrne, 2001; Hu & Bentler, 1995), Goodness of Fit (GFI) with a level of ≥ 0.90 (Byrne, 1989; Hair et al., 1998), Adjusted Goodness of Fit (AGFI) with a level of ≥ 0.80 (Hair et al., 1998; Marsh et al., 1988), Root Mean Square Error of Approximation (RMSEA) with a level of ≤ 0.08 (Hair, Black, Babin, Anderson, & Tatham, 2006; Holmes-Smith, Cunningham, & Coote, 2006), Incremental Index of Fit (IFI) with a level of ≥ 0.90 (Bollen, 1989; Byrne, 2001), Tucker-Lewis Index (TLI) with a level of ≥ 0.90 (Hair et al., 1998; Marsh et al., 1988), Comparative Fit Index (CFI) with a level of ≥ 0.90 (Bentler, 1992; Byrne, 2001; Hair et al., 1998)—all of which are taken into account for this analysis as these are employed frequently in the literature (Byrne, 1998; Hulland, Chow, & Lam, 1996). In this regards, Hair Jr, Black, Babin, and Anderson (2010), p. 583) confirmed that "*reporting the χ2 value, the CFI or TLI, and the RMSEA will usually provide sufficient unique information to evaluate a model*". In the same context, Holmes-Smith (2011) confirmed that researchers can use at least one index from each goodness category of the measurement model to achieve the acceptable model fit. Thus, this research followed the recommendations of the mentioned scholars to use at least one or two index from each category of model fitness. As a result of that, all 13 factors in the cloud computing security conceptual model were evaluated individually using this technique and the best fit of each congeneric measurement model was achieved. In this process, 15 items were been removed from the individual models. The objective of removing these 15 items was to accomplish an enhanced fit of the data in this procedure wherein 51 items were assessed in the overall measurement model (see Table 6).

Model reliability and validity: To test for model reliability and validity we employed Cronbach's Alpha using the recommended acceptance score of ≥ 0.70 (Stafford & Turan, 2011). Each of the factors in the cloud information security requirements framework exceeded the acceptance score by falling within the range of 0.789 and 0.961. We also considered the Squared Multiple Correlation (SMC) (Holmes-Smith, 2011) using the suggested value of SMC being > 0.30. The large majority of the items (38 items out of 51 items) in the final cloud information security requirements conceptual framework exceeded 0.50; and the remaining 13 items were above 0.350, with 0.372 being the lowest value. In summary, the value of SMC illustrates that all items used to measure the factors of the cloud information security requirements framework are dependable. We tested for convergent validity using Standardized Regression Weights (SRW) to check for construct consistency and the measurement limits of each of the items. The recommended factor loading to suggest significant validity of each item is an approximated value of ≥ 0.50 (Hair et al., 2006; Holmes-Smith, 2001). The SRW loading values of the factors in the final cloud computing security conceptual model were found to be between 0.588 and 0.954. Finally, the critical ratios (CR) of the cloud information security requirements conceptual framework items were between 11.281 and

ARTICLE IN PRESS

25.457, which were more than the standard value of 1.96 suggested by Holmes-Smith et al. (2006). This indicates that the cloud information security requirements conceptual framework retains significant regression validity.

4.10.2. Structural equation model (SEM)

The cloud information security requirement conceptual framework discussed earlier assisted in identifying the information security requirements for the adoption of cloud-based solution in Australian regional local governments. In this regard, 13 factors were included in the conceptual framework designed for measuring the information security requirements of cloud computing adoption. Byrne (1999) and Ozkan and Kanat (2011) explained that a SEM allows researchers to determine those factors that have a direct or indirect effect on the values of other latent variables. As a result, this research study applied the SEM technique and used IBM SPSS Amos 22 Graphics tool to evaluate and test the research hypotheses between the factors in the cloud security requirements model. SEM is one of the principal statistical techniques that researchers use to examine and evaluate several interrelated dependence relationships in a single research model (Byrne, 2013). SEM technique is a popular statistical method used in social science (Mueller, 1997) because of its flexibility in interpreting the theory to be tested and the sample data (Chin, 1998a; Hair Jr et al., 2010).

The principle of the structural model in this research is to evaluate the links via major paths between latent variables, as well as to examine the fundamental hypothesis for providing answers to the highlighted research question. As illustrated in Table 7, the findings of the structural model fit confirmed that the measurement framework achieved a good fit and most of the different indicators that were reported in this research met the recommended levels.

Also, to confirm that the cloud security requirements model is fit, Table 8 demonstrates the residual matrix which represents the differences between corresponding values in the expected and observed matrices (Schermelleh-Engel et al., 2003). The results of residual matrix are confirmed that the model is reasonably, and all elements are sufficiently close to zero.

The SEM findings demonstrated in Table 9 are measured on the basis of estimated path coefficient (β) value with the critical ratio (t-value) with the standard decision rules of t-value > 1.96 (Holmes-Smith et al., 2006), R Square (R2) with suggest levels of 0.670 substantial, 0.333 moderate, and 0.190 weak (Bollen, 1989; Chin, 1998b; Urbach & Ahlemann, 2010), and *p*-value is at least ≤0.05 or ≤ 0.01 (Byrne, 2001; Holmes-Smith et al., 2006).

The results of the regression tests presented in Table 9 indicate and confirm that 10 out of 13 factors that were developed for testing in the SEM have been accepted as having a positive impact; and have a significant relationship in the measurement of cloud information security requirements. These factors were data transmission, data storage, data privacy, encryption, backup, trustworthiness, risk management, security control, awareness, and service level agreements. The other three factors in the cloud information security requirement conceptual framework were rejected. These factors related to redundancy, compliance, and government regulation. In Fig. 3 we display the path diagram for these final relationships.

Table 7
Fit indices from SEM test results.

Indices	Structural model fit	Conclusion for fit
CMIN	2.623	Good
$\chi 2$	60.89	
RMR	0.054	Good
GFI	0.91	Good
AGFI	0.85	Good
IFI	0.92	Good
TLI	0.90	Good
CFI	0.93	Good
RMSEA	0.060	Good

5. Research discussion

The key purpose of this research paper was to explore the main critical factors considered to be beneficial in understanding the information security requirements of cloud computing within Australian regional local governments. Similarly, several research questions and hypotheses were explored in relation to the aims of the paper. Each of these has been carefully researched as described herein, and the results reported. With the rapid rise in not only the need for, but also the growth of cloud computing, this research into Australian regional local government informs the current literature on factors that might be used to measure cloud computing from a security perspective. Moreover, advice and relevant aspects of cloud security are highlighted here for regional local governments, service providers, and technology consultants. In particular, regional local governments provide services to its citizens and local businesses and, as a result, form part of an important sector in the market for software and CSPs. It is evident that CSPs need tighter and more supportive relationships with regional local governments to eliminate concerns promptly and to create conducive environments. This research study not only increases scholarly understanding of the security aspects of cloud security, but also serves to assist regional local governments in weighing up the advantages of a cloud computing security model. Next, we discuss factors in relation to information security requirements as proposed in our research framework.

5.1. Discussion of Hypothesis 1

Hypothesis 1 relates to whether organizations that need secure data transmission, data storage, and data privacy are more likely to adopt cloud computing.

Data transmission: The research model revealed that there is a significant and positive relationship between data interchange and cloud computing security. As demonstrated in Table 9 the standardized coefficient (β) was 0.312, t-value is 4.759, R Square (R2) is 0.592 and *p* value is < 0.01 level 0.006**. According to the literature review, previous studies noted that it is extremely important to ensure data transmission is secure (Paquette et al., 2010; Subashini & Kavitha, 2011). Also, previous research by Andreica, Covaci, and Kung (2015) proposed a general data interchange framework for heterogeneous systems and entities. The model proposed here uses cloud services and provides systems inter-operability capabilities for various fields, suggesting that our research findings are consistent with previous scholarly findings.

Based on the research findings, local governments will benefit from paying close attention to the data interchange factor(s) in order to increase the security rating of cloud service. This attention might involve the IT manager and senior IT staff engaging in conversations with the CSPs, networking with other councils, and engaging external consultants to become informed and educated about the data interchange between their present systems and cloud computing systems.

Data storage: The current model yielded a significant relationship between the security of an organization's data as an influential factor in the cloud security model. As demonstrated in Table 9, the standardized coefficient (β) was 0.284, t-value is 2.988, R Square (R2) is 0.589 and *p* value is < 0.01 level 0.008**. The low security rate of any innovation might act as obstacle to the adoption of any advanced technology (Fernandes et al., 2014). Data is often stored externally of company boundaries in cloud computing models at the location of the provider. It follows then that it is the CSP's obligation to ensure security aspects have been addressed in terms of staff access, leakage and in the management of security (Knapp, Denney, & Barner, 2010). Therefore, tight encoding and strict authorization to manage information is necessary

ARTICLE IN PRESS

Table 8
Residual matrix results.

	RT	SC	AW	DT	DS	DP	GR	CO	BU	EN	TR	RE	SLA
RT	0.00												
SC	0.03	0.00											
AW	0.01	0.09	0.00										
DT	0.08	−0.01	−0.07	0.00									
DS	0.07	−0.03	0.01	0.07	0.00								
DP	0.01	0.06	0.04	0.03	0.08	0.00							
GR	0.11	0.15	0.07	0.09	0.06	0.11	0.00						
CO	0.14	0.19	−0.05	0.08	−0.01	0.09	0.04	0.00					
BU	0.09	0.03	0.08	0.04	0.09	0.02	0.07	0.05	0.00				
EN	0.08	0.05	0.04	0.08	0.06	0.04	0.08	0.17	0.04	0.00			
TR	−0.04	−0.07	0.09	0.08	0.08	0.07	0.15	0.12	0.09	0.03	0.00		
RE	−0.18	0.12	0.06	0.09	0.15	0.08	0.13	0.05	0.16	0.01	0.05	0.00	
SLA	0.05	0.07	0.05	0.07	0.06	0.04	0.05	0.02	0.04	0.04	0.08	0.03	0.00

RT: Risk Management; SC: Security Control; AW: Awareness; DT: Data Transmission; DS: Data Storage; DP: Data Privacy; GR: Government Regulation; CO: Compliance; BU: Backup; EN: Encryption; TR: Trustworthiness; RE: Redundancy; SLA: Service Level Agreement.

(Subashini & Kavitha, 2011). Our research findings illustrate that the security of an organization's data is a significant factor and has a positive impact on the cloud security model. Our research results are consistent with previous studies that found the security of an organization's data to be a significant factor in the technology adoption decision (Fernandes et al., 2014; Zissis & Lekkas, 2012).

Within the local government context, it is suggested that IT managers will need to expend effort to educate both IT staff and top management about how to ensure that CSPs' information is supported by security architecture in conjunction with consistent examination by external bodies. Also, it is important to understand how to promote internal security to ensure that access controls and firewalls are conducive with cloud model security plans.

Data privacy: The research found a significant and positive relationship between privacy of an organization's data and cloud computing security. As demonstrated in Table 9, the standardized coefficient (β) was 0.485, with t-value 1.983, R Square (R2) is 0.569 and *p* value is < 0.05 level 0.010*. Privacy is a complex topic that has different interpretations depending on cultures, communities and contexts, and the United Nations has recognized it as a fundamental human right (Gholami & Laure, 2015). Risks are seen in the privacy of an organization's data in services dealing with different aspects of data such as collection, transfer, processing, sharing, and storage of sensitive and personal details (Ali, Soar, & Yong, 2016, 2017). As cloud computing becomes more widely used there is a wide range of policy issues related to data storage locations that require considerable attention (Jaeger et al., 2008). These include issues of privacy, communications capacity, and government surveillance (Delaney & Vara, 2007). According to previous studies, and consistent with our findings here, there are a number of aspects that illustrate significant privacy issues in cloud such as: lack of user control; unauthorised secondary usage; and data proliferation (Pearson & Benameur, 2010; Yadav & Singh, 2012). Also, there are some studies that report a positive correlation between privacy of an organization's data—especially information relating to location, preferences, social networks of individuals and personal health data—in the adoption and use of advanced technologies (Alshomrani & Qamar, 2013; Yadav & Singh, 2012). However, these aspects are beyond the scope of the current study.

Our research findings indicate that the privacy of an organization's data is a significant influential factor in cloud computing security and is consistent with previous literature. However, regional local governments that have adopted, or plan to adopt, cloud-based solution should demand that CSPs maintain information according to privacy regulations. This has becoming increasingly relevant with the EU moving to a stringent privacy requirement, namely, the EU-GDPR enforced in May 2018.

Table 9
Regression weights and results of the path relationships.

Paths[#]		Structural model						Results
			Standardized (β)	S.E.	C.R. (t)	R2	**P**	
Risk Management	→	Risk Assessment	0.235	0.112	2.992	0.627	**0.004****	Supported
Security Control	→		0.198	0.043	2.019	0.544	**0.024***	Supported
Awareness	→		0.203	0.094	1.987	0.552	**0.018***	Supported
Risk Assessment	→	Cloud Security Requirements	0.234	0.177	3.631	0.551	**0.009****	Supported
Data Transmission	→	Data Security	0.312	0.123	4.759	0.592	**0.006****	Supported
Data Storage	→		0.284	0.176	2.988	0.589	**0.008****	Supported
Data Privacy	→		0.485	0.247	1.983	0.569	**0.010***	Supported
Data Security	→	Cloud Security Requirements	0.398	0.235	2.034	0.590	**0.010***	Supported
Government Regulation	→	Legal & Contractual	−0.015	0.234	−0.067	0.491	0.982	Not supported
Compliance	→		0.005	0.098	0.037	0.499	0.964	Not supported
Legal & Contractual	→	Cloud Security Requirements	0.056	0.112	1.603	0.452	0.791	Not supported
Backup	→	Business & Technical	0.252	0.183	3.729	0.581	**0.009****	Supported
Encryption	→		0.181	0.046	2.239	0.561	**0.014***	Supported
Trustworthiness	→		0.136	0.069	2.118	0.541	**0.027***	Supported
Redundancy	→		0.298	0.174	1.439	0.539	0.127	Not supported
Service Level Agreement (SLA)	→		0.668	0.262	4.732	0.609	**0.005****	Supported
Business & Technical	→	Cloud Security Requirements	0.199	0.092	2.118	0.592	**0.017***	Supported

* and ** denote significant level at $p < 0.01$ and $p < 0.05$, respectively.
Demonstrates that a relationship in the structural model is supported. It can be removed since there is another column that says whether it is supported or not.

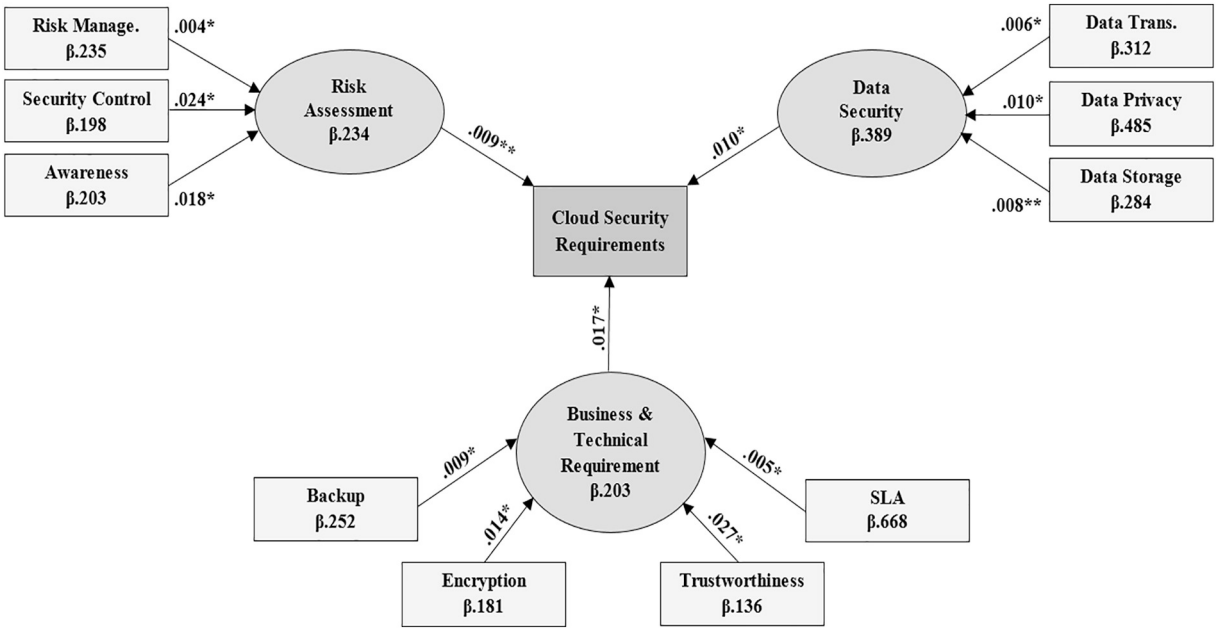


Fig. 3. Path coefficients for the cloud security requirements framework

5.2. Discussion of Hypothesis 2

Hypothesis 2 is related to whether organizations that require high-risk assessment support in risk management, security control and awareness are more likely to adopt cloud-based solution.

Risk management: The research found that there is a significant and positive relationship between risk management and cloud computing security. As shown in Table 9, the standardized coefficient (β) was 0.235 with t-value 2.992, R Square (R2) 0.627 and p value < 0.01 level 0.004**. Current technology and effective management are essential for cloud computing (Kobielus, 2009). Both strong communication between authoritative figures and IT departments and administrative cooperation are vital for control of cloud computing operations (Maches, 2010). Cloud risk management (its potential and solutions) is also a crucial component and should, therefore, be well understood by managing bodies. Furthermore, implementing risk management throughout IT departments should be commonplace (Maches, 2010; Brender & Markov, 2013). While our findings are consistent with previous literature, we suggest that risk management strongly relies on the role of the IT managers within local government who need to become innovation 'champions' by focusing on reducing risk through developing risk management programs. As part of championing the innovation, the IT manager will need to outline the risk management plan to all stakeholders and organize for professional development, networking and education of existing IT staff. This will result in the successful defence of the organization's information assets (data, hardware, software, and procedures).

Security control: The current model revealed that there is a significant and positive relationship between security control and cloud computing security. As shown in Table 9, the standardized coefficient (β) was 0.198 with t-value 2.019, R Square (R2) 0.544 and p value < 0.05 level 0.024*. In terms of security control in the cloud, it is a common fallacy that the CSP is in charge of security around the cloud environment. While CSPs have security controls in place, it is of little value if the customers who access cloud services do not have adequate protection for their networks, users or applications. In fact, most security control issues arise at the client level, thereby prompting cloud providers to look for shared responsibilities for security (Liu et al., 2015). The use of cloud services by an organization is a shared responsibility around storing potentially confidential data on a system that the organization may not own or control (Sheppard, 2014). Our finding is consistent with previous literature in this respect.

We suggest that a viable solution to the cloud computing security issues could be the introduction of trusted CSPs to assure security characteristics within the cloud environment. Regional local governments should understand how to ensure appropriate data governance relating to security in the cloud services is being utilized. IT staff within regional local governments should be cognisant that the security control must be shared between the CSP and the client organization. Regional local governments should propose a shared responsibility model that will provide guidance to organizations on the management and mitigation of the risks associated with ensuring organizations' obligation to data security.

Awareness: The current model found that there is a positive and significant relationship between the level of awareness and cloud security. As shown in Table 9, the standardized coefficient (β) was 0.203 with t-value 1.987, R Square (R2) 0.552 and p value < 0.05 level 0.018*. Our findings are consistent with previous literature (Shin, 2013). For instance, according to Roger (2003) and Zhao and Fan (2018) employee awareness can be affected by the accumulated experience using new innovations. In the case of cloud service, familiarity and awareness of how to use technologies can have a direct influence on employee perceptions regarding cloud services and security (Igbaria, Guimaraes, & Davis, 1995). However, regional local governments should invest more in IT-related skills, knowledge and experience of their employees which, among other obvious benefits, might assist in increasing the security level of cloud computing. As already discussed, professional development of IT staff in their area of expertise is paramount in assisting IT staff to come to terms with systems protection. Using evidence-based framing strategies (de Bruijn & Janssen, 2017) can be a useful exercise for local governments to build cybersecurity awareness.

5.3. Discussion of Hypothesis 3

Hypothesis 3 is related to whether legal and contractual requirements such as government regulation and compliance relating to cloud computing security positively influence cloud-computing adoption.

Government regulation: This aspect is another critical environmental factor that can influence IT innovation adoption (Harauz et al.,

2009) with both Federal and State governments formulating regulations to protect businesses by increasing the security of cloud computing (Jaeger, 2007; Kraemer, Dedrick, Melville, & Zhu, 2006). Governments have the capacity to promote the implementation of cloud-based solution through formulating regulations to encourage organizations and businesses to utilize the system (Kuan & Chau, 2001; Oliveira & Martins, 2010). Cloud computing amplifies the need for governance and this requires the control and oversight by the organization over policies, procedures, and standards for cloud computing services (Jones, Irani, Sivarajah, & Love, 2019).

Our findings, however, are not consistent with the literature. We found, for instance, that there is no significant relationship between government regulation and cloud computing security requirements. As shown in Table 9, the standardized coefficient (β) was −0.015 with t-value −0.067, R Square (R2) 0.491 and *p* value 0.982. Whilst our findings are inconsistent with previous studies (Kuan & Chau, 2001; Misuraca et al., 2012; Zhu & Kraemer, 2005), we advocate that government policy will provide assistance to local governments in rural areas that operate in isolation from urban areas. In particular, the severely isolated regions in Australia rely on satellite technology for Internet services. Government policy that provides improved Internet coverage for outback local governments is necessary for assisting organizations to adopt new Internet technology, as well as providing these organizations with procedures that might help to enhance security of their overall IT systems. It is possible that within the local government sector, local government agencies as a separate governing arm do not regard state and federal government policy efforts as important.

Compliance: The model revealed that there is no significant relationship between compliance and the cloud computing security model, suggesting that more action is required related to compliance issues in local government settings. As shown in Table 9, the standardized coefficient (β) was 0.005 with t-value 0.037, R Square (R2) 0.499 and *p* value 0.964. To address security challenges in the cloud, IT compliance models can be applicable. Research conducted by Kalaiprasath et al. (2017) and Yimam and Fernandez (2016) presented recommended security compliance models for each recognized type of security threat in the cloud, for example, denial of services can be addressed by compliance models from PCI DSS, ISO 27001, HIPPA, SOX, NIST 800-61 or ISO 17799. In research conducted by Ruiter and Warnier (2011), they noted that there are still many uncertainties regarding compliance in cloud service. As a result, it has become very difficult to analyse security and compliance among CSPs. Furthermore, they noted that many regulations shared common requirements such as privacy, integrity, security and enforcement, and that organizations were responsible for security breaches and litigation.

Our finding is counter-intuitive to existing research and we contend that the reason for this finding is perhaps due to the lack of awareness about the compliance aspects of cloud computing. The cloud computing movement has perhaps not yet recognized it as a 'mainstream' IT management issue, whereby even local governments with advanced IT facilities are only at the infant stage of moving into the cloud. Besides the limited knowledge and lack of awareness, the shared responsibility between CSPs and customers means compliance issues could be complex to implement. We found that operational compliance issues are very challenging, even though cloud providers fulfil technical compliance requirements. We contend that a repeated study of this measure in five years' time, when more IT compliant processes are more evident in local government, may result in a different finding.

5.4. Discussion of Hypothesis 4

Hypothesis 4 is related to whether business and technical requirements such as backup, encryption, trustworthiness, redundancy, and service level agreement positively influence cloud computing adoption.

Backup: The research found that there is a significant and positive relationship between backup and cloud computing security. As demonstrated in Table 9, the standardized coefficient (β) was 0.252 with t-value 3.729, R Square (R2) 0.581 and p value < 0.01 level 0.009**. A research conducted by Hemant, Chawande, Sonule, and Wani (2011) stated that there is no assurance of backup in cloud computing. Recovery of data from the cloud is critical for companies in the event of failure and can lead to serious security problems such as data loss or leakage (Cloud Security Alliance, 2010). Our research findings are consistent with other previous studies that determined backup is a significant influential factor in cloud computing security. We suggest that regional local governments should have sound knowledge of what to do in the case of an attack or lost data. Users must have the expertise to restore data, and must ascertain from the provider how and when services will be restored. Also, in a related topic, disaster recovery users must not assume that providers will assist them in all enquiries. It must be understood that if, for example, a lawsuit occurred, the provider could support such requests.

Encryption: The research found that there is a significant and positive relationship between encryption and cloud computing security. As demonstrated in Table 9, the standardized coefficient (β) was 0.181 with t-value 2.239, R Square (R2) 0.561 and p value < 0.05 level 0.014*. The research found that data security is an issue that needs to be resolved as it is acting as a key obstacle in the adoption and use of cloud service (Singla & Singh, 2013). One of the mediums to handle this problem is for data to be encrypted at both client and server ends (Asesh, 2015). The main point for encryption is to introduce a more secure transmission and storage process for handling data which can secure the current cloud services. For example, *Rijndael* is one of the safest algorithms used for encryption which can result in increases in overall reliability of the cloud environment (Asesh, 2015; Buyya & Bubendorfer, 2008). Recent developments in encryption techniques have confirmed secure cloud communication is possible in theory; however, there are still challenges in practice due to its complexity in production cloud environments (Ren et al., 2012).

Our research findings indicate that encryption is a significant influential factor considered in the cloud computing security requirements model. As a result, we suggest that regional local governments should seek evidence from CSPs about the encryption schemes that will be used and guidelines for the encryption of data.

Trustworthiness: The research model found that there is a positive and significant relationship between trustworthiness and cloud computing security. As demonstrated in Table 9, the standardized coefficient (β) was 0.136 with t-value 2.118, R Square (R2) 0.541 and p value < 0.05 level 0.027*. Our findings are consistent with previous studies (Liang et al., 2017). Issues such as managing access to networks are not a new phenomenon in trust management (Artz & Gil, 2007). To urge users to be vigilant of such concerns, system security requires a large degree of trust (Nagarajan & Varadharajan, 2011; Zissis & Lekkas, 2011), which depends largely on the adopted model as authorization of information and applications are sought externally at the provider's discretion (Zissis & Lekkas, 2012). However, regional local governments should be aware that their users must ascertain their rights in regards to hiring employees and the authorization of access and their rights in terms of surveillance (Jaeger & Bertot, 2010). Organizations should retain the right to handle their own internal hiring standards in terms of security screening for both physical and operational aspects of information security.

Redundancy: The research model shown that there is not a significant relationship between redundancy and the cloud computing security model. As demonstrated in Table 9, the standardized coefficient (β) was 0.298 with t-value 1.439, R Square (R2) 0.539 and p value 0.127. Redundancy in cloud computing is the supplying of duplicate copies of different data or equipment to be used in the event that part of one's cloud computing system fails or cannot be accessed (Norman, 2012). Managing large sets of data is beyond the capacity of most local data storage systems. Therefore, storage-as-a-service became very

popular in cloud service. Almost all organizations are opting to outsource data to remote CSPs (Islam & Hasan, 2016). However, the research indicates that archival storage requires guarantees about availability and redundancy (Islam & Hasan, 2016). Amazon's S3 claims storing data on multiple devices via multiple facilities (Amazon, 2017). However, this research finds that there is no impact between the redundancy and the security of cloud computing. This is surprising given the role of redundancy as a technology feature in the adoption of cloud computing where local government stakeholders are advised to understand the role of redundancy in reliable cloud services.

Service level agreement (SLAs): The current research model found that there is a positive and significant relationship between SLAs and cloud computing security. As demonstrated in Table 9, the standardized coefficient (β) was 0.668 with t-value 4.732, R Square (R2) 0.605 and p value < 0.01 level 0.005**. SLAs provide service agreements in relation to the level of service provided, including monetary aspects (Buyya, Garg, & Calheiros, 2011; Faniyi & Bahsoon, 2015). Since cloud computing systems are usually large scale, SLAs need to be formally described to enable their automated handling and protection (Dikaiakos, Katsaros, & Mehra, 2009; Durkee, 2010). A SLA ensures that organizations receive the quality of service that they expect from the CSPs (Dikaiakos et al., 2009). Also, one of the best security measures is to enforce claims by SLAs that promote continuous monitoring towards adaptive trust management (Li & Du, 2013). The quality of service integrated in the SLAs is an important issue for both CSPs and consumers who require efficient SLA management from the complete SLAs lifecycle perspective (Kyriazis, 2013; Mubeen et al., 2017). Our research findings indicate that SLAs are a significant influential factor considered in cloud computing security and is consistent with previous literature. For this reason, we encourage regional local governments to prepare and discuss SLAs parameters of interest to CSPs at different levels of provisions such as cost, security, privacy of data, and back-up.

Our research also sought to establish the relationship of cloud adoption with the people within organizations seeking cloud services. Research by Al-Hariri and Al-Hattami (2017) suggested that adopting advanced technologies within organizations has a positive impact on the way people think. Steven (2006) also posited that technology is making people more intelligent due to our novel means of obtaining, processing information and interpreting. Consequently, increasing the adoption level of advanced technologies such as cloud computing will lead to increased staff and customer comprehension of content; and in the development of skills in areas such as creative thinking, information evaluation, and problem solving (Panel, 2002).

Likewise, this research suggests adoption of cloud services has a significantly positive impact on the underlying business processes where cloud services are used. Technological advances in the past few decades have led to a significant increase in the competitive nature of the world economic business (Johnston & Carrico, 1988; Nikoloski, 2014). Companies have used computers and the Internet to transform their businesses from local workplaces into national and international competitors in the marketplace. Many companies have responded to these changes by automating their business processes and capturing industry-related information and using it to their advantage (Melville, Kraemer, & Gurbaxani, 2004). Technologies such as cloud computing have enabled business processes to remain flexible and to adapt their operations to contemporary and enhanced technological advances (Dedrick, Kraemer, & Xu, 2004).

6. Implications for theory and practice

With the rapid rise in not only the need for, but also the growth of cloud computing in governments, this research into Australian regional local governments has significant implications to theory and practice in determining cloud computing requirements from a security perspective.

6.1. Implications for theory

Research on cloud security has traditionally focused on security controls (Wang & Mu, 2011) and the technical and operational issues (Venters & Whitley, 2012; Yang & Tate, 2012), rather than security issues, at a holistic level. There is also a lack of organizational perspective into cloud security issues (Grispos et al., 2013; Nkhoma & Dang, 2013; Trigueros-preciado et al., 2013). This research integrated the ISO 27002 information security standard (ISO, 2013) with extant literature and found that operational security and compliance pose more significant government challenges than the often-highlighted technical cloud security complexities.

The international standard ISO 27002 promotes a risk management approach and suggests a number of good practice security controls for organizations; and ISO/IEC 27017 (ISO/IEC, 2015) provides additional controls for cloud computing. However, the standards fail to define specific cloud security requirements based on risk assessments, legal and contractual requirements, and business and technical requirements in an organization. This research considers new developments and challenges in the cloud security requirements, such as risk mitigation practices (Brender & Markov, 2013), shared responsibility between CSPs and customers (Liu et al., 2015), and unique and complex environments in which cloud services deliver value to customers (Ren et al., 2012). Incorporating these new developments has resulted in a new conceptual cloud computing security requirements model being proposed with four components—data security; risk assessment; legal and compliance requirements; and business and technical requirements—together with ten empirically-validated factors for consideration towards determining security requirements for cloud computing, which form the major theoretical implication of this research study.

A number of other findings from this research have implications to theoretical understanding of cloud security requirements. While this research confirmed the role of technical complexities of cloud security in terms of data security, as well as business and technical requirements towards adoption of cloud services (Fernandes et al., 2014; Zissis & Lekkas, 2012), it also re-affirmed the role of CSPs and organizations in promoting shared responsibility in managing cloud services (Liu et al., 2015). While current studies suggest cloud security control be managed based on a shared responsibility model between CSPs and organizations, our research has also argued for the dual role of risk management and employee awareness of cloud services in achieving a holistic cloud security environment, therefore, these factors must be considered in executing security controls.

Another significant implication to theory stemming from this research is the finding that the legal and contractual requirements relating to cloud security do not significantly influence cloud adoption at the local government level. This study effectively challenged the well-established notion that government regulations influence IT adoption decisions (Harauz et al., 2009). Similarly, compliance of legal and contractual requirements is a convoluted process with the presence of multiple models (e.g. PCI DSS, ISO 27001, HIPPA, SOX) that intertwine requirements (Ruiter & Warnier, 2011), thereby lacking a uniform model for compliance assessment towards cloud security. As a policy implication, this issue has been shown to have limited engagement opportunities and capacity at the local government level in Australia to form appropriate regulations and compliance measures of cloud security, compared to their state and federal government counterparts.

6.2. Implications for practice

This research provides a number of implications for practice for local governments. In particular, regional local governments provide services to its citizens and businesses and, as a result, are part of an important sector in the marketplace for software and CSPs. It is evident that CSPs need tighter and more supportive relationships with regional local governments to eliminate concerns promptly and to create

conducive environments for the successful adoption of cloud services. The findings from this research offer a number of insights for key decision-makers in local governments.

Our research highlighted concerns in terms of how risk assessment is managed in local governments. IT managers within local governments need to become innovation 'champions' and focus on reducing risks by developing appropriate risk management programs. As part of championing the innovation, the IT manager will need to outline the risk management plan to all stakeholders and organize for professional development, networking and ongoing education of existing IT staff since familiarity of using cloud technology has a direct influence on employee perceptions regarding cloud computing security (Kuan & Chau, 2001).

Using the cloud security requirements model presented in this research, local governments can introduce a trusted CSP network to ensure consistent and reliable security characteristics within the cloud environment. This can be achieved by local governments working together to demand uniform data governance requirements for security in cloud services—which can be facilitated by the proposed model.

Local governments can ensure that security control is shared between CSP and local governments whereby the shared responsibility model is not only limited to technological security aspects, but also includes the management and mitigation of the risks associated with ensuring shared obligations to data security. Likewise, the proposed model can govern CSP services that are supported by a stable security architecture, combined with consistent examination by external bodies to ensure compliance. For example, local governments can determine how to promote internal security to ensure that access controls and firewalls are conducive with cloud model security plans.

Based on the cloud security requirements model, local governments can ensure that operational risks for security and privacy issues are minimized. Local governments can make certain that senior IT staff are engaging with the CSPs, networking with other local governments, and working with external consultants to become well-informed and educated about the data interchange between their present systems and cloud services. For example, local governments can collectively request evidence from CSPs about the encryption schemes that will be used and the guidelines for the encryption of data. Similarly, local governments can jointly demand that CSPs maintain information according to relevant privacy regulations, as local governments store highly sensitive and private citizen data. This issue is becoming increasingly relevant internationally, as evidenced by the EU's move for a stringent privacy requirement, for example, the EU-GDPR introduced in May 2018.

7. Limitations and future studies

Our Study 1 qualitative investigation in this research draws on extensive engagement with IT staff in local governments while conducting interviews and collecting data. We focus on the socially constructed reality presented by the interviewees to propose an initial conceptual framework. In doing so, while we are focused on the challenges of the IT sector in local governments, our findings lack a heterogeneous view on the wider perspectives by other stakeholders in the cloud ecosystem – cloud service providers, higher level government bodies and commercial service providers. Furthermore, to ensure validity and reliability, our Study 2 quantitative questionnaire attempted to test the structural model of the research conceptual framework, again focused on the views of the local government representatives. We encourage other researchers to expand the generalizability of our proposed model given that we worked with a fairly homogeneous sample in terms of the level of government.

This study provides an Australian regional perspective and an understanding of cloud computing in local governments only. On a geographical dimension, this research was limited to the state of Queensland in Australia. This geographical limitation may inhibit generalizability of our key findings to other local governments because of the unique context of the Queensland Government's digital strategy— "Digital First" (Queensland Government, 2017)—which includes all local governments involved in this research study. This might lead to a potential bias in our findings. For this reason, empirical investigation into different local governments may be needed for more generalized findings. Future research directions could build on this research study by investigating additional critical factors that might be used to understand cloud computing security from domains beyond organization and technology aspects. Also, it would be interesting to apply the research proposed framework to other countries and to different industries or sectors. Further, the findings may also be applied to regional local governments in other different countries with similar socio-economic conditions. Small and Medium Enterprises (SMEs) usually have similar budget constraints to those of local governments, and studies on those contexts are another interesting future research consideration.

8. Conclusion

There is a lack of organizational perspective into cloud security issues. The international standard ISO 27002 promotes a risk management approach and suggests a number of good practice security controls. However, the standards fail to define specific cloud security requirements for governments based on risk assessments, legal and contractual requirements, and business and technical requirements. Incorporating these parameters into our study has resulted in a new conceptual cloud computing security requirements model comprising four components—data security; risk assessment; legal and compliance requirements; and business and technical requirements—together with ten empirically-validated factors for consideration towards determining security requirements for cloud computing in the government sector. In proposing the model, we have not only increased the scholarly insights of the security aspects of cloud computing within the local government sector, but we also intend to enable governments in weighing up the advantages of using a cloud computing security model, as proposed in this research.

Based on the first component of data security, this study identified that local governments will benefit from paying close attention to the communication capacity between their present legacy systems and cloud services. It is also important to promote internal security to ensure that access controls and firewalls are conducive with cloud security plans. As cloud computing becomes more widely used, there is a wide range of policy issues related to data storage locations, for example political considerations for government surveillance, that can have serious privacy implications. Regional local governments that have adopted, or plan to adopt, cloud-based solutions should demand that cloud service providers maintain information according to relevant privacy regulations. Based on the cloud security requirements model, local governments can ensure that operational risks for security and privacy issues are minimized by collectively demanding that cloud service providers comply with the privacy regulations, since local governments store highly sensitive and private citizen data.

According to the second component on risk assessment, the emphasis is on the role of IT leadership within the local government to engage as innovation 'champions' by focusing on reducing risk through risk management programs. It is also important to appreciate that the use of cloud services by the government is a shared responsibility around storing potentially confidential data on a system that the government may not own or control. Therefore, regional local governments should negotiate a shared responsibility model that will provide guidance to governments on the management and mitigation of the risks associated with ensuring governments' obligation to data security. Therefore, this study re-affirmed the role of cloud service providers and governments in promoting shared responsibility to manage cloud services. Equally important is building awareness on cloud security by investing more on IT-related skills, knowledge and experience of local

ARTICLE IN PRESS

government employees.

In terms of the third component of legal and compliance requirements, it is important to recognize that cloud computing amplifies the need for governance and this requires the control and oversight by the government over policies, procedures, and standards for cloud services. There is a lack of uniform model for compliance assessment towards cloud security. This study also highlighted an interesting finding that compliance was not significantly related to cloud security, suggesting that more action is required related to compliance issues in local government settings.

Finally, the component of business and technical requirements suggests the need for regional local governments to be knowledgeable in data backup, redundancy and encryption as part of cloud services. Trust is a highly significant cloud security factor while considering adoption of cloud services by local governments. Therefore, regional local governments should aim to work proactively with the cloud service providers to prepare and discuss Service Level Agreements (SLAs) at different levels of provisions such as cost, security, privacy of data, and scalability.

This research expands scholarly knowledge about the critical factors related to the security requirements for cloud computing in regional local governments. We found that technology and process maturity for cloud security requirements is high; however, operational maturity, people awareness and legal environments provide significant challenges that must be addressed in future research and practice.

We posit that our research will provide critical insights for governments that are adopting cloud services. The four components that are proposed in the cloud security requirements framework: data security; risk assessment; legal and compliance requirements; and business and technical requirements are significant considerations in determining the security requirements for cloud computing within the Australian regional local government context. This research lends considerable support to the case for identifying and understanding the impact of these factors in measuring cloud computing security, not only in local governments in Australia, but also within other government institutions and agencies, non-profit organizations and smaller business operations in Australia and other countries that possess technologically-advanced economies. To this extent, it is possible to generalize this research to other sectors/organizations that face similar and increasing calls for cloud security. Indeed, the results obtained from this research can be used as a foundation for future research in the area of cloud security. The findings of this research study are expected to assist local governments in planning and implementing cloud service to achieve their strategic objectives.

Declaration of Competing Interest

None.

References

Algirdas, A., Jean-Claude, L., Brian, R., & Carl, L. (2004). Basic concepts and taxonomy of dependable andsecure computing. *IEEE Transactions on Dependable and Secure Computing, 1*(1), 11–33.

Al-Hariri, M. T., & Al-Hattami, A. A. (2017). Impact of students' use of technology on their learning achievements in physiology courses at the University of Dammam. *Journal of Taibah University Medical Sciences, 12*(1), 82–85.

Ali, M., Khan, S. U., & Vasilakos, A. V. (2015). Security in cloud computing: Opportunities and challenges. *Information Sciences, 305*, 357–383.

Ali, O., Soar, J., & Shrestha, A. (2018). Perceived potential for value creation from cloud computing: A study of Australian regional governments. *Behaviour and Information Technology*. https://doi.org/10.1080/0144929X.2018.1488991.

Ali, O., Soar, J., & Yong, J. (2016). An investigation of the challenges and issues influencing the adoption of cloud computing in Australian regional municipal governments. *Journal of Information Security and Applications, 27*(28), 19–34.

Ali, O., Soar, J., & Yong, J. (2017). Challenges and issues that are perceived to influence cloud computing adoption in local government. *The 21st IEEE international conference on computer supported cooperative work in design* (pp. 426–432). .

Aljabre, A. (2012). Cloud computing for increased business value. *International Journal of Business and Social Science, 3*(1), 234–239.

Alshomrani, S., & Qamar, S. (2013). Cloud based e-government: Benefits and challenges. *International Journal of Multidisciplinary Sciences and Engineering, 4*(6), 1–5.

Amazon.com, Inc (2017). Object storage details - Amazon simple storage service (S3) – AWS. Accessed on June 02, 2017, available at: https://aws.amazon.com/s3/details/.

Andreica, A., Covaci, F., & Kung, J. (2015). A general model for cloud data interchange. *IEEE Computer Society,* 138–142.

Anthopoulos, L., Reddick, C. G., Giannakidou, I., & Mavridis, N. (2016). Why e-government projects fail? An analysis of the Healthcare.gov website. *Government Information Quarterly, 33*(1), 161–173.

Artz, D., & Gil, Y. (2007). A survey of trust in computer science and the semantic web. *Journal of Web Semantics: Science, Services and Agents on the World Wide Web,* 58–71.

Asesh, A. (2015). Encryption technique for a trusted cloud computing environment. *Journal of Computer Engineering, 17*(1), 53–60.

Asthana, S. (2003). Allocating resources for health and social care: The significance of reality. *Health and Social Care in the Community. 11*(6), 486–493.

Atanassov, E., Gurov, T., & Karaivanova, A. (2012). Security issues of the combined usage of grid and cloud resources. *The 35th International Convention of Information Communication Technology, Electronics and Microelectronics* (pp. 417–420). .

Ateniese, G., Burns, R., Curtmola, R., Herring, J., Kissner, L., Peterson, Z., & Song, D. (2007). Provable data possession at untrusted stores. *The ACM conference on Computer and communications security* (pp. 598–609). .

Australian Government Department of Finance. (2014). Australian government cloud computing policy: Smarter ICT Investment. Accessed on December 25, 2018, available at: https://www.finance.gov.au/sites/default/files/australian-government-cloud-computing-policy-3.pdf.

Baxter, J., Hayes, A., & Gray, M. (2011). Families in regional, rural and remote Australia. *Australian Institute of Family Studies,* 1–8.

Behl, A. (2011). Emerging security challenges in cloud computing: An insight to cloud security challenges and their mitigation. *World Congress on Information and Communication Technologies,* 217–222.

Bentler, P. M. (1992). On the fit of models to covariance's and methodology to the Bulletin. *American Psychological Association. 112*(3), 400–404.

Bentler, P. M., & Bonett, D. G. (1980). Significance tests and goodness of fit in the analysis of covariance structures. *Psychological Bulletin, 88*(3), 588–606.

Bhagawat, V. C., & Kumar, A. L. S. (2015). Survey on data security issues in cloud environment. *International Journal of Innovative Research in Advanced Engineering,* 31–35.

Bhattacherjee, A., & Premkumar, G. (2004). Understanding changes in belief and attitude toward information technology usage: A theoretical model and longitudinal test. *MIS Quarterly, 28*(2), 229–254.

Bishop, M. (2003). What is computer security? *IEEE Security & Privacy, 99*(1), 67–69.

Bollen, K. A. (1989). *Structural equations with latent variables.* New York: Wiley.

Brender, N., & Markov, I. (2013). Risk perception and risk management in cloud computing: Results from a case study of Swiss companies. *International Journal of Information Management, 33*(5), 726–733.

de Bruijn, H., & Janssen, M. (2017). Building cybersecurity awareness: The need for evidence-based framing strategies. *Government Information Quarterly, 34*(1), 1–7.

Best, S. J., Kreuger, B. S., & Ladewig, J. (2008). The effect of risk perceptions on online political participatory decisions. *Journal of Information Technology and Politics, 4*(1), 5–17.

Buyya, R., & Bubendorfer, K. (2008). *Market oriented grid and utility computing.* New York, USA: Wiley Press.

Buyya, R., Garg, S. K., & Calheiros, R. N. (2011). SLA-oriented resource provisioning for cloud computing: Challenges, architecture, and solutions. *The international conference on cloud and service computing* (pp. 1–10). .

Buyya, R., Yeo, C. S., & Venugopal, S. (2008). Market-oriented cloud computing: Vision, hype, and reality for delivering IT services as computing utilities. *The 10th IEEE international conference on high performance computing and communications* (pp. 5–13). .

Byrne, B. M. (1989). *Primer of LISREL: Basic applications and programming for confirmatory factor analytic models.* New York: Spring-Verlag.

Byrne, B. M. (1998). *Structural equation modeling with LISREL, PRELIS, and SIMPLIS: Basic concepts, applications, and programming.* Mahwah, NJ: Lawrence Erlbaum Associates, USA.

Byrne, B. M. (1999). *Structural equation modelling with LISREL, PRELIS, and SIMPLIS: Basic concepts, applications, and programming.* NJ: Lawrence Erlbaum Associates Mahwah.

Byrne, B. M. (2001). *Structural equation modelling with AMOS: Basic concepts, applications, and programming.* Mahwah, NJ: Lawrence Erlbaum Associates, USA.

Byrne, B. M. (2013). *Structural equation modeling with AMOS: Basic concepts, applications, and programming.* Routledge.

Carrico, J. C., & Smalldon, K. L. (2004). Licensed to ILL: A beginning guide to negotiating e-resources licenses to permit resource sharing. *Journal of Library Administration, 40*(1/2), 41–54.

Carson, D., Gilmore, A., Perry, C., & Gronhaug, K. (2001). *Qualitative marketing research.* London: Sage Publications.

Cebula, J. J., & Young, L. R. (2010). A taxonomy of operational cyber security. *Software engineering institute, technology note: CMU/SEI-2010-TN-028* , Pittsburgh, PA, USA.

Chang, H. H. (2006). Technical and management perceptions of enterprise information system importance, implementation and benefits. *Information Systems Journal, 16*(3), 263–292.

Chang, V., & Ramachandran, M. (2016). Towards achieving data security with the cloud computing adoption framework. *IEEE Transactions on Services Computing, 9*(1), 138–151.

Chen, D., & Zhao, H. (2011). Data security and privacy protection issues in cloud computing. *Proceedings of the IEEE International conference on Computer Science and Electronics Engineering* (pp. 647–651). .

Chen, D., & Zhao, H. (2012). Data security and privacy protection issues in cloud computing. *International conference on computer science and electronics engineering* (pp.

ARTICLE IN PRESS

647–651). .
Chin, W. W. (1998a). Issues and opinion on structural equation modeling. *MIS Quarterly, 22*(1), vii–xvi.
Chin, W. W. (1998b). The partial least squares approach to structural equation modelling. In G. A. Marcoulides (Ed.). *Modern methods for business research* (pp. I295–1336). Mahwah, NJ: Lawrence Erlbaum Associates.
Choi, M., & Lee, C. (2015). Information security management as a bridge in cloud systems from private to public organizations. *Sustainability, 7*, 12032–12051. https://doi.org/10.3390/su70912032.
Cloud Security Alliance (CSA) (2010). Top Threats to Cloud Computing V1.0. Accessed on September 02, 2016, available at https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf.
Cozby, P. C., & Bates, S. C. (2012). *Methods in Behavioural research.* New York: McGraw-Hill.
De Hert, P., & Papakonstantinou, V. (2016). The new general data protection regulation: Still a sound system for the protection of individuals. *Computer Law & Security Review, 32*(2), 179–194.
Dedrick, J., Kraemer, K. L., & Xu, S. (2004). Information technology payoff in e-business environments: An international perspective on value creation of e-business in the financial services industry. *Journal of Management Information Systems, 21*(1), 17–54.
Delaney, K. J., & Vara, V. (2007). Google plans services to store users' data. *Wall street journal*. accessed on March 16, 2018, available at: http://online.wsj.com/article/SB119612660573504716.html?mod=hps_us_whats_news.
Dennis, A. R., & Garfield, M. J. (2003). Adoption and use of GSS in project teams: Toward more participative processes and outcomes. *MIS Quarterly, 27*(2), 289–323.
Department on Innovation Industry Science and Research (2011). Cloud computing-opportunities and challenges. *IT Industry Innovation Council* (pp. 1–31). .
Dikaiakos, M., Katsaros, D., & Mehra, P. V. (2009). Cloud computing - distributed internet computing for IT and scientific research. *Internet Computing, IEEE* (pp. 10–13). .
Dillon, T., Wu, C., & Chang, E. (2010). Cloud computing: Issues and challenges. *The 24th IEEE international conference on advanced information networking and applications (AINA)* (pp. 27–33). .
Dragovic, M. (2004). Towards an improved measure of the Edinburgh handedness inventory: A one factor congeneric measurement model using confirmatory factor analyses, *Laterality: Asymmetries of Body. Brain and Cognition, 9*(4), 411–419.
Duffy, M., & Chenail, R. (2008). Values in quantitative and qualitative research. *Journal of Counselling and Values, 53*(1), 22–38.
Durkee, D. (2010). Why the cloud computing will never be free. *Communication of the ACM, 53*(5), 62–69.
Eloff, J. H. P., Eloff, M. M., Dlamini, M. T., & Zielinski, M. P. (2009). Internet of people, things and service: The convergence of security, trust and privacy. The 3rd Companion Able Workshop, Novotel Brussels, Brussels. Available at: http://hdl.handle.net/10204/4409.
Fan, W., & Yan, Z. (2010). Factors affecting response rates of the web survey: A systematic review. *Computers in Human Behavior, 26*(2), 132–139.
Faniyi, F., & Bahsoon, R. (2015). A systematic review of service level management in the cloud. *ACM Computing Surveys, 48*(3), 1–27.
Fernandes, D. A., Soares, L. F. B., & Gomes, J. V. (2014). Security issues in cloud environments: A survey. *International Journal of Information Security, 13*, 113–170.
Field, A. (2009). *Discovering statistics using SPSS.* London: SAGE Publications Ltd.
Foo, F. (2014). *Gov 'cloud first' policy has clear gaps.* The Australian Business Review. Technology Report, accessed on Sep. 15, 2018, available at: https://www.theaustralian.com.au/business/technology/gov-cloudfirst-policy-has-clear-gaps/news-story/7352591ed78077e8084c4c1d2f76e4e0.
Gaskell, G. (2000). Individual and group interviewing. In M. Bauer, & G. Gaskell (Eds.). *Qualitative Researching with Text, Image and Sound.* London: Sage.
Gerber, M., & Von Solms, R. (2008). Information security requirements–interpreting the legal aspects. *Computers & Security, 27*(5–6), 124–135.
Gholami, A., & Laure, E. (2015). Security and privacy of sensitive data in cloud computing: A survey of recent developments. *Computer Science and Information Technology,* 131–150.
Greene, J. C., & Caracelli, V. J. (1997). Defining and describing the paradigm issue in mixed-method evaluation. *New Directions for Evaluation, 74*, 5–17 San Francisco: Jossey-Bass.
Grimsley, M., & Meehan, A. (2007). E-government information systems: Evaluation-led design for public value and client trust. *European Journal of Information Systems, 16*(2), 134–148.
Grispos, G., Glisson, W. B., & Storer, T. (2013). Cloud security challenges: Investigating policies, standards, and guidelines in a fortune 500 organization. *The 21st European Conference on Information Systems, 5–8 Jun 2013, Utrecht, The Netherlands*.
Grobauer, B., Walloschek, T., & Stöcker, E. (2010). Understanding cloud computing vulnerabilities. *IEEE Security and Privacy, 99*, 50–57.
Hackney, R. A., Jones, S., & Losch, A. (2007). Towards an e-government efficiency agenda: The impact of information and communication behaviour on e-reverse auctions in public sector procurement. *European Journal of Information Systems, 16*(2), 178–191.
Hair, J. F., Anderson, R. E., Tatham, R. L., & Black, W. C. (1995). *Multivariate Data Analysis* (4th ed.). New Jersey: Prentice-Hall Inc.
Hair, J. F., Anderson, R. E., Tatham, R. L., & Black, W. C. (1998). *Multivariate Data Analysis.* Upper Saddle River, NJ: Prentice Hall.
Hair, J. F., Black, W. C., Babin, B. J., Anderson, R. E., & Tatham, R. L. (2006). *Multivariate Data Analysis* (6th ed.). Upper Saddle River, NJ: Pearson Prentice Hall.
Hair, J. F., Black, W. C., Babin, R. J., & Tatham, R. L. (2005). *Multivariate data analysis.* Upper Saddle River, New Jersey: Prentice Hall.
Hair, J., Jr., Black, W. C., Babin, B. J., & Anderson, R. E. (2010). *Multivariate data analysis; a global perspective.* New Jersey, USA: Pearson Education Inc5.
Hand, E. (2007). Head in the clouds. *Nature, 449*, 963.
Hanson, D., & Grimmer, M. (2005). The mix of qualitative and quantitative research in major marketing journals. *European Journal of Marketing, 41*(2), 58–70.
Harauz, J., Kauifman, L. M., & Potter, B. (2009). Data security in the world of cloud computing. *Proceedings in the IEEE Security and Privacy, 7*(4), 61–64.
Hashem, I. A. T., Yaqoob, I., Anuar, N. B., Mokhtar, S., Gani, A., & Khan, S. U. (2015). The rise of "big data" on cloud computing: Review and open research issues. *Information Systems, 47*, 98–115.
Heiser, J., & Nicolett, M. (2008). Assessing the security risks of cloud computing. Gartner report. Accessed by September 20, 2019available at: https://www.gartner.com/doc/685308/assessing-security-risks-cloud-computing.
Hemant, P., Chawande, N. P., Sonule, A., & Wani, H. (2011). Development of servers in cloud computing to solve issues related to security and backup. *The IEEE international conference on cloud computing and intelligence systems* (pp. 158–163). .
Henson, R. K., & Roberts, J. K. (2006). Use of exploratory factor analysis in published research: Common errors and some comment on improved practice. *Educational and Psychological Measurement, 66*(3), 393–416.
Holmes-Smith, P. (2001). *Introduction to structural equation modelling using LISREL.* Perth: ACSPRI-Winter training program.
Holmes-Smith, P. (2011). *Structural Equation Modelling Using AMOS, Australian consortium for social and political research incorporated.* Clayton: Monash University.
Holmes-Smith, P., Cunningham, E., & Coote, L. (2006). *Structural equation modelling: From the fundamentals to advanced topics.* School Research, Evaluation and Measurement Services, Education and Statistics Consultancy, Stateline.
Hsieh, H. F., & Shannon, S. E. (2005). Three approaches to qualitative content analyses. *Qualitative Health Research, 15*(9), 1277–1288.
Hu, L. T., & Bentler, P. M. (1995). Evaluating model fit. In R. H. Hoyle (Ed.). *Structural equation modelling: Concepts, issues, and applications* (pp. 76–99). Thousand Oaks, CA, US: Sage Publication.
Hulland, J., Chow, Y. H., & Lam, S. (1996). Use of causal models in marketing research: A review. *International Journal of Research in Marketing, 13*(2), 181–197.
Igbaria, M., Guimaraes, T., & Davis, G. B. (1995). Testing the determinants of microcomputer usage via a structural equation model. *Journal of Management Information Systems, 11*(4), 87–114.
International Organization for Standardization (1989). *ISO 7498-2: Information processing systems- Open Systems Interconnection.* International Organization for Standardization (ISO). accessed by April 12, 2017, available at https://www.iso.org/standards-catalogue/browse-by-ics.html.
Islam, M. K., & Hasan, R. (2016). Verifiable data redundancy in the cloud. *The IEEE International Conferences on Big Data and Cloud Computing (BDCloud), Social Computing and Networking (SocialCom), Sustainable Computing and Communications (SustainCom)* (pp. 29–36). .
Jaeger, P. T. (2007). Information policy, information access, and democratic participation: The national and international implications of the Bush administration's information politics. *Government Information Quarterly, 24*, 840–859.
Jaeger, P. T., & Bertot, J. C. (2010). Transparency and technological change: Ensuring equal and sustained public access to government information. *Government Information Quarterly, 27*(4), 371–376.
Jaeger, P. T., Lin, J., & Grimes, J. M. (2008). Cloud computing and information policy: Computing in a policy cloud. *Journal of Information Technology and Politics, 5*(3), 269–283.
Jansen, W. A. (2011). Cloud hooks: Security and privacy issues in cloud computing. *The 44th Hawaii International Conference on System Sciences (HICSS)* (pp. 1–10). .
Janssen, M., & Joha, A. (2010). Connecting cloud infrastructures with shared services. *The 11th annual international digital government research conference on public administration online: Challenges and opportunities, Pueblo, Mexico*.
Janssen, M., & Joha, A. (2011). Challenges for adopting cloud-based software as a service (SaaS) in the public sector. *European Conference on Information Systems* (pp. 1–13). .
Jensen, M., Schwenk, J., Gruschka, N., & Iacono, L. L. (2009). On technical security issues in cloud computing. *IEEE international conference on cloud computing* (pp. 109–116). .
Johnson, R. B., & Onwuegbuzie, A. J. (2004). Mixed methods research: A research paradigm whose time has come. *American Educational Researcher Association, 33*(7), 14–26.
Johnson, R. B., Onwuegbuzie, A. J., & Turner, L. A. (2007). Toward a definition of mixed methods research. *Journal of Mixed Methods Research, 1*(2), 112–133.
Johnston, H., & Carrico, S. (1988). Developing capabilities to use information strategically. *MIS Quarterly, 12*(1), 37–48.
Jones, S., Irani, Z., Sivarajah, U., & Love, P. E. D. (2019). Risks and rewards of cloud computing in the UK public sector: A reflection on three organizational case studies. *Information Systems Frontiers, 21*(2), 359–382.
Jöreskog, K. G., & Sörbom, D. (1993). *LISREL 8: Structural Equation Modeling with the SIMPLIS Command Language.* Chicago: Scientific Software International.
Juels, A., Kaliski, B. S., Jr., Bowers, K. D., & Oprea, A. M. (2013). Proof of Retrievability for Archived Files, accessed by April 26, 2017. available at: http://www.arijuels.com/wp-content/uploads/2013/09/JK07.pdf.
Julisch, K., & Hall, M. (2010). Security and control in the cloud. *Information Security Journal: A Global Perspective, 19*(6), 299–309.
Kalaiprasath, R., Elankavi, R., & Udayakumar, D. R. (2017). Cloud security and compliance - a semantic approach in end to end security. *International Journal of Mechanical Engineering and Technology, 8*(5), 482–494.
Kanthe, R. R., & Patel, R. C. (2015). Data security and privacy protection issues in cloud computing. *International Journal of Computer Science and Information Technology Research* (pp. 1130–1134). .
Kaufman, L. M. (2009). Data security in the world of cloud computing. *IEEE Security and Privacy, 7*(4), 61–64.
Kimball, M. B. (2011). Mandated state-level open government training programs.

ARTICLE IN PRESS

Government Information Quarterly, 28, 474–483.
King, N. J., & Raja, V. T. (2012). Protecting the privacy and security of sensitive customer data in the cloud. *Computer Law & Security Review, 28*(3), 308–319.
Kline, R. B. (2015). *Principles and practice of structural equation modeling.* New York: Guilford Publications.
Knapp, K. J., Denney, G. D., & Barner, M. K. (2010). Key issues in data Centre security: An investigation of government audit reports. *Government Information Quarterly, 28*(4), 533–541.
Kobielus, J. (2009). Storm clouds ahead: SOA governance clashes with cloud computing model. *Network World.* accessed by December 12, 2015, available at: http://www.networkworld.com/article/2261852/data-breach/storm-clouds-ahead.html?page=2.
Kraemer, K. L., Dedrick, J., Melville, N., & Zhu, K. (2006). *Global e-commerce: Impacts of national environments and policy.* Cambridge, UK.
Kresimir, P., & Zeljko, H. (2010). Cloud computing security issues and challenges. *The 3rd international conference on advances in human-oriented and personalized mechanisms, technologies, and Services* (pp. 344–349). .
Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computers & Security, 25*(4), 289–296.
Krumm, J. (2008). A survey of computational location privacy. *Personal and Ubiquitous Computing, 13*(6), 291–399.
Kuan, K. Y., & Chau, P. Y. K. (2001). A perception-based model for EDI adoption in small businesses using a technology-organization-environment framework. *Information and Management, 38*(8), 507–521.
Kyriazis, E. D. (2013). Cloud computing service level agreements - exploitation of research results. *European Commission Directorate General Communications Networks, Content and Technology Unit E2 – Software and Services, Cloud* (pp. 1–61). . accessed on Feb. 10, 2018, available at: http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=2496.
Lagesse, B. (2011). Challenges in securing the interface between the cloud and pervasive systems. *IEEE international conference on pervasive computing and communications workshops* (pp. 106–110). .
Leuprecht, C., Skillicorn, D. B., & Tait, V. E. (2016). Beyond the Castle Model of cyber-risk and cyber-security. *Government Information Quarterly, 33*(2), 250–257.
Li, X., & Du, J. (2013). Adaptive and attribute-based trust model for service-level agreement guarantee in cloud computing. *IET Information Security, 7*(1), 39–50.
Liang, Y., Qi, G., Wei, K., & Chen, J. (2017). Exploring the determinant and influence mechanism of e-government cloud adoption in government agencies. *Government Information Quarterly, 34*(3), 481–495.
Liu, L., Yu, E., & Mylopoulos, J. (2003). Security and privacy requirements analysis within a social setting. *The 11th IEEE International Requirements Engineering Conference* (pp. 151–161). .
Liu, S. M., & Kim, Y. (2018). Special issue on internet plus government: New opportunities to solve public problems? *Government Information Quarterly, 35*(1), 88–97.
Liu, Y., Sun, Y., Ryoo, J., Rizvi, S., & Vasilakos, A. V. (2015). A survey of security and privacy challenges in cloud computing: Solutions and future directions. *Journal of Computing Science and Engineering, 9*(3), 119–133.
Local Government Association Queensland LGAQ (2013). Digital productivity report. *Local Government Association Queensland,* 1–36.
Maches, B. (2010). The impact of cloud computing on corporate IT governance. *HBC Wire.* Accessed by December 10, 2015, available at: https://www.hpcwire.com/2010/01/25/the_impact_of_cloud_computing_on_corporate_it_governance/.
Mahmood, Z. (2011). Data location and security issues in cloud computing. *IEEE international conference on emerging intelligent data and web technologies* (pp. 49–54). .
Marsh, H. W., Balla, J. R., & McDonald, R. P. (1988). Goodness-of-fit indexes in confirmatory factor analysis: The effect of sample size. *Psychological Bulletin, 103*(3), 391–410.
Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J., & Ghalsasi, A. (2011). Cloud computing: The business perspective. *Decision Support Systems, 51*(1), 176–189.
Mather, T., Kumaraswamy, S., & Latif, S. (2009). *Cloud security and privacy: An enterprise perspective on risks and compliance.* Sebastopol, CA, USA: O'Reilly Media.
Melville, N., Kraemer, K., & Gurbaxani, V. (2004). Review: Information technology and organizational performance: An integrative model of IT business value. *MIS Quarterly, 28*(2), 283–322.
Miles, M. B., Huberman, A. M., & Saldana, J. (2014). *Qualitative data analysis.* London: Sage Publications.
Misuraca, G., Broster, D., & Centeno, C. (2012). Digital Europe 2030: Designing secnarios for ICT in future governance and policy making. *Government Information Quarterly, 29*, 121–131.
Morgan, D. L. (1998). Practical strategies for combining qualitative and quantitative methods: Applications to health research. *Qualitative Health Research, 8*, 362–376.
Mubeen, S., Asadillah, S. A., Papadopouls, A. V., Ashjaei, M., Pei-Breivold, H., & Behnam, M. (2017). Management of service level agreements for cloud services in IoT: A systematic mapping study. *Journal of IEEE Access.* 1–25.
Mueller, R. O. (1997). Structural equation modeling: Back to basics. Structural equation modeling. *A Multidisciplinary Journal, 4*(4), 353–369.
Myers, M. D., & Avison, D. (1997). Qualitative research in information systems. *MIS Quarterly, 21*, 241–242.
Nagarajan, A., & Varadharajan, V. (2011). Dynamic trust enhanced security model for trusted platform based. *Future Generation Computer Systems* (pp. 564–573). .
Niehaves, B., Plattfaut, R., & Becker, J. (2013). Business process management capabilities in local governments: A multi-method study. *Government Information Quarterly, 30*(3), 217–225.
Nikoloski, K. (2014). The role of information technology in the business sector. *International Journal of Science and Research, 3*, 303–309.
NIST (2009). *Cloud computing.* National Institute of Standards and Technology. accessed on October 27, 2015, available at: http://csrc.nist.gov/groups/SNS/cloudcomputing/.
Nkhoma, M., & Dang, D. (2013). Contributing factors of cloud computing adoption: A technology-organization-environment framework approach. *International Journal of Information System and Engineering, 1*, 38–49.
Norman, J. (2012). Why redundancy in the cloud is a marvellous thing. *Cloud computing security*. accessed on Jan. 21, 2018, available at: https://cloudtweaks.com/2012/06/cloud-redundancy/.
Oliveira, T., & Martins, M. F. O. (2010). Understanding e-business adoption across industries in European countries. *Industrial Management and Data Systems, 110*(9), 1337–1354.
Ozkan, S., & Kanat, I. E. (2011). E-government adoption model based on theory of planned behaviour: Empirical validation. *Government Information Quarterly, 28*, 503–513.
Panel, I. L. (2002). Digital transformation: A framework for ICT literacy. *Educational Testing Service* (pp. 1–53). Report of the international ICT literacy panel.
Paquette, S., Jaeger, P. T., & Wilson, S. C. (2010). Identifying the security risks associated with governmental use of cloud computing. *Government Information Quarterly, 27*(3), 245–253.
Patton, M. Q. (2002). *Qualitative research and evaluation methods.* Thousand Oaks, CA: Sage Publications.
Pearson, S. (2009). Taking account of privacy when designing cloud computing services. *ICSE Workshop on Software Engineering Challenges of Cloud Computing, IEEE Computer Society Washington, DC, USA* (pp. 44–52). .
Pearson, S., & Benameur, A. (2010). Privacy, security and trust issues arising from cloud computing. *The 2nd IEEE international conference on cloud computing technology and science* (pp. 693–702). .
Pee, L. G., & Kankanhalli, A. (2016). Interactions among factors influencing knowledge management in public-sector organizations: A resource-based view. *Government Information Quarterly, 33*(1), 188–199.
Poolsappasit, N., Kumar, V., Madria, S., & Chellappan, S. (2011). Challenges in secure sensor-cloud computing. *The International Conference on Secure Data Management* (pp. 70–84). .
PopMell, P., & Grance, T. (2009). *Draft NIST working definition of cloud computing. 15*, 1–7.
Price, M. (2011). Pinning down the cloud. *The Wall Street Journal, R3*.
Punch, K. F. (1998). *Introduction to social research: Quantitative and qualitative approaches.* Thousand Oaks, CA: Sage Publications.
Queensland Government (2017). Digital 1st: Advancing our digital future. *The Queensland Government Digital Strategy for 2017-2022*. Accessed on December. 15, 2018, available at: https://digital1st.initiatives.qld.gov.au/documents/digital-strategy.pdf.
Ramgovind, S., Eloff, M. M., & Smith, E. (2010). The management of security in cloud computing. *IEEE international conference on cloud computing* (pp. 1–7). .
Rao, H. S., & Perry, C. (2007). Convergent interviewing: A starting methodology for an Enterprise research program. In D. Hine, & D. Carson (Eds.). *Innovative Methodologies in Enterprise Research* (pp. 86–100). Northampton, Massachusetts: Edward Elgar.
Ren, K., Wang, C., & Wang, Q. (2012). Security challenges for the public cloud. *IEEE Internet Computing, 16*(1), 69–73.
Robson, C. (2002). *Real world research: A resource for social scientists and practitioner-researchers.* Oxford: Wiley-Blackwell.
Roger, E. M. (2003). *Diffusion of innovations* (5th ed.). New York: Free Press.
Ruiter, J., & Warnier, M. (2011). *Computers, privacy and data protection: An element of choice.* Springer Netherlands361–376.
Sale, J. E. M., Lohfeld, L., & Brazil, K. (2002). Revisiting the quantitative-qualitative debate: Implications for mixed-methods research. *Quality and Quantity, 36*(1), 43–53.
Schermelleh-Engel, K., Moosbrugger, H., & Müller, H. (2003). Evaluating the fit of structural equation models: Tests of significance and descriptive goodness of-fit measures. *Methods of Psychological Research, 8*(2), 23–74.
Schilling, J. (2006). On the pragmatics of qualitative assessment: Designing the process for content analysis. *European Journal of Psychological Assessment, 22*(1), 28–37.
Scupola, A. (2003). The adoption of internet commerce by SMEs in the south of Italy: An environmental, technological and organizational perspective. *Journal of Global Information Technology Management, 6*(1), 52–71.
Shaughnessy, J. J., Zechmeister, E. B., & Zechmeister, J. S. (2012). *Research Methods in Psychology* (9th). New York: McGraw-Hill.
Sheppard, D. (2014). Is loss of control the biggest hurdle to cloud computing? Accessed on October 24, 2017, available at: http://www.itworldcanada.com/blog/isloss-ofcontrol-the-biggest-hurdle-to-cloud-computing/95131.
Shin, D. H. (2013). User centric cloud service model in public sectors: Policy implications of cloud services. *Government Information Quarterly, 30*(2), 194–203.
Singla, S., & Singh, J. (2013). Cloud data security using authentication and encryption technique. *International Journal of Advanced Research in Computer Engineering and Technology, 2*(7), 2232–2235.
Sivarajah, U., Irani, Z., & Weerakkody, V. (2015). Evaluating the use and impact of Web 2.0 technologies in local government. *Government Information Quarterly, 32*(4), 473–487.
Soffer, P., & Hadar, I. (2007). Applying ontology-based rules to conceptual modelling: A reflection on modelling decision making. *European Journal of Information Systems, 16*(5), 599–611.
Softlayer. (2009). Service Level Agreement and Master Service Agreement, accessed by April 10, 2016, available at: http://www.softlayer.com/sla.htmlS.
Song, M., Van Der Bij, H., & Weggeman, M. (2005). Determinants of the level of knowledge application: A knowledge-based and information-processing perspective. *Journal of Product Innovation Management, 22*(5), 430–444.
Stafford, T. F., & Turan, A. H. (2011). Online tax payment systems as an emergent aspect of governmental transformation. *European Journal of Information Systems, 20*(3), 343–357.

ARTICLE IN PRESS

Stergiou, C., Psannis, K. E., Kim, B. G., & Gupta, B. (2018). Secure integration of IoT and cloud computing. *Future Generation Computer Systems, 78*, 964–975.
Steven, J. (2006). Everything bad is good for you: How today's popular culture is actually making us smarter. *New York Time*.
Stine, K., Kissel, R., Barker, W. C., Fahlsing, J., & Gulick, J. (2008). *Guide for mapping types of information and information systems to security categories.* National Institute of Standards and Technology (NIST). accessed by April 10, 2017, available at: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-60v1r1.pdf.
Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications, 34*(1), 1–11.
Swisher, L. L., Beckstead, J. W., & Bebeau, M. J. (2004). Factor analysis as a tool for survey analysis using a professional role orientation inventory as an example. *Physical Therapy, 84*(9), 784–799.
Tabachnick, B. G., & Fidell, L. S. (2001). *Using multivariate statistics* (4th ed.). Needham Heights, Mass: Allyn and bacon.
Takabi, H., Joshi, J. B. D., & Ahn, G. J. (2010). Security and privacy challenges in cloud computing environments. *IEEE Security and Privacy, 8*(6), 24–31.
Tan, X., & Ai, B. (2011). The issues of cloud computing security in high-speed railway. *IEEE international conference on electronic and mechanical engineering and information technology* (pp. 4358–4363). .
Teddlie, C., & Tashakkori, A. (2009). *Foundations of mixed methods research.* Thousand Oaks, CA: Sage Publications.
Thompson, B. (2007). Exploratory and confirmatory factor analysis: Understanding concepts and applications. *Washington, DC: American Psychological Association, 31*(3), 245–248.
Trigueros-preciado, S., Perez-gonzalez, D., & Solana-gonzalez, P. (2013). Cloud computing in industrial SMEs: Identification of the barriers to its adoption and effects of its application. *Electron Markets, 23*(2), 105–114.
Urbach, N., & Ahlemann, F. (2010). Structural equation modeling in information systems research using partial least squares. *Journal of Information Technology Theory and Application, 11*(2), 4–40.
Van Zoonen, L. (2016). Privacy concerns in smart cities. *Government Information Quarterly, 33*, 472–480.
Vandenberg, R. J. (2006). Statistical and methodological myths and urban legends. *Organizational Research Methods, 9*(2), 194–201.
Vault (2014). Australia's Cloud First Policy. accessed by April 11, 2018, available at: https://vaultcloud.com.au/cloud-first-policy/.
Venkatesh, V., Brown, S. A., & Bala, H. (2013). Bridging the qualitative-quantitative divide: Guidelines for conducting mixed methods research in information systems. *MIS Quarterly, 37*(1), 21–54.
Venters, W., & Whitley, E. A. (2012). A critical review of cloud computing: Researching desires and realities. *Journal of Information Technology, 27*(3), 179–197.
Walsham, G. (2006). Doing interpretive research. *European Journal of Information Systems, 15*(3), 320–330.
Wang, J., & Mu, S. (2011). Security issues and countermeasures in cloud computing. *IEEE international conference on Grey systems and intelligent Services* (pp. 843–846). .
Waters, D. (2011). *Quantitative methods for business.* England: Pearson Education Limited.
Whitman, M. E. (2012). *Principles of information security* (4th). Boston, MA: Course Technology.
Wholey, J. S., Hatry, H. P., & Newcomer, K. E. (2004). *Handbook of practical program evaluation.* San Francisco: John Wiley and Sons, Inc.
Williams, B., Brown, T., & Onsman, A. (2010). Exploratory factor analysis: A five step guide for novices. *Australasian Journal of Para-medicine, 8*(3), 1–13.
Wyld, D. C. (2009). *Moving to the cloud: An introduction to cloud computing in government. E-government series.* IBM Centre for the Business of Government1–83.
Yadav, N., & Singh, V. B. (2012). E-governance: Past, present and future in India. *International Journal of Computer Applications, 53*(7), 36–48.
Yang, H., & Tate, A. (2012). A descriptive literature review and classification of cloud computing research. *Communications of the Association for Information Systems, 31*(2), 35–60.
Yimam, D., & Fernandez, E. B. (2016). A survey of compliance issues in cloud computing. *Journal of Internet Services and Applications, 7*(5), 1–12.
Zhang, Q., Cheng, L., & Boutaba, R. (2010). Cloud computing: State-of-the-art and research challenges. *Journal of Internet Services Application, 1*(1), 7–18.
Zhang, Q., Cheng, L., & Boutaba, R. (2010a). Cloud computing: State-of-the-art and research challenges. *Journal of Internet Services and Applications, 1*(1), 7–18.
Zhang, X., Wuwong, N., Li, H., & Zhang, X. (2010). Information security risk management framework for the cloud computing environments. *The IEEE 10th international conference on computer and information technology* (pp. 1328–1334). .
Zhang, Z., Waszink, A., & Wijngaard, J. (2000). An instrument for measuring TQM implementation for Chinese manufacturing companies. *International Journal of Quality and Reliability Management, 17*(7), 730–755.
Zhao, Y., & Fan, B. (2018). Exploring open government data capacity of government agency: Based on the resource-based theory. *Government Information Quarterly, 35*(1), 1–12.
Zhu, K., & Kraemer, K. L. (2005). Post-adoption variations in usage and value of e-business by organizations: Cross-country evidence from the retail industry. *Information Systems Research, 16*(1), 61–84.
Zhu, X. (2017). The failure of an early episode in the open government data movement: A historical case study. *Government Information Quarterly, 34*(2), 256–269.
Zikmund, W., Babin, B., Carr, J., & Griffin, M. (2012). *Business research methods.* Mason, USA: Cengage Learning.
Zikmund, W. G., Babin, B. J., Carr, J. C., & Griffin, M. (2013). *Business research methods* (9th edn). USA: South-Western, Cengage Learning.
Zissis, D., & Lekkas, D. (2011). Securing e-government and e-voting with an open cloud computing architecture. *Government Information Quarterly, 28*(2), 239–251.
Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. *Future Generation Computer Systems, 28*, 583–659.

Omar Ali is PhD in information systems at University of Southern Queensland, Australia. He had two master degree. The first one in information and communication technology, and the second one in information systems and technology by research, both of the master degree from University of Wollongong. He is sessional staff in Information Systems with the School of Management and Enterprise within the Faculty of Business, Education, Law, and Art at University of Southern Queensland in Australia. His research interests include RFID; cloud computing; Blockchain technology; IT governance; information system security; System analysis and design, and research methodology. He is reviewer for many leading journals including Government Information Quarterly, Information Systems Management, Behaviour and Information Technology, Industrial Management and Data Systems, and Computer Standards and Interfaces. Also, he has published in International Journal of Information Management, Behaviour and Information Technology, Journal of Information Security and Applications, Journal of Web Intelligent, Services Transactions on Cloud Computing, and Journal of Contemporary Issues in Business and Government.

Anup Shrestha is a lecturer and PhD in Information Systems from the University of Southern Queensland, Australia. His research interests include IT service management, process assessment, software engineering, IT standards, design science research, cloud computing and knowledge management. His PhD research, working on an Australian Research Council (ARC) industry linkage grant in the IT Service Management industry, was awarded the best Australian PhD in Information Systems ACPHIS (Australian Council of Professors and Heads of Information Systems) prize in 2016 and the Queensland IT innovation award in 2015. He is currently serving as the Standards Australia national representative for the development and review of ISO/IEC JTC1/SC7 standards of software engineering. He has published in Information and Management, International Journal of Information Management, Computer Standards & Interfaces, Behaviour and Information Technology, Journal of Networks and Journal of Decision Systems. Prior to his academic journey, Anup worked in the IT industry where his career progressed from programmer to project manager for 8 years.

Akemi Takeoka Chatfield, M.B.A. and Ph.D. in Business Administration (MIS & Management Sciences summa cum laude) from Texas Tech University in the U.S. Dr. Chatfield is director, E-Government & E-Governance Research Group within the Centre for Big Data Analytics and Intelligent Systems and senior lecturer in Information Technology with the School of Computing and Information Technology within the Faculty of Engineering and Information Sciences at University of Wollongong in Australia. Her research interests include networked organizations, network technology benefits realization, social media and government, social network analysis, big data analytics, and open data policy. She published in Journal of Management Information Systems, European Journal of Information Systems, Journal of Information Systems Frontier, Communications of the ACM, Data Base, Information Technology for Development, International Journal of Electronic Governance, Electronic Journal of E-Government, International Journal of Public Administration in the Digital Age, Government Information Quarterly, Information Polity, Social Sciences Computer Review, and Journal of Homeland Security and Emergency Management.

Peter A. Murray is currently Professor of Management at the University of Southern Queensland. Professor Murray is an applied researcher in strategic change and diversity management and lectures more broadly in strategic management, change management and human resource management. He is also an associate editor, editorial board member and reviewer for many leading journals including Human Resource Management Journal, International Journal of Human Resources, Personnel Management and Management Learning. His most recent co-authored book titled 'The Palgrave Handbook of Knowledge Management' was published in May 2018. Professor Murray has been a leading researcher in many Government reports, books and Quartile 1 ranked journal articles such as Human Resource Management Journal, Management Learning, Supply Chain Management, International Journal of Human Resource Management and Asia Pacific Journal of Human Resources.