Proceedings Paper:
Peng, G.C., Dutta, A. and Choudhary, A. (2014) Exploring critical risks associated with enterprise cloud computing. In: Leung, V.C.M. and Chen, M., (eds.) Cloud Computing. 4th International Conference on Cloud Computing, 17th - 19th October 2013, Wuhan, China. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, 133 . Springer International Publishing , 132 - 141.

https://doi.org/10.1007/978-3-319-05506-0_13

Exploring Critical Risks Associated with Enterprise Cloud Computing

Guo Chao Alex Peng[1]*, Arnab Dutta[1], and Alok Choudhary[2]

[1]Information School, University of Sheffield, Regent Court, Sheffield, S1 4DP, UK
[2] Management School, University of Sheffield, IWP Building, Sheffield, S10 2TN, UK
{g.c.peng, ADutta2, a.choudhary}@sheffield.ac.uk

Abstract. While cloud computing has become an increasingly hot topic in the industry, risks associated with the adoption of cloud services have also received growing attention from researchers and practitioners. This paper reports the results of a study that aimed to identify and explore potential risks that organisations may encounter when adopting cloud computing, as well as to assess and prioritise the identified risks. The study adopted a deductive research method based on a cross-sectional questionnaire survey. The questionnaire was distributed to a group of 295 carefully selected and highly experienced IT professionals, of which 39 (13.2%) responses were collected and analysed. The research findings identified a set of 39 cloud computing risks, which concentrated around diverse operational, organisational, technical, and legal areas. It was identified that the most critical risks were caused by current legal and technical complexity and deficiencies associated with cloud computing, as well as by a lack of preparation and planning of user companies.

Keywords: Cloud computing, Risks, Legal, Organisational, Operational, Technical.

1 Introduction and Background of Study

In order to sustain business competitiveness in the digital age, modern organisations have implemented and used an increasing number of information technology (IT) applications and possessed an ever complicated IT infrastructure. These IT resources (such as, data, software, PCs, CPUs, memory cards, and servers) are traditionally hosted and maintained by user organisations internally. However, the increasing number of internal IT facilities and resources has now become very costly and time-consuming for user companies to maintain. Consequently, organisations nowadays are facing the dilemma to remain high usage of advanced IT applications to sustain competitiveness on the one hand, and to substantially reduce their IT operation and maintenance costs on the other hand. With the development of new IT and web technologies, cloud computing emerges in late 2000s as a solution to this IT dilemma.

Cloud computing is an advanced IT model to host and share both software and hardware resources over the Internet. It allows organisations to use a pool of IT resources and applications as services virtually through the web, without physically holding these computing resources internally [1]. Nowadays organizations are increasingly looking for adopting the various cloud services for supply-chain

integration and access to real-time data. Cloud computing provides the facility to access shared resources and common infrastructure, offering services on demand over the network to meet changing business needs [1]. It also promises to deliver high-quality and advanced IT services to organisations with substantially reduced costs [2], such as reduced hardware investments, less maintenance fees, and lower electricity consumption associated with IT usage. In this context, cloud computing can also be perceived as one of the green technologies that enables environmentally sustainable use of IT in modern organisations in the long term.

However, despite these very attractive facts, migrating the hitherto internal IT resources and sensitive business data to a third-party cloud vendor is never an easy decision to be made by CEOs, CIOs and IT managers. In fact, the adoption of cloud computing is associated with a wide range of potential risks and challenges. For instance, the inherent features of cloud computing determine that IT operation within a third-party cloud provider will be by no means transparent to user companies, who also have limited control on the subscribed cloud services [3]. Such lack of transparency and control may raise potential risks related to the security and privacy of business and customer data stored in the cloud [1]. Moreover, user companies need to make a range of internal changes (e.g. designing new business processes, refining IT roles, and downsizing IT department) to prepare themselves to the new cloud environment [4]. This however may potentially lead to job dissatisfaction of in-house IT and business staff. Consequently, fully exploring and understanding these cloud risks and challenges is fundamental for organisations to decide strategically whether or not cloud computing is the right tool for them, as well as to better prepare them to deal with the potential cloud problems and thus avoid severe technical failure and business disasters.

This paper reports a study that aimed to identify, explore and assess a comprehensive list of risks associated with cloud computing. A systematic literature review was carried out at the early stage of the research. As a result of this extensive review, the researchers established a theoretical risk ontology that contains 39 potential risks that organisations may encounter during cloud computing adoption and usage. A questionnaire was constructed based on this theoretical risk ontology and it was used to seek IT professionals' perceptions of the established cloud risks. This paper is organized in the following manner. The next section of the paper presents the research methodology including a discussion of the theoretical risk ontology and the research questionnaire design. Section 3 presents the analysis and results derived from the questionnaire survey. Finally, section 4 concluded this study with a note of its research and practical implications.

2 Research methodology

2.1 The theoretical risk ontology

In order to establish an explicit IT lens to frame the study and generate data collection tools, a desktop study, based on the process of a critical literature review, was carried out at the early stage of the research. As discussed above, an initial literature review

of the study identified that current research on cloud computing risks has been very limited and focused mainly on security and privacy aspects. Faced with this scarcity of studies on the topic, a more extensive literature review was conducted. This critical review followed the systematic approach proposed by Peng and Nunes [5, 6]. Specifically, apart from reviewing studies that directly address cloud computing risks, this systematic review also covers general IT and computing journal papers, conference proceedings, books, industrial white papers, and technical reports. The purpose here was "to identify broadly any possible factors and issues that might lead to potential" cloud computing failure [5]. This endeavour resulted in the identification of a large amount of valuable literature, which addressed various IT, cloud computing, legal, and business issues. Subsequently, these retrieved articles and materials were "systematically and critically analysed, compared and synthesised, and then used as raw materials to construct arguments and standpoints for risk identification" [5]. Consequently, through this extensive and critical literature review, the researchers established and proposed a set of 39 potential cloud computing risks. A risk ontology is then developed to organise and present these identified cloud risks (Figure 1 below).

As shown in Figure 1, the established cloud risks were organised into 4 main categories and 12 sub-categories in the risk ontology. The 4 main risk categories include:

- *Organisational risks (OGR).* Cloud adoption can lead to significant impacts on diverse organisational aspects, such as IT governance, compliance to industrial regulations, in-house IT experts, and IT planning. Risks related to these organisational and managerial aspects are categorised as organisational risks.
- *Operational risks (OPR).* The adoption of cloud computing significantly changes the hitherto internal IT and business operations in user companies. Risks affecting daily business and IT operations are thus categorised as operational risks.
- *Technical risks (TR).* The complicated cloud infrastructure and inherent IT deficiencies existed in the company can raise a set of technical risks during cloud computing adoption.
- *Legal risks (LR).* The nature and inherent features of cloud computing can lead to a range of legal risks related to data privacy, intellectual property, and contracts.

In order to examine and explore the suitability of this theoretical risk ontology in current cloud computing practices, a deductive research design based on a cross-sectional questionnaire survey was selected and used as the suitable data collection tool of this study, as further discussed below.

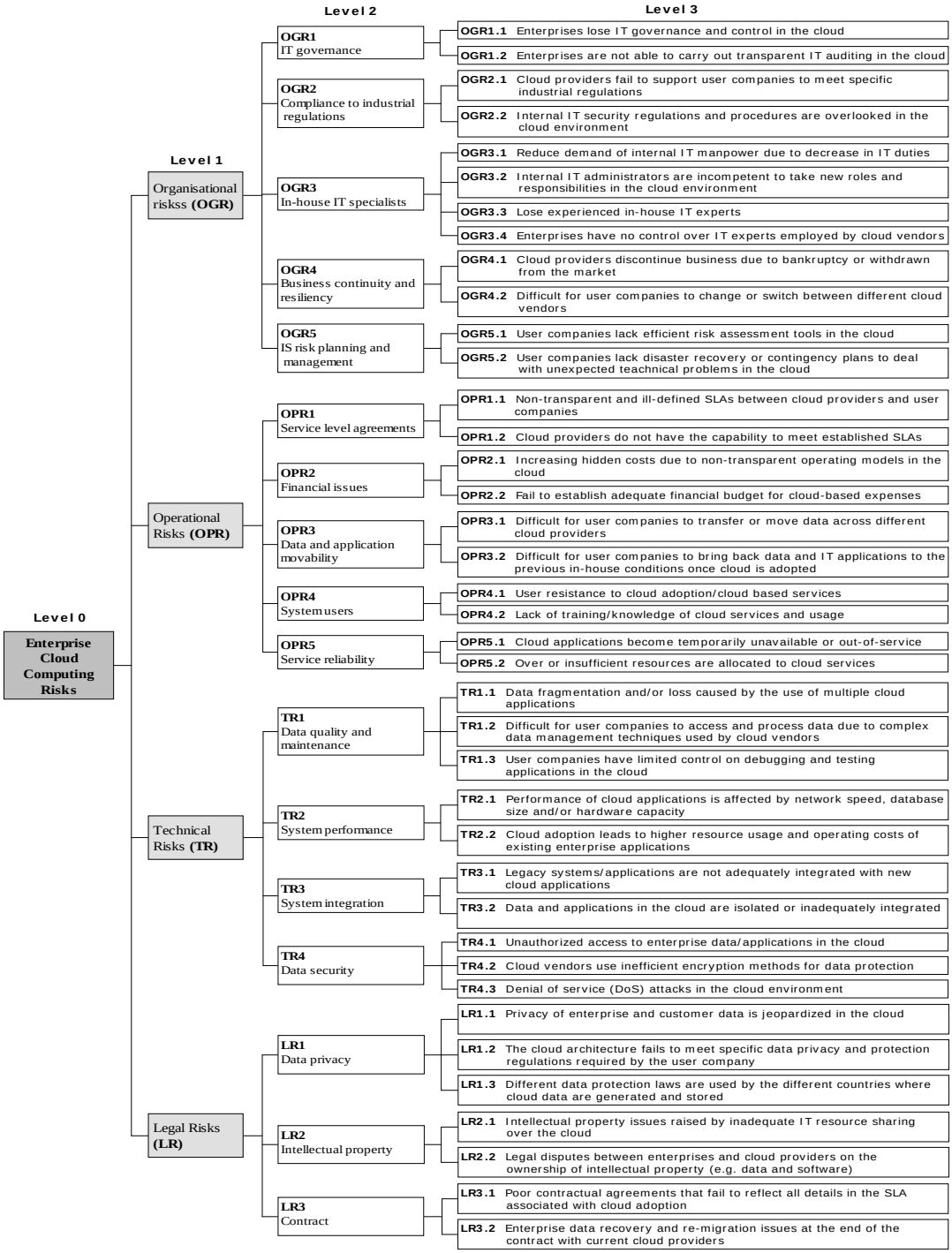

Fig. 1. The ontology of cloud computing risks

2.2 The questionnaire design

The questionnaire began by asking general questions related to respondents' previous experience of IT, cloud computing, and risk assessment. Subsequently, the main part of the questionnaire was designed by using the cloud risk ontology as the theoretical basis. In detail, the researchers attempted to identify which of the 39 established events would be perceived by respondents as risks for cloud adoption, and to explore respondents' perceptions on the importance of each identified risk based on its probability of occurrence, level of impact, and frequency of occurrence. In order to achieve these purposes, each predefined risk event was examined in the questionnaire through four questions:

1) Whether this event can be perceived as a risk to cloud adoption (1 = yes, 2= no).
2) What the perceived probability of occurrence of this risk event will be (measured on a 3-point Likert scale, ranging from high [3] to low [1]).
3) What level of impact this risk is perceived to result in (measured on a 3-point Likert scale, ranging from high [3] to low [1]).
4) What the perceived frequency of occurrence of this risk event will be (measured on a 5-point Likert scale, ranging from very often [5] to very rarely [1]).

Moreover, it was expected that stakeholders, who are interested in cloud computing and have the necessary cloud knowledge to answer the questionnaire, should have good computer literate skills. These potential respondents of the questionnaire thus may prefer filling in the questionnaire electronically, rather than in the traditional paper-based format. Therefore, this questionnaire was developed and conducted electronically.

2.3 Target respondents

It was considered that cloud computing as a relatively new concept may not currently be fully understood by business managers and users, who thus may not have sufficient insights on the cloud computing risks explored in this study. In contrast, IT consultants and experts working in the frontier areas of the IT industry were expected to hold more in-depth knowledge on cloud computing issues. These considerations led the researchers to select IT professionals and consultants as the prospective respondents of the designed questionnaire. Moreover, Linkedin as a social networking site has been increasingly used by professionals to establish and maintain personal and specialist networks. This networking site was thus used as a valuable resource to identify and select potential IT specialists to get involved in the survey. In order to identify and choose suitable IT professionals registered on Linkedin to be involved in the survey, a set of selection criteria were established and used. In particular, the prospective respondents should:

- Have at least 3 years of professional IT experience;
- Have experience and/or knowledge of cloud computing;
- Have experience in IT risk assessment and management.

By using these criteria, a sample of 295 highly-qualified IT professionals registered on Linkedin was identified and selected to participate in this questionnaire survey.

An invitation email, which contained 1) a covering letter to explain the purpose of the study, and 2) the URL to the online questionnaire, was sent to these 295 IT professionals. Three weeks after the original email, a reminder was sent out. With these efforts, a total of 39 valid and usable responses were received, representing a response rate of 13.2%.

3 Data Analysis and Findings

3.1 Overall risk findings

The questionnaire findings show that all of the 39 events contained in the risk ontology were perceived by the majority (86%) of the respondents as risk events to cloud computing adoption. Nonetheless, these risks were perceived to have different levels of importance. In particular, the questionnaire asked respondents to assess the importance of each risk item from three dimensions, namely perceived probability of occurrence, level of impact, and frequency of occurrence. The need for all this information lies in the fact that from a risk management perspective, a risk event that has a high probability of occurrence may not have a high impact, and vice versa. Moreover, while probability refers to 'how likely' a risk event may occur, frequency refers to 'how often' this event may happen. Therefore, when evaluating the importance of a risk event, it is necessary and vital to take into account all these three risk aspects [7]. Consequently, and in order to facilitate risk assessment, the following formula was developed:

$$\textit{Risk score of each cloud computing risk} = \Sigma\ [W\ *(\textit{Probability} + \textit{Impact} + \textit{Frequency})]$$

This formula was initially established and proposed by Peng and Nunes [7] and then further improved by Pan et al [8], which aimed to identified and assessed ERP post-implementation risks. Because the structure of this formula is consistent with and clearly reflects the questionnaire design of this research, it is adopted as a suitable method to assess cloud computing risks in this study. Based on this formula, the calculation of the risk score for each identified risk event should go through the following 3 steps:

Step 1 *(Probability + Impact + Frequency)*: sum up the values given by each respondent for the three independent dimensions of a risk event, namely perceived probability of occurrence (i.e. high = "2", medium = "1", low = "0.5"), perceived level of impact (i.e. high = "2", medium = "1", low = "0.5"), and perceived frequency of occurrence (i.e. 5 values from very often to very rarely = "2", "1.5", "1", "0.75" and "0.5").

Step 2 *W*(Probability + Impact + Frequency)*: 'W' refers to whether or not the respondent perceived this risk event as a cloud computing risk, with '1' stands for 'yes' and '0' means 'no'. In case that the respondent did not perceive the given risk event as a cloud computing risk, the formula will turn the value generated from Step 1 into 0.

Step 1 and 2 thus generate the individual score that each respondent gave for a specific risk event.

Step 3 Σ *[W*(Probability + Impact + Frequency)]*: sum up the individual score that each of the 39 respondents of the survey gave for a particular risk event, and thus generate the total risk score that this risk event received.

By using this formula, the researchers calculated the risk scores for all of the 39 cloud computing risks identified, and then prioritised these risks based on their risk scores. The top 10 cloud risks ranked by their risk scores are shown in Table 1. These top 10 risks were identified as the most critical to current cloud computing practice.

Table 1. Top 10 cloud computing risks as perceived by IT experts

Rank	***Risk ID***	***Top 10 Critical Risk Events for Cloud Computing***	***Risk Score (n=39)***
1	LR1.1	Privacy of enterprise or customer data is jeopardised in the cloud	153.50
2	LR1.3	Inconsistent data protection laws adopted by different countries where cloud data are generated and stored	151.75
3	OGR4.2	Difficult for user companies to change cloud vendors even in the case of service dissatisfaction (also known as vendor lock-in)	148.50
4	OGR5.2	User companies lack disaster recovery and contingency plans to deal with unexpected technical issues in cloud environment	147.75
5	LR3.2	Enterprise data re-migration difficulties at the end of the cloud contract	140.25
6	OPR4.2	Inadequate user training/knowledge on cloud services and usage	139.75
7	OPR5.1	Cloud applications become temporarily unavailable or out-of-service	137.25
8	OPR2.1	Increasing hidden costs due to non-transparent operating models in the cloud	136.00
9	TR4.3	Denial-of-Service (DoS) attacks in the cloud environment	135.50
10	TR4.1	Unauthorised access to enterprise data/applications	135.00

As discussed above, when sensitive business and customer data is processed by third-party service providers outside the organisation, business managers of user companies are less immediately aware of the occurrence of any risks in the cloud, and also have no direct ability to control and manage these risks [9]. These inherent features in the cloud raise immediate concerns and risks related to data privacy and security, which have been the main focus of the majority of current academic studies [e.g. 10, 11, 12] and industrial reports [e.g. 9] on cloud computing. The findings of this study confirmed that data privacy and security risks represent some of the significant challenges in the cloud. However, the findings also identified that the most critical cloud computing risks do not just cluster around privacy and security aspects. That is, critical cloud risks as shown in Table 1 were also found across diverse legal, operational and business areas. Therefore, it seems that potential failure

of cloud computing adoption may not just be simply attributed to privacy and security risks, but may also be triggered by various operational, organisational, and managerial problems related to both cloud vendors and user companies. In order to validate this conclusion, a further bivariate analysis was carried out to explore potential casual relationships between the cloud computing risks identified, as presented below.

3.2 Correlations between the identified cloud computing risks

A bivariate analysis is a statistical technique that aims at identifying the correlation between two variables. In this study, the researchers used bivariate analysis to explore potential relationships between the identified cloud computing risks. Specifically, we aimed to explore that when the probability of occurrence of Risk A (e.g. inconsistent data protection laws adopted by different countries where cloud data are stored) was perceived to be high/low in practice, whether the probability of occurrence of Risk B (e.g. data privacy is jeopardised) would be correspondingly perceived as high/low. If so, then we interpret that Risk A is likely to have influence on Risk B. As illustrated earlier, Likert scales were used in the survey to examine the perceived probability of occurrence of each identified risk, data variables generated were therefore ordinal data sets. According to Field [13] and Bryman and Cramer [14], Spearman's rho (rs) is the most common and appropriate approach to use to measure bivariate correlations between ordinal variables. As a consequence, Spearman's rho was adopted for this study. Moreover, one-tailed test was used to test further the statistical significance (P value) of each correlation identified. By following this approach, the researchers identified 18 statistically significant correlations between all the 39 identified risks. Figure 2 presents a conceptual map to summarise and represent these correlations.

By scanning this conceptual map, it becomes immediately apparent that in the perceptions of IT professionals, the identified cloud computing risks, especially the top 10 critical risks (as highlighted with grey colour in the map), are interwoven and closely related with each other. Therefore, the occurrence of these critical risks proves to be very difficult for user companies to manage, mitigate and contain. Moreover, by further investigating the conceptual map, it emerges that about half of the identified correlations was related with privacy and security risks (e.g. LR1.1, TR4.1 and TR4.3). These findings thus confirm the importance of privacy and security issues in cloud computing adoption. More importantly, the findings also identified that these critical privacy and security risks can be originated by current legal and technical complexity and difficulties in the cloud (e.g. LR1.2, LR1.3 and TR1.2). On the other hand, the second half of the correlations shown in the conceptual map was found between various organisational and operational risks (e.g. OGR5.2, OPR4.2, OGR4.2 and LR3.2). These business-related risks were also triggered by legitimate deficiencies (e.g. LR3.1) and IT infrastructure complexity (e.g. TR1.2) in the cloud.

Overall, the results of this bivariate analysis supported the early conclusion by confirming that within the sophisticated virtualized cloud environment, critical risks, which are interrelated and can cause potential failure of cloud computing, can occur

in not just privacy and security aspects but also across different IT operation and business areas.

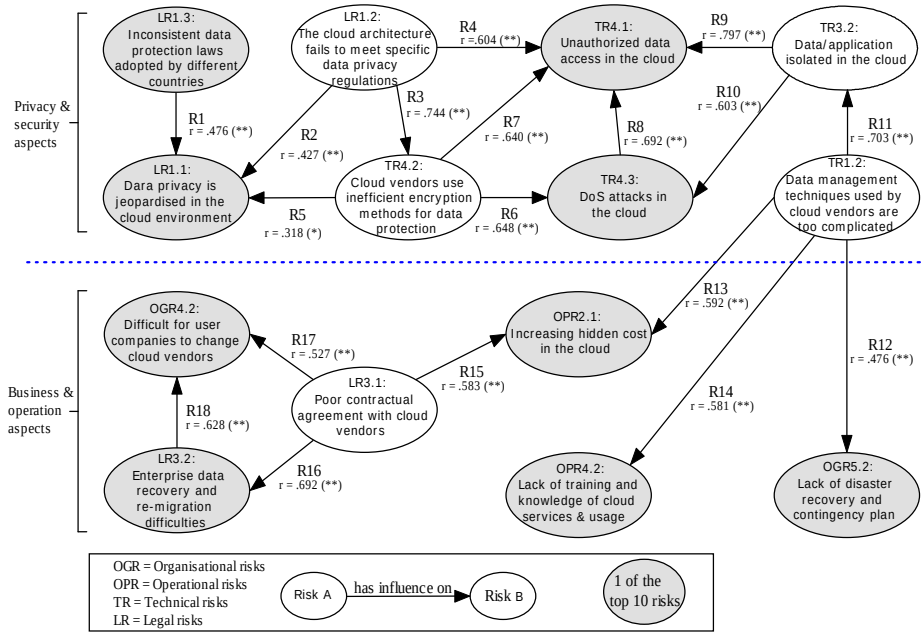

Fig. 2. Conceptual map of correlations between identified cloud computing risks

4. Conclusions

The study reported in this paper employed a questionnaire survey to explore potential risks that companies may encounter during cloud computing adoption. Previous cloud computing studies conventionally put a strong emphasis on data privacy and security challenges. The findings of this study suggest that under the very complicated socio-technical environment in the cloud, risks that can lead to potential cloud computing failure are not restricted to security and privacy aspects. In fact, the study confirmed that a much wider range of cloud computing risks can occur in diverse legal, operational, organisational, and technical areas. More importantly, the most critical top 10 risks were found to be originated by current legal and technical complexity and deficiencies in the cloud environment. Such legitimate deficiencies and technical complexity can raise substantial challenges for enterprise preparation and planning towards cloud service adoption and usage. Overall, it can be concluded that despite the potential IT and business benefits promised by cloud vendors, the adoption of cloud computing is in fact fraught with challenges and difficulties. In order to achieve success in cloud adoption, companies must neither hold an over-optimistic view nor rely merely on their service providers. Instead, a clear understanding and awareness on the identified risks, as well as a thorough preparation

across all levels of the organisation, are essential to prevent potential cloud computing failure and business disasters.

The results of this study have important practical and research implications. In practical terms, the identified cloud risks in general and the top 10 critical risks in particular, can be used by business managers and IT experts, as a checklist for risk identification, management and prevention in cloud adoption. The findings of this study also provide useful and valuable insights to support CEOs, CIOs and IT managers in the process of strategic planning and decision making towards successful cloud adoption. In research terms, the comprehensive risk ontology established in this study does not just fill the current knowledge gap in cloud computing risk, but can also serve as a starting point and theoretical foundation for IS researchers to carry out further investigation in this increasingly important research area.

Reference

1. Voorsluys, W., Brober, J. and Buyya, R.: Introduction to cloud computing. In: Buyya, R., Broberg, J. and Goscinski, A. (eds.), Cloud Computing Principles and Paradigms, pp. 1-41. New Jersey: John Wiley & Sons Inc. (2011)
2. Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J. and Ghalsasi, A.: Cloud computing - the business perspective. Decision Support Systems. 51 (1), 176-189 (2011)
3. Chow, R., Golle, P., Jakobsson, M., Shi, E., Staddon, J., Masuoka, R. and Molina, J.: Controlling data in the cloud: outsourcing computation without outsourcing control. In: Proceedings of the 2009 ACM workshop on Cloud computing security, pp. 85-90, Chicago, Illinois, USA. (2009)
4. Ali, K.H.: Cloud migration: a case study of migrating an enterprise IT system to IaaS. In Proceedings of the 3rd IEEE International Conference on Cloud Computing, pp. 450-457, Miami, Florida. (2010)
5. Peng, G.C. and Nunes, J.M.B.: Surfacing ERP exploitation risks through a risk ontology. Industrial Management & Data Systems. 109 (7), 926-942 (2009)
6. Peng, G.C. and Nunes, J.M.B.: Establishing and verifying a risk ontology for surfacing ERP post-implementation. In Ahmad, M., Colomb, R.M. and Abdullah, M.S. (eds.), Ontology-based applications for enterprise systems and knowledge management, pp. 43-67, Hershey, USA: IGI Global (2012)
7. Peng, G.C. and Nunes, J.M.B.: Identification and assessment of risks associated with ERP post-implementation in China. Journal of Enterprise Information Management. 22 (5), 587-614 (2009)
8. Pan, K., Nunes, J.M.B. and Peng, G.C.: Risks affecting ERP post-implementation: insights from a large Chinese manufacturing group. Journal of Manufacturing Technology Management. 22 (1), 107-130 (2011)
9. Heiser, J. and Nicolett, M.: Assessing the security risks of cloud computing. Available at: http://www.globalcloudbusiness.com/SharedFiles/Download.aspx?pageid=138&mid=220&fileid=12 (2008). [accessed Mar 2012]
10. Mather, T., Kumaraswamy, S. and Latif, S.: Cloud security and privacy: an enterprise perspective on risks and compliance. Sebastopol: O'Reilly (2009).
11. Onwubiko, C.: Security issues to cloud computing. In: Antonopoulos, N. & Gillam, L. (eds.), Cloud Computing Principles, Systems and Applications. pp. 271–288, London: Springer (2010)

12.Bisong, A. and Rahman, S.S.M.: An overview of the security concerns in enterprise cloud computing. International Journal of Network Security & Its Applications. 3(1), 30-45 (2011)
13.Field, A.: Discovering statistics using SPSS: and sex, drugs and rock'n'roll, 2nd ed. London: SAGE Publication (2005)
14.Bryman, A. and Cramer, D.: Quantitative data analysis with SPSS 12 and 13: a guide for social scientists. East Sussex: Routledge (2005)