A SURVEY ON SECURITY RISK MANAGEMENT FRAMEWORKS IN CLOUD COMPUTING

Rana Alosaimi[1] and Mohammad Alnuem[2]

Department of Information Systems,
King Saud University, Riyadh, Saudi Arabia
[1]Rana.io@hotmail.com
[2]malnuem@ksu.edu.sa

ABSTRACT

Cloud computing technology has experienced exponential growth over the past few years. It provides many advantages for both individuals and organizations. However, at the same time, many issues have arisen due to the vast growth of cloud computing. Organizations often have concerns about the migration and utilization of cloud computing due to the loss of control over their outsourced resources and cloud computing is vulnerable to risks. Thus, a cloud provider needs to manage the cloud computing environment risks in order to identify, assess, and prioritize the risks in order to decrease those risks, improve security, increase confidence in cloud services, and relieve organizations' concerns on the issue of using a cloud environment. Considering that a conventional risk management framework does not fit well with cloud computing due to the complexity of its environment, research in this area has become widespread. The aim of this paper is to review the previously proposed risk management frameworks for cloud computing and to make a comparison between them in order to determine the strengths and weaknesses of each of them. The review will consider the extent of the involvement and participation of consumers in cloud computing and other issues.

KEYWORDS

Cloud Computing; Risk Management & Information Security

1. INTRODUCTION

Cloud computing is a new paradigm shift in the technological industry which will continue to grow and develop in the next few years. The rate of organizations migrating to a cloud computing environment is increasing daily due to its advantages [1, 2]. The major cloud computing advantages which benefit organizations are: high scalability and flexibility in organizations' resources in order to meet peak time demand, excellent reliability and availability in that resources can be accessed from anywhere and at any time, and there is no upfront cost for installing and managing the software and hardware infrastructure [3, 4, 5, 6].

On the other hand, cloud computing also has brought many risks to organizations due to the fact that they outsource IT resources which make services completely managed and delivered by a third party. Therefore, such organizations might lose control over how they secure their environment and they might be concerned with privacy and security as the new technology is a

Natarajan Meghanathan et al. (Eds) : ACITY, VLSI, AIAA, CNDC - 2016
pp. 01–11, 2016. © CS & IT-CSCP 2016 DOI : 10.5121/csit.2016.60901

major source of new vulnerabilities in these areas [7, 8, 9, 10]. Therefore, it is important to establish several controls which will work together to decrease the risks, provide layered security, increase confidence in cloud services, and relieve the fear of using a cloud computing environment. Risk management is one of the cloud computing environment controls which aims to assess and manage risks related to cloud computing and to prevent those risks from impacting business goals.

This paper will provide a systematic review of the previously proposed risk management frameworks for cloud computing environments. The paper will be organized as follows. In section II, an overview of the two main subjects – cloud computing and risk management – will be provided. Section III will include reviews of relevant work on previously proposed cloud computing risk management frameworks. Section IV will present the advantages and disadvantages of each of them. Section V will include a discussion of the results of the review and a comparison of the frameworks. Section VI will conclude the paper and will include recommendations for future work in this area.

2. BACKGROUND

2.1. Cloud Computing

Cloud computing is a new type of computing model extended from distributed computing, parallel computing, and grid computing. It provides various additional features to users such as secure, quick, and convenient data storage and a net computing service centred on the Internet. The factors that have propelled the frequency of occurrence and development of cloud computing include the development of grid computing, the appearance of high-quality technology in storage and data transportation, and the appearance of Web 2.0 – especially the development of virtualization [11]. Cloud computing consists of five essential characteristics: on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service [12, 13].
Cloud computing generally provides services on three main diverse levels [14, 15]. These models are:

- Software as a Service (SaaS) – cloud computing delivers an application which is already customied with all of the required hardware, software, operating system, and network to be accessible by various consumers (regardless of their location) by using the Internet without the need to install software on the servers [16].

- Platform as a Service (PaaS) – cloud computing offers a developmental environment and all the developers' requirements (such as software tools, libraries, programming languages, and services for cloud consumers to develop or install their own software and applications). The applications are then delivered to the users via the Internet [17].

- Infrastructure as a Service (IaaS) – cloud computing offers fundamental computing resources (such as processing, servers, storage, and networks) and virtualization technology for consumers to install and run their own operating systems and applications [18].

Furthermore, cloud computing services can be deployed in four ways dependent on consumers' requirements [19]. These four deployment models are:

- Public Cloud – the cloud infrastructure and computing resources are made available to public consumers over a public network. Multiple organizations can work on and access the provided infrastructure at the same time. The public cloud model is controlled and managed by a third party: a cloud provider [5, 20].

- Private Cloud – cloud services are dedicated only to a specific consumer (organization) and offer the highest security of client data and greater control over the cloud infrastructure. A private cloud may be managed and owned by the organization itself or a cloud provider [21].

- Community Cloud – in a community cloud, the cloud infrastructure is provisioned for a group of consumers (organizations) which have the same shared demands. They can share resources by using the connections between the associated organizations. The community cloud is similar to a private cloud in that it can be managed and owned either by the relevant community organizations or a cloud provider [5, 20].

- Hybrid Cloud – A hybrid cloud is a mixture of two or more types of cloud deployment models (public, private, or community) which are connected together to allow for the transfer of data and application between them but without affecting each other [21].

2.2. Risk Management

Organizations usually face and are exposed to several types of risk (e.g. policy, programme, operational, project, financial, human resources, technological, health, safety, and political risks) [22]. The International Organization for Standardization (ISO) defined risk as “the effect of uncertainty on objectives”. Otherwise, the risk is expressed as a combination of the consequences of an event and the associated probability of occurrence [23].

Risk management is a systematic mechanism for managing the risks or threats facing an organization in order to enable it to recognize the events that may result in unfortunate or damaging consequences and to establish the best course of action for identifying, assessing, understanding, acting on, and communicating risk issues [22, 24]. Risk management adds value and offers many objectives to an organization. Some of these objectives are: increasing system security, protecting and enhancing the organization’s assets, making well-informed decisions, and optimizing operational efficiency [25, 26].

3. Risk Management Frameworks in Cloud Computing

The researchers’ efforts are based on three different perspectives on cloud computing risk assessment. The first proposed risk assessment frameworks can be used only by a cloud computing consumer. It was suggested that, in some cases, risk should be transferred to the cloud provider or a trusted third party [27, 28]. However, these researchers ignore the fact that the cloud provider owns and manages the infrastructure of the cloud environment and cannot disclose their security models and procedures to anyone who might be a malicious user. On the other hand, other researchers have proposed risks should only be assessed by the cloud provider, without taking into account the importance of involving the cloud consumers in the process because the cloud provider is the real owner of the data and the only party who knows the real value of the assets in the cloud environment [29, 30]. Thereafter, some researchers believed in the importance of involving the consumers in the risk assessment process [31, 32, 33]. When and to what extent the consumers are involved in this process was considered differently by the different proposed risk assessment frameworks.

3.1. Risk Management by Cloud Consumers

Saripalli and Walters [27] presented a quantitative framework by which the impact and risk of cloud security (based on the Federal Information Processing Standards (FIPS)) can be assessed [25]. Thus, in addition to the security objectives already defined by the US Federal Information

Security Management Act (FISMA) for information and information systems – confidentiality, integrity, and availability – Saripalli and Walters added three more security objectives in the context of cloud platforms – multiparty trust, mutual auditability, and usability. These six security objectives of cloud platforms are referred to as the CIAMAU framework. The typical threats and events are mapped into one or more of these six categories. Saripalli and Walters assessed risk as a combination of the probability of a security threat event and its measured consequence or impact. The probability of a threat event is assessed by using statistical data and the impact of a threat event is evaluated based on expert opinions by using the modified Wideband Delphi method to collect the necessary information [34].

Tanimoto, et al. [28] considered the risk factors in cloud computing from a consumer's viewpoint based on the risk breakdown structure (RBS) method. Their study aimed to address three main security subjects in terms of the cloud environment: the security guarantees in a disclosure environment, the existence of two or more stakeholders, and mission critical data problems. They classified the risk factors into three main divisions: risks for a company which is introducing cloud computing, risks for a cloud service provider, and risks for others. Therefore, in terms of risk analysis, a hybrid method has been proposed based on a quantitative decision tree analysis and the qualitative risk matrix method. Thus, the risk matrix method categorizes risk into four classifications in accordance with the degree of incidence and generation frequency: risk avoidance, risk mitigation, risk acceptance, and risk transference. Consequently, the analyzed and evaluated risks and a detailed countermeasure and proposal have been produced based on these results.

3.2. Risk Management by a Cloud Provider

Fito, et al. [29] proposed a semi-quantitative BLO-driven cloud risk assessment (SEBCRA) approach which is based on the Federation of European Risk Management Association's standards [35]. Fito, et al.'s risk management procedure aims to determine the risk impacts (either positive or negative) on the level of the business objectives (BLOs) of a given cloud organization instead of its impact on the whole cloud environment. Therefore, their risk management framework involves these steps: SEBCRA (the overall process of risk analysis and evaluation), risk reporting and communication, risk treatment, and risk monitoring. SEBCRA was proposed as it is a core sub-process by which cloud risks can be prioritized according to their impact and consequences on different BLOs. In the risk analysis process, Fito, et al. used a standard level matrix to extract the risk level estimation (RLE) as the output for each of the affected BLOs, which is the product of the risk probability and its impact on the BLO. Thus, any risks in which RLE is within unacceptable ranges and has a negative impact on the BLOs are avoided and this has the benefit of leading to an improvement in achieving the BLOs.

Zhang, et al. [30] presented an information risk management framework for cloud computing which covers all cloud service models and cloud deployment models. The framework is based on the evolving ISO/IEC 27001 standards [36], the NIST risk management guide for information technology systems [25], and the Booz Allen Hamilton information security governance [37]. Furthermore, it is similar to the traditional standard quality management (Plan, Do, Check, Act) cycle of continuous improvement and involves seven processes: selection of the relevant critical areas, strategy and planning, risk analysis, risk assessment, risk mitigation, the assessment and monitoring programme, and risk management review. Thus, Zhang, et al. focused on critical areas in cloud computing which must be protected and designed in order to protect the security objectives of information assets: confidentiality, integrity, and availability. In addition, risk analysis and assessment processes, threats, vulnerability identification, and assessment of the output from the identification can ascertain the risk levels (High, Medium, and Low) of relevant critical areas which were selected previously from 12 critical areas which address both tactical and strategic security.

3.3. Risk Management by Cloud Providers and Consumers

Almorsy, et al. [31] proposed a security management framework aimed at improving collaboration between cloud providers, service providers, and service consumers in terms of managing the security of the cloud platform and the hosted services. Cloud consumers are advised to participate in every step of the risk assessment processes in order to extend their security management process (SMP) to include cloud-hosted assets. The framework has been introduced based on aligning the NIST-FISMA standard with the cloud computing model [38]. Almorsy, et al.'s framework consists of three main layers: a management layer, an enforcement layer, and a feedback layer. The framework includes six main phases: service security categorization, security controls selection, security controls implementation, security controls assessment, service authorization, and security monitoring. Their security management framework can be applied to each developed and deployed service in cloud computing and it is considered the overall security categorization for each service.

Xie, et al. [32] presented a risk management framework which includes users, providers, and third party agencies. The main aim of their framework is for cloud providers to ascertain a user's requirements clearly and to enhance the trust between them. The framework is composed of five basic processes: user requirement self-assessment, cloud service providers' desktop assessment, risk assessment, third party agencies review, and continuous monitoring. In the user requirement self-assessment phase, the user should determine the required cloud computing service and deployment model and the security level of authentication, access control, auditing, data integrity, etc. in order to determine potential cloud providers based on these selections. Thus, the aims of the cloud providers' desktop assessment phase are to evaluate the plans of those candidates and to review their past security levels. The risk assessment phase consists of seven stages: preparation of the risk assessment, asset identification, threat identification, vulnerability identification, existing security measures, risk analysis, and risk assessment documentation. The third party agencies review phase involves authoritative security evaluation institutions (including the review group and expert group) which review the procedures of the security assessment plan of the user.

Albakri, et al. [33] proposed a security risk assessment framework based on the SaaS model with a public deployment model based on the ISO/IEC 27005 standard. The framework considered both the cloud provider and the cloud consumer in the risk assessment process by providing a dynamic relationship between them. They aim to balance the realistic results which will derive from the participation of consumers and the potential complexity which may occur due to their involvement. Thus, cloud computing consumer participation in risk management processes is limited to only three tasks: determining the regulatory and legal requirements, determining the security risk factors, and getting feedback from the cloud provider and applying the required security tasks. Therefore, their framework consists of six phases: context establishment, risk assessment, risk treatment, risk acceptance, risk communication and consultation, and risk monitoring and review. In the context establishment process, each consumer should start its own context establishment for its data which will move to the cloud environment to define legal compliance. Furthermore, the same applies to the risk assessment process. Each consumer should identify the risk for its own data which will move to the cloud. Thereafter, the cloud provider will be able to perform a risk analysis and the rest of the processes for its entire infrastructure and consumers' data.

4. RISK MANAGEMENT FRAMEWORKS PROS AND CONS

There is no perfect risk management framework and, due to the complexity of the cloud computing environment, there are many reasons which could make a framework more effective or which could reduce its effectiveness. Table 1 below represents the strengths and weaknesses of each of the above mentioned security risk management frameworks which have been proposed for use in a cloud computing environment.

Table 1. Risk Management Frameworks Advantages and Disadvantages.

Research paper	**Advantages**	**Disadvantages**
Saripalli and Walters	• The approach is fully iterative convergence and enables a comparative assessment of the relative robustness of different cloud vendor offerings in a defensible manner. • It proposes three additional specific security objectives for a cloud environment to be appropriate for a cloud security risk assessment.	• It requires the careful and precise collection of input data for a probability calculation of threat events, which needs to be used to assess cloud computing risks. • It only focuses on risk assessment, which is only one step in the risk management process. The remaining steps are still required. • A quantitative risk assessment method has been used; thus, the results may be confusing and even imprecise. In addition, the method is expensive and requires solid experience with advanced tools. • The risk assessment has focused only on the cloud consumer and has overlooked that the cloud provider is the manager and owner of the cloud infrastructure.
Tanimoto, et al.	• This approach analyses and ascertains the risk factors of cloud computing and gives detailed countermeasures. • It uses a combination of quantitative and qualitative methods for risk analysis and achieved the advantages of both. It has avoided bias and inaccuracy in the assessment results.	• It lacks a risk identification process for the threats, vulnerabilities, and assets of a cloud computing environment. • The risk factors were ascertained only from the consumers' viewpoints and the approach overlooked that the cloud provider is the manager and owner of the cloud infrastructure.
Fito, et al.	• This approach evaluates the impact of cloud risks on the BLOs of a cloud organization, instead of considering the impacts on the whole cloud environment. It therefore has strong focus and precision. • It uses a combination of quantitative and qualitative methods for risk analysis and achieves the advantages of both. It has avoided bias and inaccuracy in the assessment results.	• There is no explanation for the risk identification method, which is an important and critical process in the risk assessment of cloud environment. • The impact of risks has been evaluated based only on the BLOs of a cloud provider and has overlooked consumers' objectives and the fact that the cloud consumer is the real owner of the data assets.

Zhang, et al.	• The risk management was based on selecting critical areas in a cloud computing environment, which makes the risk assessment process strongly focused.	• The risk management was semi-static because the list of critical areas was fixed. This may make the risk assessment of the cloud environment inflexible and some of the risks may be ignored. • A qualitative risk assessment method was followed. This makes the costs and benefits analysis during the selection of recommended controls difficult. • The risk management has focused only on the cloud provider and has overlooked that the cloud consumer is the real owner of the data assets.
Almorsy, et al.	• This approach tackles the loss of trust and security control problems by enabling cloud consumers to extend their SMP to include cloud-hosted assets. • It mitigates the loss of control for cloud providers in terms of the hosted services developed by other parties. • The security management framework was undertaken separately for each of the provided services. This is where the problem of multi-tenancy lies.	• Cloud consumers were involved in every step of the risk assessment processes. This complicates the risk assessment processes, particularly when the number of consumers increases. • A qualitative risk assessment method was followed. This makes the costs and benefits analysis during the selection of recommended controls difficult.
Xie, et al.	• This approach analyses the security status of cloud service providers by reviewing historical incidents. • It introduces third party assessment agency to ensure the effectiveness and safety of cloud computing applications.	• Consumer involvement was not really considered to be active in the risk assessment process, which is only able to decide the security level in general and to select a cloud computing service and deployment model. • Consumers are only involved in determining the appropriate cloud providers based on their requirements. • A qualitative risk assessment method was followed. This makes the costs and benefits analysis during the selection of recommended controls difficult. • There is a lack of risk treatment or acceptance in terms of the appropriate action to be taken for each risk.

Albakri, et al.	• This approach activates the involvement of consumers in the risk management process. • It tries to balance between the benefits of the participation of consumers and the complexity caused thereby.	• The involvement of consumers involves notifying them at each phase that their participation is needed and completion of their responses must be awaited. This could disrupt or delay the process. • The cloud computing consumer does not participate in risk treatment and acceptance. It is the consumer who experiences the risks to its own assets and, therefore, they should make the decision. • A qualitative risk assessment method has been followed. This makes the costs and benefits analysis during the selection of recommended controls difficult.

5. RESULTS AND DISCUSSION

Based on the review of several frameworks proposed previously by different authors, it can be confirmed that the traditional risk management may fail and may not fit well with a cloud computing environment. Thus, the strengths and weaknesses of those frameworks lead to a conclusion that some of key issues should be taken into account when applying a risk management framework to a cloud computing environment. These issues are outlined as follows:

- The involvement of consumers in the risk management process is important because they are the only ones who know the value of their assets.

- Consumer participation should not be limited to the extent of inactivity and consumers should not be involved in each step to the extent of complicating the process.

- Context establishment and risk identification (sub-processes of risk assessment) are critical processes in risk management.

- The participation of cloud consumers in the risk treatment process is significant due to the fact that they are part of the problem; therefore, they must be a part of the solution.

- It is preferable for the risk assessment process to be performed for each of the provided services separately in order to handle conflicts in the consumers' security requirements, due to the multi-tenancy feature of cloud computing.

- The conflict between consumers which appears in the risk identification process should be handled well in order to implement their security requirements and to achieve consumer satisfaction.

- It is advisable to use a combination of quantitative and qualitative methods in the risk analysis process in order to benefit therefrom and to avert their disadvantages.

6. Conclusion and Future Work

The conventional risk management framework does not fit well with a cloud computing environment due to its specific characteristics. Therefore, several studies have been conducted on risk management in cloud computing. There are no specific criteria by which a risk management framework can be considered very bad or very good. A perfect risk management framework cannot be achieved. On the other hand, a particular framework can be decided on the basis of whether it is appropriate and effective or not based on a cloud environment.

This paper has reviewed the previously proposed risk management frameworks in cloud computing with specific regards to the participation of consumers therein and has determined the strengths and weaknesses of each. It was concluded that some specific issues are important when proposing a risk management framework for a cloud computing environment.

In future work, the researchers hereof propose a new risk management framework which takes the advantages of the previously proposed risk management frameworks and averts their disadvantages.

References

[1] R. Charanya, M. Aramudhan, K. Mohan, S. Nithya, “Levels of Security Issues in Cloud Computing,” International Journal of Engineering and Technology, 2013.

[2] M. Alzain, B. Soh, E. Pardede, “A Survey on Data Security Issues in Cloud Computing: From Single to Multi-Clouds,” Journal of Software, 2013.

[3] L. Qian, Z. Luo, Y. Du, and L. Guo, “Cloud Computing: An Overview,” M. Jaatun, G. Zhao, & C. Rong, Cloud Computing, pp. 626-631. Berlin: Springer Berlin Heidelberg, 2009.

[4] R. Bhadauria, and S. Sanyal, “Survey on Security Issues in Cloud Computing and Associated Mitigation Techniques,” International Journal of Computer Applications, 2012.

[5] A. Apostu, F. Puican, G. Ularu, G. Suciu, and G. Todoran, “Study on advantages and disadvantages of Cloud Computing – the advantages of Telemetry Applications in the Cloud,” Recent Advances in Applied Computer Science and Digital Services, 2013.

[6] A. Apostu, F. Puican, G. Ularu, G. Suciu, G. Todoran, “Study on advantages and disadvantages of Cloud Computing – the advantages of Telemetry Applications in the Cloud,” Recent Advances in Applied Computer Science and Digital Services, 2013.

[7] M. Hölbl, “Cloud Computing Security and Privacy Issues,” The Council of European Professional Informatics Societies, 2011.

[8] G. Tucker, and C. Li, “Cloud Computing Risks,” Proceedings on the International Conference on Internet Computing, 2012.

[9] T. Chou, “Security Threats on Cloud Computing Vulnerabilities,” International Journal of Computer Science & Information Technology, 2013.

[10] M. Ryan, “Cloud computing security: the scientific challenge, and a survey of solutions,” Journal of Systems and Software, 2013.

[11] S. Zhang, S. Zhang, X. Chen, and X. Huo, “Cloud Computing Research and Development Trend,” Second International Conference on Future Networks, 2010.

[12] M. Ali, S. Khan, A. Vasilakos, “Security in cloud computing: Opportunities and challenges,” Informatics and Computer Science Intelligent Systems Applications, 2015.

[13] F. Ahamed, S. Shahrestani, A. Ginige, “Cloud Computing: Security and Reliability Issues,” IBIMA, 2013.

[14] P. Sareen, “Cloud Computing: Types, Architecture, Applications, Concerns, Virtualization and Role of IT Governance in Cloud,” International Journal of Advanced Research in Computer Science and Software Engineering, 2013.

[15] I. Ashraf, “An Overview of Service Models of Cloud Computing,” International Journal of Multidisciplinary and Current Research, 2014.

[16] G. Kulkarni, P. Chavan, H. Bankar, K. Koli, and V. Waykule, “A new approach to Software as Service Cloud,” 7th International Conference on Telecommunication Systems, Services, and Applications, 2012.

[17] J. Gibson, D. Eveleigh, R. Rondeau, and Q. Tan, “Benefits and Challenges of Three Cloud Computing Service Models,” Fourth International Conference on Computational Aspects of Social Networks, 2012.

[18] W. Hsu, “Conceptual Framework of Cloud Computing Governance Model - An Education Perspective,” IEEE Technology and Engineering Education, 2012.

[19] R. Sharma, R. Trivedi, “Literature review: Cloud Computing –Security Issues, Solution and Technologies,” International Journal of Engineering Research, 2014.

[20] F. Liu, J. Tong, J. Mao, R. Bohn, J. Messina, L. Badger, and D. Leaf, “NIST Cloud Computing Reference Architecture,” National Institute of Standards and Technology, 2011.

[21] A. Gajbhiye, and K. Shrivastva, “Cloud Computing: Need, Enabling Technology, Architecture, Advantages and Challenges,” Confluence The Next Generation Information Technology Summit, 2014.

[22] H. Berg, “Risk Management: Procedures, Methods and Experiences,” Bundesamt für Strahlenschutz, Salzgitter, Germany, 2010.

[23] ISO/Guide 73, “Risk Management-Vocabulary,” International Organization for Standardisation, 2009.

[24] G. Dickson, “Principles of Risk Management,” Glasgow Caledonian University, 1995.

[25] G. Stoneburner, A. Goguen, and A. Feringa, “NIST SP 800-30 Risk Management Guide for Information Technology Systems,” pp. 8-26, NIST, 2002.

[26] “A Risk Management Standard,” The Institute of Risk Management (AIRMIC) and The Public Risk Management Association (Alarm), 2002.

[27] P. Saripalli, and B. Walters, “A Quantitative Impact and Risk Assessment Framework for Cloud Security,” IEEE 3rd International Conference on Cloud Computing, pp. 280-288, IEEE, 2010.

[28] S. Tanimoto, M. Hiramoto, M. Iwashita, H. Sato, and A. Kanai, “Risk Management on the Security Problem in Cloud Computing,” First ACIS/JNU International Conference on Computers, Networks, Systems, and Industrial Engineering, pp. 147-152, IEEE, 2011.

[29] J. Fito, M. Macıas, and J. Guitart, “Toward Business-driven Risk Management for Cloud Computing,” Network and Service Management (CNSM), pp. 238-241, IEEE, 2010.

[30] X. Zhang, N. Wuwong, H. Li, and X. Zhang, “Information Security Risk Management Framework for the Cloud Computing Environments,” IEEE International Conference on Computer and Information Technology, pp. 1328-1334, IEEE, 2010.

[31] M. Almorsy, J. Grundy, and A. Ibrahim, “Collaboration-Based Cloud Computing Security Management Framework,” IEEE 4th International Conference on Cloud Computing, pp. 364-371, IEEE, 2011.

[32] F. Xie, Y. Peng, W. Zhao, D. Chen, X. Wang, and X. Huo, “A Risk Management Framework For Cloud Computing,” IEEE 2nd International Conference, pp. 476-480, IEEE, 2012.

[33] S. Albakri, B. Shanmugam, G. Samy, N. Idris, and A. Ahmed, “Security risk assessment framework for cloud computing environments,” Security and Communication Networks, Wiley Online Library, 2014.

[34] H. Linstone, and M. Turoff, “The Delphi Method: Techniques and Applications,” Addison-Wesley, 1975.

[35] FERMA, “FERMA’s Risk Management Standard,” 2003, Retrieved from http://www.ferma.eu/Portals/2/documents/RMS/RMS-UK(2).pdf

[36] E. Humphreys, “mplementing the ISO/IEC 27001 Information Security Management System Standard,” Artech Print on Demand, 2007.

[37] J. Miller, L. Candler, and H. Wald, “Information Security Governance Government Considerations for the Cloud Computing Environment,” Booz Allen Hamilton, pp. 4-11, 2009.

[38] NIST, “Standards for Security Categorization of Federal Information and Information Systems,” FIPS-199, 2002, Retrieved from http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf

AUTHOR

Rana Musaad Alosaimi is a Master student of Information Systems at the College of Computer and Information Sciences of King Saud University (KSU), Saudi Arabia. She received her bachelor's degree in Information Technology from the same university. Her fields of research interests include Information Systems, Cloud Computing, and Information Security.

Mohammed Abdullah Alnuem is an Assistant Professor in the field of Computer Science, in the college of Computer and Information Sciences, King Saud University, Saud Arabia. Further, he is also serving as Vice Dean for Development and Quality in E-Transactions and Communications. He received his PhD in Mobile Computing and Networks from the school of Informatics, University of Bradford, UK and M.S. in Distributed Systems and Networks from the same university. His fields of research interests include Computer Networks, Distributed Systems, Wired and Wireless Networks and Software Engineering.