2015 9th International Conference on Next Generation Mobile Applications, Services and Technologies

Cloud Security Risk Management

A Critical Review

Temesgen Kitaw Damenu
Department of Computing
Edge Hill University
Ormskirk, UK
temesgen.damenu@go.edgehill.ac.uk

Chitra Balakrishna
Department of Computing
Edge Hill University
Ormskirk, UK
balakris@edgehill.ac.uk

Abstract— **Cloud computing has created a remarkable paradigm shift in the IT industry and brought several advantages such as on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service. These advantages enabled cloud to have significant impact on different sectors of smart cites. However, cloud adoption has increased the sophistication of the ever changing security risks which frustrate enterprises on expanding their on-premises infrastructure towards cloud horizons. These risks have the potential of being a major concern for smart cities due to the increasing impact of cloud on them. Managing these security risks requires adopting effective risk management method which involve both the cloud service provider and the customer. The risk management frameworks currently applied to manage enterprise IT risks do not readily fit the cloud environment and the dynamic nature of clouds, which are characterized by on demand self-service and rapid elasticity. Therefore, researchers have proposed different cloud security risk management methods and frameworks. This paper critically reviews these risk management methods and frameworks. In addition, it conducts critical analysis on two of them using qualitative content analysis technique, and evaluates their effectiveness for assessing and mitigating cloud security risks.**

Keywords— cloud security risk management; cloud security risk assessment; security risk management; cloud security risk

I. INTRODUCTION

Cloud computing has been transformed from being a promising business concept to one of the rapidly growing segments of the IT industry which shifted the computing paradigm [2]. This computing paradigm shift provides an opportunity to eliminate complexities, cost and capital expenditure in much the same way that using an electricity provider removes the need for every company to build power generators [8]. Cloud computing provides advantages such as on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service [7].

Cloud computing has significant impact on smart cites. Government G-clouds are promising models for smart cities which can create urban clouds that reduce IT costs, and provide platforms for small business applications and e-services [27]. The UK government's G-cloud is an exemplary initiation in this regard [29]. Cloud computing gives opportunity to design different services which can support the necessities of smart cities such as cloud-based intelligent car parking service [28] and smart city logistics [30]. In addition, it has the potential to centralize the world's computing power [29]. This will have an impact on reducing consumption of energy, which is one of the key sectors of smart cities. Cloud computing is also opening new possibilities in virtualizing physical spaces and substituting by digital ones [27].

However, the increasing rate of cloud adoption has amplified the sophistication of the alarming security risks. The increasing on-demand application, platform and infrastructure usage has increased the potential of cyber-attacks [1], which in turn has caused considerable risks on smart cities. Now a days, enterprises are looking towards cloud computing horizons to expand their on-premises infrastructure, but most of them are frustrated due to the security risks [2]. According to a survey conducted on IT executives/CIOs and their line-of business (LOB) colleagues, security is the first challenge of cloud computing [3].

Although cloud security providers (CSPs) claim that their cloud is sufficiently protected, there have been instances when their security has been invaded and the whole system had been down for hours [1]. In addition, various attacks which exposed customers data were occurred in different CSPs. Episilon, a cloud email marketing service provider, faced a data breach which exposed huge amount of customer data including customer email IDs and bank account details [1]. This heavily affected a large section of its customers including JP Morgan Chase, Citibank, Barclays Bank, hotel chains such as Marriott and Hilton, and big retailers such as Best Buy and Walgreens [1]. At-least half a dozen of security breaches have been occurred in 2013, revealing the major gaps in the security management of major CSPs [1].

Managing cloud security risks requires adopting effective risk management method. Researchers have proposed different risk management methods and frameworks. This paper critically reviews these risk management methods and frameworks. It also conducts detail critical analysis on two of them, and evaluates their effectiveness for assessing and mitigating cloud security risks. The paper is organized in six sections. Section II will briefly discuss cloud security risks. Section III will address general issues of cloud security risk management. Section IV will review cloud security management methods and frameworks found in literature. Two of the frameworks will be critically analysed in section V. Section VI provides a critical reflective conclusion.

978-1-4799-8660-6/15 $31.00 © 2015 IEEE
DOI 10.1109/NGMAST.2015.25

II. CLOUD SECURITY RISKS

The security risks associated with different cloud models vary accordingly. The risks are dependent on a wide range of factors including the sensitivity of information assets, and the cloud architectures and security controls involved in a particular cloud environment [3]. Most of cloud security risks can be categorized in to application level, network level, and data and data storage risks [1]. Application level risks include DoS, DDoS, cross site scripting (XSS), SQL injection, backdoor, cookie poisoning, captcha breaking, hidden field manipulation, malicious file execution, hypervisor attack, and other vulnerabilities resulting from programming errors and design flaws [1, 12]. Network level risks include DNS attacks, sniffer attack, BGP prefix hijacking, data-tapping through fibre optic networks, and attacks due to reusing IP addresses [1]. Data and data storage risks include data breach or leakage, data loss and unavailability, data remanence, phishing, exposure of unencrypted data, data lineage, and fraudulent CSP personnel with privileged data access [1, 19]. These attacks can be launched by hackers, nefarious clients (abusers) or malicious insiders [18].

In addition to the above risks, most of the security risks challenging the current on-premises IT environments are also the risks of cloud environments [1]. Managing these security risks is a challenge for both the CSP and the customer. Therefore, effective cloud security risk management is vital to realize secure cloud environment and safer cyber space. The next section discusses issues of cloud security risk management.

III. CLOUD SECURITY RISK MANAGEMENT

Risk management consists risk assessment and risk treatment phases. Risk assessment involves identifying threats which can exploit organisational vulnerability and assessing the likelihood of these threats and their potential impact; while, risk treatment deals with the process of responding the identified risks [4]. Therefore, cloud security risk management involves assessing the security risks of the cloud and mitigating those risks.

Risk assessment is the main sub process of risk management. Its outcomes determines the focus of the risk treatment. Effective risk assessment method is necessary to properly assess security risks. For example, ISO27001 requires to select a risk assessment methodology which follows a qualitative approach and fulfils the requirements mentioned on the standard [4]. There are many risk assessment methodologies currently applied to assess the security risks of enterprise IT infrastructures. ISO27005, NIST SP 800-30, CRAMM, OCTAVE are some of the widely applied methodologies [4]. In addition, the Information Security Forum (ISF) has developed security risk assessment tools: IRAM, SARA, SPRINT and FIRM, which are used by its members and not publicly available [4].

Albakri et al [6] argued that these risk assessment methodologies, which they call traditional methods, are unfit to assess the risks of cloud computing. Most of these traditional methods assume that the information assets of an organisation are found in its data centre [6, 7]. This enables the organisation to fully manage its assets and all security management processes. However, the cloud computing environment is different from the traditional enterprise environment and the characteristics of the cloud model invalidate this assumption making the traditional methods unfit for cloud environment [6]. In addition, these methods do not readily fit the dynamic nature of clouds, which are characterized by on demand self-service and rapid elasticity [9].

Security assessment in cloud is a challenging domain and identifying security risks that may face the cloud customer is a complex task [9]. The cloud customer is not allowed to assess the security risks of the CSP since hackers who claimed to be customers may use the result of the risk assessment to exploit the vulnerability of the CSP [6]. In addition, revealing the risks will likely lead to reduced confidence of customers on the cloud services and uncertainties on the quality and level of security implemented [9]. On the other hand, the CSP can't exactly calculate the risk since it does not know the real value of the data assets of the customer [6]. Lack of cloud security standard also created a challenge in cloud risk assessment [9]. Therefore, an effective cloud security risk management methodology is necessary to adequately assess and mitigate cloud security risks. Different risk management methods and frameworks are proposed in order to address this concern. The following section critically reviews existing methods and frameworks found in literature.

IV. REVIEW OF CLOUD SECURITY RISK MANAGEMENT FRAMEWORKS

Cloud security risk management is one of the focus areas in current cloud computing research. As a result, researchers proposed different security risk management methods and frameworks. Alturkistani and Emam [9] reviewed cloud risk assessment methods by classifying them into five categories as: assessment as a service, qualitative and quantitative, hierarchical, graph analysis and security matrix assessment [9]. They identified the main processes and components of the methods but they didn't assess the effectiveness of those methods. Drissi et al [21] surveyed existing knowledge on cloud computing risk assessment. However they didn't critically analyse the use cases in detail.

Alnuem et al [31] reviewed and compared seven different cloud security risk management frameworks. They classified the seven frameworks in to three based on the following coverage areas: frameworks for security evaluation in cloud environments, frameworks for analysing the security risks in cloud environments and frameworks based on security policies. The comparison was undertaken according to these coverage areas and the requirements in ISO 27001 [31]. However, the comparison didn't critically analyse the frameworks and identify their gaps.

Some studies focused on specific aspect of cloud security risk management such as service level agreement (SLA) risk management [13, 14] and virtual machine images risk management [18]. Morin et al [14] proposed SLA risk management framework to improve governance, risk and compliance. The SLA monitoring framework proposed in [13] consists reputation assessment module and transactional risk assessment module.

A risk management approach led by CSP's business-level objectives (BLOs) is presented in [16]. The other risk

management procedure presented in [15] aims to determine the risk impacts on BLOs. The proposed BLO-driven cloud risk assessment procedure prioritized cloud risks according to their impact on different BLOs [15]. However, both of these risk assessment methods focused only on the BLO of the CSP and overlooked the involvement of the cloud customer, who is the real owner of the data.

On the other hand, Tanimoto et al [17] analysed security risks from the users' viewpoint using risk breakdown structure (RBS) and risk matrix methods. They also developed countermeasures for the identified risks. However, their study focused on the cloud user and overlooked that the CSP is the owner and manager of the cloud infrastructure [7]. Saripalli & Walters [11] proposed a quantitative impact and risk assessment framework. Nevertheless, Djemame et al [26] argued that the challenge and difficulty of applying such quantitative framework is the meticulous collection of historical data for threat events probability calculation which requires data input from those to be assessed cloud computing platforms and their vendors.

Zhang et al [8] developed a security risk management framework which can be used by CSPs to perform risk analysis, risk assessment and risk mitigation. Albakri et al [7] also proposed a cloud security risk assessment framework for CSPs which involve cloud customers at the early stages of the risk assessment process. The frameworks developed by Zhang et al [8] and Albakri et al [7] will be critically analysed in the following section.

V. CRITICAL ANALYSIS OF TWO RISK MANAGEMENT FRAMEWORKS

The cloud security risk assessment frameworks developed by Zhang et al [8] and Albakri et al [7] have their own strengths and limitations. These frameworks will be analysed using qualitative content analysis technique.

Qualitative content analysis is a "research method for the subjective interpretation of content of text data through the systematic classification process of coding and identifying themes or patterns" [5, p.2]. This analysis technique will be used to review the two frameworks and analyse their strengths and limitations. The qualitative content analysis will be done based on the following thematic areas:

1. Does the framework effectively address both phases of risk management (risk assessment and risk treatment)?
2. Does the framework enable the CSP and the customer to efficiently assess and mitigate cloud security risks?

A. Zhang et al's Framework

The framework proposed by Zhang et al [8] follows the Plan, Do, Check, Act (PDCA) cycle and contains seven processes: selecting relevant critical areas, strategy and planning, risk analysis, risk assessment, risk mitigation, assessing and monitoring program, and risk management review, as shown in Fig 1.

The first phase, Architecting and Establishing the Risk Management Program (PLAN), involves selecting relevant critical area that highlights twelve critical areas to address both the strategic and tactical security 'pain points' within any cloud model. The CSP selects applicable critical areas for the specific cloud environment before moving to strategy and planning process. Strategy and planning involves assigning a responsible body for the risk management, establishing directions, defining goals, requirements and scope, and planning to achieve the defined goals and requirements.

The Implement and Operate (Do) phase includes risk analysis, risk assessment and risk mitigation processes. The Monitoring and Review (Check, Act) stage involves 'assessing and monitoring program' and 'risk management review' to ensure the effectiveness of the overall risk management program.

The framework was applied to manage the risks of a SaaS platform which provide a real time logistic web-based application software service to support logistic industry in China. The framework is evaluated based on the thematic areas as follows.

1. Does the framework effectively address both phases of risk management (risk assessment and risk treatment)?

The framework addressed both the risk assessment and risk treatment phases. However, some components of context establishment and asset identification, which are the primary steps to be performed during risk management [24], are not considered.

Context establishment involves setting criteria of risk evaluation, impact, and risk acceptance. It also includes setting the scope and boundaries of the risk assessment, and establishing an appropriate body that perform the risk

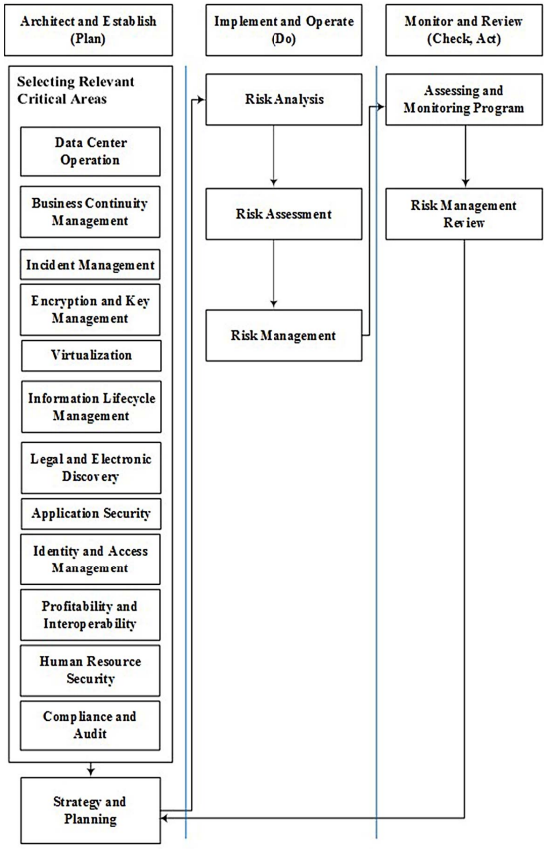

Figure 1. Cloud computing risk management framework proposed by Zhang et al [8]

management [7, 25]. Although assigning a responsible body and defining the scope are included, the other components of context establishment are overlooked in the framework. The quality of the results produced when performing context establishment and asset identification has a crucial influence on subsequent steps such as identifying loss, vulnerabilities, possible attacks and defining countermeasures [24]. Therefore, ignoring these components have negative impact on the effectiveness of the risk management. In addition, 'control recommendation', which is included in the risk assessment process, is a component of risk treatment [4]. It is better to group controls recommendation in the risk mitigation process.

2. Does the framework enable the CSP and the customer to efficiently assess and mitigate cloud security risks?

The framework is applicable for all cloud service models and cloud deployment models [20]. However, it considers only the CSP and overlook the role of the customer in the risk management processes. The customer is the real owner of the data assets. The only one who knows the real value of the data and the realistic impact of data security breaches is the customer [7]. Hence, ignoring the customer's involvement will result inaccurate security risk level evaluation and inefficient risk management.

Alruwaili and Gulliver [22] criticized the framework that it lacks details on important elements such as the cloud risk control matrix, threats and vulnerabilities, proactive detection and response, risk control strategies, secure service level agreement parameters, and compliance and monitoring process. Xie et al [23] also noted that the framework is very similar with the traditional quality management. In addition, the framework lacks a risk communication feature which is an important component for cloud, since the communication between the CSP and the customer is vital for effective cloud security risk management [7]. The above limitations significantly minimize the efficiency of the framework to assess and mitigate cloud security risks.

B. Albakri et al's Framework

Albakri et al [7] proposed a cloud security risk assessment framework shown in Fig. 2. They relied on ISO27005 standard [25] to define the main steps of the framework. The proposed framework considers both the cloud customer and the CSP during the risk assessment process and defines their responsibilities. It limits the involvement of the customer on evaluation of security risk factors to avoid the complexity that can result due to the involvement of the customer in the whole risk assessment process.

The framework consists two main parts: the CSP and the cloud clients (CCs). The CSP side contains four main entities: CSP risk assessment manager [CSPRAM], CSP and CC communicator [CSP3C], CSP security requirements classifier [CSPSRC], and CSP database interface [CSPDI]. The CCs side contains the cloud client risk assessment assistance (CCRAA) only.

The CSPRAM is the CSP body responsible for managing the risk assessment processes as a whole. The CSP3C is used to handle all communication with the CCs during the process. The CSP3C transfer information received from the CCs to the CSPSRC. The CSPSRC categorizes this information and saves them in the database. It makes decisions on the security requirements and the importance of threats received from the CCs. The CCRAA is the CC entity responsible for communication with the CSP.

The context establishment process involves three sub processes: setting the basic criteria (risk evaluation,

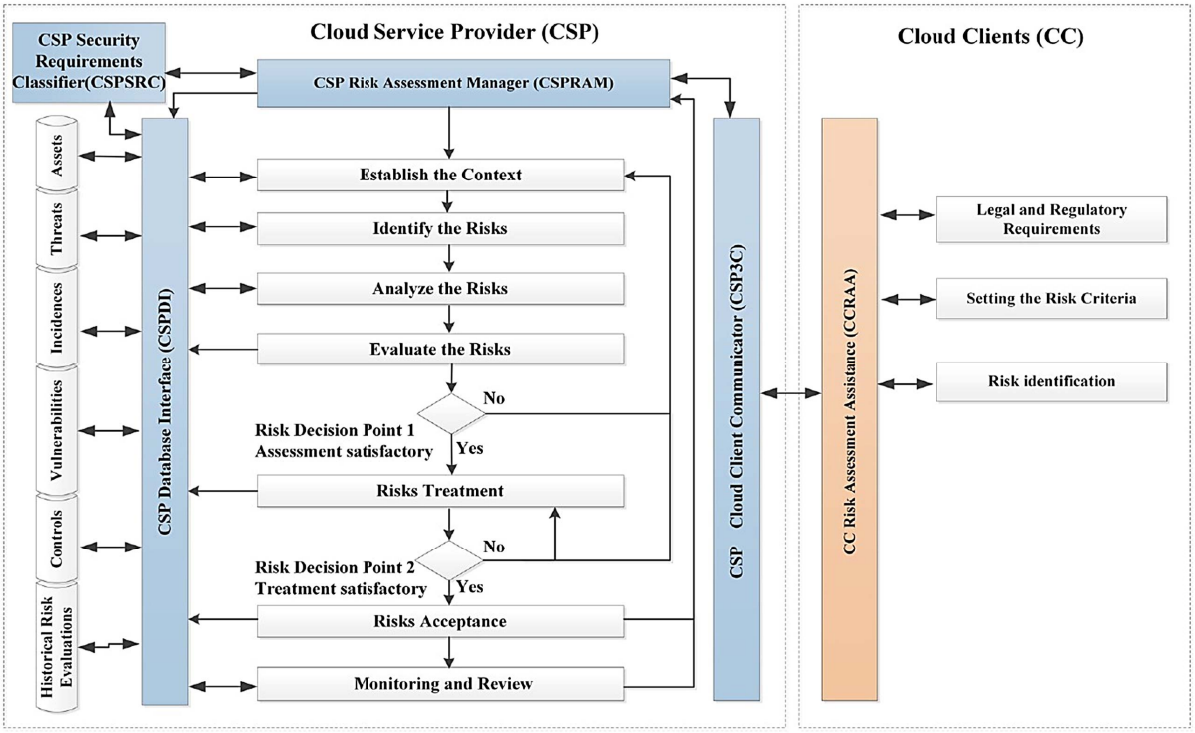

Figure 2. Cloud security risk assessment framework proposed by Albakri et al [7]

impact, and risk acceptance criteria), setting the scope and boundaries, and organizing the information security risk management process. CCs are expected to assess their data and define their criteria for risk evaluation, risk impact, and risk acceptance. The CSP establishes the context and considers the criteria and expectations of the CCs at this phase.

The next phases include risk identification, risk analysis, and risk evaluation which constitute the risk assessment process. Each CC is expected to evaluate its assets, identify the threats and vulnerabilities, and submit the information to the CSPRAM through the CSP3C. The CSP conduct its own risk identification and integrate the CCs' risks and prioritize them.

The risk treatment phase involves preparing risk treatment plan and implementing appropriate security controls to address the risks. In the risk acceptance phase, residual risks should be identified and the CSP should ensure that the treatment plan has decreased the risk to an acceptable level based on the CCs risk acceptance criteria. The last phase requires the CSP to monitor and review the risks and their factors to consider any change in the next iteration.

Albakri et al [7] performed an initial experiment on the framework by using it for a scenario which assess the security risks of a SaaS provider which provides a website package for medium and small organisations that sell products on the Web. The framework is evaluated based on the thematic areas as follows.

1. Does the framework effectively address both phases of risk management (risk assessment and risk treatment)?

The framework effectively addresses both risk assessment and risk management although it is named as a risk assessment framework and gives much focus for the risk assessment phase. The framework follows a qualitative risk assessment approach. Qualitative approach helps to prioritize the risks and identify areas for immediate improvement [4]. However, it doesn't provide specific quantifiable magnitude of the risk impacts, thus making the cost-benefit analysis calculation of recommended controls difficult [4].

2. Does the framework enable the CSP and the customer to efficiently assess and mitigate cloud security risks?

The framework considers both the CSP and the customer, and mitigates the major limitations of traditional risk assessment methods [6]. However, it targets only SaaS as claimed by the authors. Therefore, it may not be efficient to assess and mitigate the risks of PaaS and IaaS environments. The involvement of the client in the risk assessment process is limited to a minimum in order to decrease complexity. Although minimizing the client's involvement makes the process easier for the CSP, it may create negative impact on the effectiveness of certain phases and may cause client dissatisfaction. Ignoring the involvement of clients especially on risk treatment and risk acceptance, and providing them only reports on these issues can limit the effectiveness of the risk treatment. As clients are part of the problem, making them part of the solution will be important. The clients should also have a chance to comment whether the selected controls meets their expectation and the residual risk is acceptable or not. This limitation will have higher impact in case of PaaS and IaaS, and may make the framework inefficient for these models. In addition, the framework assumes that the client have the capability to perform a risk assessment, which may not be the reality in all SaaS clients.

Finally, the review and analysis of the risk management frameworks mentioned in this section showed that the frameworks follow different approaches and have their own strengths and limitations. Despite their limitations, these frameworks can be used in different cloud environments to assess and mitigate cloud security risks. However, their applicability to manage the security risks of a given cloud environment should be evaluated before applying them. Their limitations should also be considered or mitigated.

VI. CONCLUSION

Security risks are primary challenges and issues of cloud computing [8]. Cloud security risk management is vital to secure the cloud and create a safer cyber space as cloud is becoming significant component of the global cyber space. Managing security risks is the heart of cloud security [10].

Different cloud security risk management frameworks and approaches have been proposed in literature. This paper reviewed some of them and critically analysed two frameworks [7, 8] using qualitative content analysis technique. The critical review of these frameworks revealed their strengths and limitations. This can help CSPs and cloud customers to understand the frameworks and select the better one. The research community can also use the review to understand the gaps on the current frameworks and conduct further research to improve them. In addition, this review helps to understand the security risks of cloud and available frameworks and methods to manage those risks.

The risk assessment methods and frameworks analysed in this paper follow different approaches. The framework proposed by Zhang et al [8] adopted the PDCA cycle and contains seven processes: selecting relevant critical areas, strategy and planning, risk analysis, risk assessment, risk mitigation, assessing and monitoring program, and risk management review. The authors suggested that the framework is applicable for all cloud service models and deployment models although it is tested only on SaaS cloud. However, the framework overlooks some components of context establishment and asset identification which are primary stages of risk management [24, 25]. In addition it considers only the CSP and overlooks the role of the customer which is the important stakeholder of the cloud security risk management.

On the other hand, the framework proposed by Albakri et al [7] considers both the cloud customer and the CSP during the risk assessment process and defines their responsibilities although it limits the involvement of the customer to avoid complexity. The framework relies on ISO 27005 [25] to define the main steps and consists two main parts: the CSP and the cloud customers (CCs). The framework effectively addresses the risk assessment and risk treatment phases. However, it is targeting only SaaS and may not be efficient to assess and mitigate the risks of PaaS and IaaS. In addition, it involves the customer only

on security risk factors evaluation. Therefore, it overlooks customer involvement on certain important phases such as risk treatment and risk acceptance. This can create negative impact on the effectiveness of the risk treatment.

Despite their limitations, both of these frameworks and the others reviewed in this paper can be applied to manage the security risks of cloud environments if the necessary evaluations are made and their limitations are considered or mitigated. Further research is required to develop an efficient framework applicable for all cloud models. In addition, comprehensive cloud security risk management methodologies and standards are necessary.

REFERENCES

[1] Bhadauria, R., Chaki, R., Chaki, N., & Sanyal, S. (2011). A survey on security issues in cloud computing. arXiv preprint arXiv:1109.5388.

[2] Popovic, K., & Hocenski, Z. (2010, May). Cloud computing security issues and challenges. In *MIPRO, 2010 proceedings of the 33rd international convention* (pp. 344-349). IEEE.

[3] Zhang, X., Wuwong, N., Li, H., & Zhang, X. (2010, June). Information security risk management framework for the cloud computing environments. In *Computer and Information Technology (CIT), 2010 IEEE 10th International Conference* on (pp. 1328-1334). IEEE.

[4] Calder, A. and Watkins, S.G. (2010). Information Security Risk Management for ISO27001/ISO27002. Cambridgeshire: IT Governance Ltd.

[5] Okere, I., Van Niekerk, J., & Carroll, M. (2012, August). Assessing information security culture: A critical analysis of current approaches. In *Information Security for South Africa (ISSA)*, 2012 (pp. 1-8). IEEE.

[6] Albakri, S. H., Shanmugam, B., Samy, G. N., Idris, N. B., & Ahmed, A. (2014). Traditional Security Risk Assessment Methods in Cloud Computing Environment: Usability Analysis. *IRICT Proceeding*, pp. 483-495, 12th -14th September, 2014, Universiti Teknologi Malaysia, Johor, Malaysia.

[7] Albakri, S. H., Shanmugam, B., Samy, G. N., Idris, N. B., & Ahmed, A. (2014). Security risk assessment framework for cloud computing environments. *Security and Communication Networks*, 7(11), 2114-2124.

[8] Zhang, X., Wuwong, N., Li, H., & Zhang, X. (2010, June). Information security risk management framework for the cloud computing environments. In *Computer and Information Technology (CIT), 2010 IEEE 10th International Conference* (pp. 1328-1334). IEEE.

[9] Alturkistani, F. M., & Emam, A. Z. (2014). A Review of Security Risk Assessment Methods in Cloud Computing. In *New Perspectives in Information Systems and Technologies, Volume 1* (pp. 443-453). Springer International Publishing.

[10] Blakley, B., McDermott, E., & Geer, D. (2001, September). Information security is information risk management. In *Proceedings of the 2001 workshop on new security paradigms* (pp. 97-104). ACM.

[11] Saripalli, P., & Walters, B. (2010, July). Quirc: A quantitative impact and risk assessment framework for cloud security. In *Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on* (pp. 280-288). IEEE.

[12] Mather, T., Kumaraswamy, S., & Latif, S. (2009). *Cloud security and privacy: an enterprise perspective on risks and compliance*. "O'Reilly Media, Inc.".

[13] Hammadi, A. M., & Hussain, O. (2012). A framework for SLA assurance in cloud computing. In *Advanced Information Networking and Applications Workshops (WAINA)*, 2012 26th International Conference on (pp. 393-398). IEEE.

[14] Morin, J., Aubert, J., & Gateau, B. (2012). Towards cloud computing SLA risk management: issues and challenges. In *System Science (HICSS), 2012 45th Hawaii International Conference on* (pp. 5509-5514). IEEE.

[15] Fitó, J. O., & Guitart, J. (2014). Business-driven management of infrastructure-level risks in Cloud providers. (pp. 41-53). *Future Generation computer systems*, *32*,

[16] Fitó, J.; Macías, M.; Guitart, J. (2010). Toward business-driven risk management for cloud computing. *Proceedings of the 2010 International Conference on Network and Service Management*. (pp. 238-241): IEEE Computer Society Publications.

[17] Tanimoto, S., Hiramoto, M., Iwashita, M., Sato, H., & Kanai, A. (2011, May). Risk management on the security problem in cloud computing. In *Computers, Networks, Systems and Industrial Engineering (CNSI), 2011 First ACIS/JNU International Conference on* (pp. 147-152). IEEE.

[18] Bindra, G. S., Singh, P. K., Kandwal, K. K., & Khanna, S. (2012, June). Cloud security: analysis and risk management of VM images. In *Information and Automation (ICIA), 2012 International Conference on* (pp. 646-651). IEEE.

[19] Winkler, V. J. (2011). *Securing the Cloud: Cloud computer Security techniques and tactics.* Elsevier.

[20] Katal, A., Wazid, M., & Goudar, R. H. (2012). Enhanced Security Framework for Cloud Computing. *Proc. Int. Conf. on Computational Intelligence and Information Technology,* (pp. 365-370), Elsevier.

[21] Drissi, S., Houmani, H., & Medromi, H. (2013). Survey: Risk assessment for cloud computing. *International Journal of Advanced Computer Science and Applications (IJACSA)*, *4*(12).

[22] Alruwaili, F. F., & Gulliver, T. A. (2014). Safeguarding the Cloud: An Effective Risk Management Framework for Cloud Computing Services. *International Journal of Future Generation Distributed Systems (IJFGDS)*, *1*(2).

[23] Xie, F., Peng, Y., Zhao, W., Chen, D., Wang, X., & Huo, X. (2012, October). A risk management framework for cloud computing. In *Cloud Computing and Intelligent Systems (CCIS), 2012 IEEE 2nd International Conference on* (Vol. 1, pp. 476-480). IEEE.

[24] Beckers, K., Schmidt, H., Kuster, J., & Faßbender, S. (2011, August). Pattern-based support for context establishment and asset identification of the ISO 27000 in the field of cloud computing. In *Availability, Reliability and Security (ARES), 2011 Sixth International Conference on* (pp. 327-333). IEEE.

[25] ISO/IEC 27005. (2008). Information technology–Security techniques-Information security risk management. *ISO/IEC, 66.*

[26] Djemame, K., Armstrong, D., Kiran, M., & Jiang, M. (2011, September). A risk assessment framework and software toolkit for cloud service ecosystems. In *CLOUD COMPUTING 2011, The Second International Conference on Cloud Computing, GRIDs, and Virtualization* (pp. 119-126).

[27] Komninos, N., Schaffers, H., & Pallot, M. (2011, October). Developing a policy roadmap for smart cities and the future internet. In *eChallenges e-2011 Conference Proceedings, IIMC International Information Management Corporation*. IMC International Information Management Corporation.

[28] Ji, Z., Ganchev, I., O'Droma, M., Zhao, L., & Zhang, X. (2014). A Cloud-Based Car Parking Middleware for IoT-Based Smart Cities: Design and Implementation. *Sensors*, *14*(12), 22372-22393.

[29] Townsend, A., Maguire, R., Liebhold, M., Crawford, M. (2011). A Planet of Civic Laboratories. The Future of Cities, Information and Inclusion. *Institute for the Future*.

[30] Nowicka, K. (2014). Smart City Logistics on Cloud Computing Model. *Procedia-Social and Behavioral Sciences*, *151* (pp. 266-281)

[31] Alnuem, M., Alrumaih, H., & Al-Alshaikh, H. (2015). A Comparison Study of Information Security Risk Management Frameworks in Cloud Computing. In *CLOUD COMPUTING 2015: The Sixth International Conference on Cloud Computing, GRIDs, and Virtualization on* (pp. 103-109).