# A Review of Security Risk Assessment Methods in Cloud Computing

Fatimah M. Alturkistani and Ahmed Z. Emam

College of Computer & Information System, King Saud University
Riyadh, Saudi Arabia
Fatma@ccis.imamu.edu.sa, aemam@ksu.edu.sa

**Abstract.** The Cloud computing is a major technological trend that continues to evolve and flourish. It has potential benefits in achieving rapid and scalable resource provisioning capabilities as well as resource sharing. However, a number of security risk are emerging in association with cloud usage that need to be assessed before cloud computing is adopted. This paper presents a review of the security risk assessment methods in cloud computing. The paper aims to summarize, organize and classify the information available in the literature to identify any gaps in current research then suggest areas for further investigation. At the end, the paper suggests to have a collaborative security risk assessment method that will add great assistance to both service providers and consumers.

**Keywords:** Cloud computing security, security risk, risk analysis, risk assessment, threat analysis.

## 1 Introduction

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction [16]. Cloud offers an optimized and efficient computing by enhancing collaboration, agility, scalability, availability, and cost reduction.

Although cloud computing has a considerable benefits over traditional computing models, yet it raises severe security concerns that limit its widespread adoption; loss of governance, lock-in, isolation failure, data protection and insecure data deletion are some examples. While creating a zero risk service is impractical, if not impossible, assessing security risk of cloud based solutions is important to establish trust and to increase the level of confidence of cloud service consumers. Moreover, it provides cost effectiveness, reliable service and infrastructure of cloud providers [4].

Generally, security risk assessment is an assessment aimed at examining possible threats and vulnerabilities as well as the likelihood and impact of them in accordance with the external and internal relative technology standards. By considering the essential cloud characteristics such as the on demand self-service and rapid elasticity, the traditional assessments developed for conventional IT environments do not readily

Á. Rocha et al. (eds.), *New Perspectives in Information Systems and Technologies, Volume 1*, Advances in Intelligent Systems and Computing 275,
DOI: 10.1007/978-3-319-05951-8_42, 

fit the dynamic nature of clouds. Hence, the introduction of cloud specific security assessment methodology has significant importance and scope. Recently, several studies have been conducted to improve traditional security assessment techniques and present new paradigms for analyzing and evaluating security risks within cloud environment.

However, security assessment in cloud is still challenging domain and a growing area of research. Identifying security risks that cloud consumers encounter is a complex task [18]. Cloud computing is a multilayered environment that mainly encompasses deployment model layer, followed by delivery model layer. Each of these fundamental layers poses a specific set of security risks that are inherited through the layers. Therefore, different combinations of deployment models and the utilized delivery models have different security risks that must be addressed and considered.

A lack of security standards and security control transparency present further challenges in cloud risk assessment. Security standards are important to measure security risks of cloud providers. Hence, security assessment can't give information unless it is compared with standard [3]. In addition, the lack of transparency is because the cloud providers usually do not want to reveal their own infrastructure to consumers for monitoring or risk assessment, as this will likely lead to reduced confidence in cloud services due to the uncertainties associated with the quality and level of security implementation. By considering the above challenges, how can we assess security risks of adopting cloud services? What are the methodologies and how effective are they? To answer the above questions, this paper presents a review of security risk assessment methods in cloud computing, classify them and compare their process in order to identify the gaps in current research then suggest areas for further investigation. The reminder of this paper is organized as follows: Section 2 presents a literature review of security risk assessment in cloud. In Section 3, we describe the method we adopted to carry out the review. Section 4 discusses the results obtained from the review. Finally, some conclusions and future work are provided.

## 2 Literature Review

### 2.1 The Process of Risk Assessment

Risk assessment is the core process of risk management. Organizations use risk assessment to determine the extent of the potential threats associated with the information system. The output of this process helps to identify controls that are fully proportionate with the risks to which the organization is exposed. The identified controls are used to reduce and/or eliminate risk during the risk mitigation process [5]. Meanwhile, risk assessment involves two processes: risk analysis and risk evaluation. Risk analysis is the systematic approach for describing and calculating risk. It includes the identification of undesired events, and the causes and consequences of these events [22]. Whereas, risk evaluation is the comparison of risk analysis results with the acceptance criteria for risk and other decision criteria.

There are a number of distinct approaches to risk analysis. However, these essentially break down into two types: quantitative and qualitative. In quantitative approach, the value of the potential losses associated with threat needs to be determined. Then the probability of the occurrence of the risk failure needs to be estimated. Finally, the Annual Loss Expectancy (ALE) is calculated and risk priority is determined accordingly [5]. While qualitative analysis deals with estimated potential loss and probability data is not required. Most qualitative risk analysis methodologies make use of a number of interrelated elements: threats, vulnerabilities and controls.

### 2.2 Security Risk Assessment Frameworks in Cloud Computing

The European Network and Information Security Agency (ENISA) [6] has published a guide that allow an informed assessment of the security risks and benefits of using cloud computing. For the purposes of the risk assessment, a medium-sized company was used as a use case and the aim was to expose all possible information security risks. The risks identified in the assessment are classified into three categories: technical, legal and policy and organizational issues. Each risk is presented in a table which includes probability level, impact level, reference to vulnerabilities, reference to affected assets and level of risk. The estimation of risk levels is based on ISO/IEC 27005.

In addition, ENISA makes concrete recommendations on how to address the risks and maximize the benefits. One of the most important recommendations is a set of assurance criteria designed to: (1) assess the risk of adopting cloud services, (2) compare different cloud provider offers, (3) obtain assurance from the selected cloud providers and (4) reduce the assurance burden on cloud providers. The recommendation provides a set of questions that an organization can ask a cloud provider to assure themselves that they are sufficiently protecting the information entrusted to them. However, this guidance does not provide detailed recommendations with regard to the cloud and risk assessment function.

Another initiative in assessing security risks is taken by Cloud Security Alliance (CSA). The CSA leads a number of ongoing research initiatives through which it provides white papers, tools and reports to help companies and vendors secure cloud computing services. It has published guidelines on different security issues related to cloud computing. The guide consists of twelve domains and the second domain is dedicated to governance and enterprise risk management. The proposed guidelines are not compulsory and may not all be applicable to every cloud deployment, but help to identify threats in the cloud context and choose the best options by which to mitigate vulnerabilities. Meanwhile, a simple framework for evaluating initial cloud risks and informs security decisions is provided [3]. Among the CSA's recommendations, high emphasis is placed on defining metrics and standards for measuring the performance of information security, which should be assessed and be documented on the contracts. Furthermore, the CSA provides Governance, Risk and Compliance Stack [27] as a toolkit for assessing private and public clouds against industry-established security best practices. Also, the CSA has established a CloudAudit project that seeks

to simplify the process of gathering audit data by creating a standard method for cloud providers to communicate how they address security, governance and compliance.

### 2.3 A Classification of Cloud-Based Security Risk Assessment Methods and Tools

Recently, several studies have been conducted to improve traditional security assessment techniques and present new paradigms for analyzing and evaluating security risks in cloud environment. We classified cloud-based risk assessment methods into five risk categories as shown in Table1.

**1) Risk assessment as a service:** Security as a service (SecaaS) solutions have been developed to provide and support security assessments in which a cloud- hosted solution performs the assessments and stores the resulting data. Today, several tools for a number of security assessment areas have been implemented using the SecaaS delivery model [14], [29]. In the SecaaS delivery model, customers get the typical benefits of using cloud computing such as scalability and on demand service. CSA have developed guidance for SesaaS implementation [31].

In [19], risk assessment as a service is introduced as the new paradigm for measuring risk in real-time by one or more of the entities in the cloud. A cloud provider can perform continuous self-assessments as a best practice through evaluation of its own run-time environment. Moreover, a trusted third party and cloud customer could assess the provider on an ongoing basis through privileged access to certain internal measurement interfaces. However, this work has not implemented such a service but rather offer it as a paradigm to be pursued.

**2) Qualitative and quantitative assessment:** Risk assessment have analyzed security risk by using qualitative or/and quantitative approach. Several quantitative risk assessment methods exist. In [22], a quantitative risk and impact assessment framework (QUIRC) is introduced to assess associated six key categories of security objectives (SO) (i.e., confidentiality, integrity, availability, multi- party trust, mutual audit ability and usability) in a cloud computing platform. The framework defines risk as a combination of the probability of a security threat event and its severity, measured as its Impact. The impact is determined by Subject Matter Experts (SME), the knowledgeable about the impact of threats on their particular type of business. The probability of each event should also be collected from earlier records and research, specific to the business and the geographical region, using sources such as SANS report. Table 2 shows the pros and cons of QUIRC assessment method.

In [30], a SEmi-quantitative BLO-driven Cloud Risk Assessment (SEBCRA) prioritizes and categorizes cloud risks according to their impact on different Business Level objectives in a given organization. The approach is designed for a Cloud Service Provider (CSP) to improve the achievement of a BLO, i.e., profit maximization, by managing, assessing, and treating Cloud risks. In an exemplary experimentation, the risk assessment approach demonstrates that it enables a CSP to maximize its profit by transferring risks of provisioning its private Cloud to third-party providers of cloud infrastructures. Table 2 shows the pros and cons of SEBCRA

assessment method. However, a simple method for qualitative or quantitative analysis will lead to the inaccuracy and one-sidedness of the evaluation results. Therefore, several studies used an integrated method of qualitative and quantitative analysis to assess risk in cloud environment [4], [20], [23], [30].

**Table 1.** A Classification of Cloud Security Risk Assessment Methods and Tools

| Methods | Risk Modeling | Stakeholders | Ref. |
|---|---|---|---|
| Assessment As a Service | Cloud service model | Cloud customer | [14],[19], [29] |
| Qualitative/ Quantitative Analysis | Textual language model | Cloud provider | [8], [12], [25] |
| | Threat and vulnerability analysis | Cloud customer and provider | |
| Graphs Analysis | Attack Defense Trees (ADT) | Cloud provider | [15],[21], [23] |
| | Decision Tree Analysis (DTA) | Cloud customer | |
| | Graph mathematical model | Cloud provider | |
| Hierarchal Assessment | Risk Breakdown Structure (RBS) | Cloud customer | [7],[20], [23],[24] |
| | Analytic Hierarchy Process (AHP) | Cloud customer and provider | |
| | Hierarchical assessment Indicator system | | |
| Security Matrix | Trust Matrix | Cloud customer | [1], [17], [26], [27] |
| | Cloud Control Matrix (CCM) | Cloud customer and provider | |
| | Trust and Assurance Registry (STAR) | Cloud customer | |

**3) Graphs analysis assessment:** Graphs and mathematical models can be used to address and calculate security risk in clouds by simulating attacker possibilities. In [15] they presented a mathematical model for threats that considers communication in order to identify security risk for individual entities, and then calculates it for a whole enterprise. The model is built by representing communications as a directed graph and then established a matrix to discover the risk. Furthermore, in [23] a hybrid risk-analysis method based on decision tree analysis (quantities) and risk matrix (qualitative) is proposed for risk assessment. In this method, risk factor from a user's viewpoint is systematically extracted with the Risk Breakdown Structure (RBS) method then analyzed and evaluated. A detailed countermeasure and proposal

are produced on the basis of these results. The risk matrix method is used to classify risk into four kinds (Risk Avoidance, Risk Mitigation, Risk Acceptance, and Risk Transference) in accordance with the generation frequency and degree of incidence.

**4) Hierarchal assessment:** In [20] a security risk assessment method has been introduced based on an Analytic Hierarchy Process (AHP) model. The assessment is carried out using the principles of: decomposition, pairwise comparison, and synthesis of weights. Thus, AHP has three layers of decomposition: formulating the problem of assessing cloud security risk in a hierarchical structure is the first step in AHP. Then, in level two, 8 major factors were identified for assessing. In level three, 39 factors were identified corresponding to higher levels and specific local conditions. The evaluation module uses the constructed AHP tree to assess the system with the help of the judgment matrix that is filled by the cloud's experts. Finally calculating the weighted vectors and getting the final risk order. Table 2 shows the pros and cons of the above hierarchal assessment method.

**Table 2.** Pros and Cons of Risk Assessment Methods

| Ref. | Pros | Cons |
|---|---|---|
| [4] | It supports service provider and infrastructure provider as well as wide range of scenarios such as Cloud bursting and Cloud brokerage. | Risk assessment model need to be developed to suit each of the identified risk categories. |
| [9] | It enables cloud service providers to include security in their SLA offerings, increasing the likelihood that their services will be used. | It can be used just to compare between cloud providers to select the best one based on calculation of risk factor of each one |
| [20] | It based on collaborative computing. It can effectively decompose the risk assessment in cloud (complex problem) into an orderly hierarchy. | There is a lack of complete model or method of risk assessment in cloud computing environment |
| [22] | It enables cloud vendors, customers and regulation agencies to comparatively assess the relative robustness of different cloud vendor offerings in a defensible manner | The precise collection of historical data for threat events probability calculation, which requires data input from those to be assessed Cloud computing platforms and their vendors. |
| [25] | Develop a custom, domain specific language for cloud deployments by their functional and non- functional security relevant properties. Then, derive risk profile to secure cloud deployment | The method is static because: (1) it doesn't consider the evolution of a cloud deployment and (2) the way to it derives risk related values. |
| [30] | It evaluates the impact of cloud-related risks on BLOs considered, instead of considering effects on the whole loud organization. | There is a lack of complete model or method of risk assessment in cloud computing environment |

In [7], a hierarchical framework is built to analyze the risk and set the goal for the assessment. After that, an indicator system is built under each principle and sub-indicators are introduced for assessment. For example, the first indicator could be risk of cloud computing platform, risk of cloud storage, risk of cloud security and so on. Secondary indicators of cloud platform risk could then be risk of operating system, risk of application software and risk of availability.

**5) Security matrix assessment:** In [1], Trust Matrix is used for security risk analysis in cloud environments. Two variables, namely "data cost" and "provider's history" are considered. In "data cost" users can assign a cost to data based on the data's criticality whereas "Provider's history" includes the record of the past services provided by the provider to consumers. Additionally, Cloud Control Matrix (CCM) has been released by CSA in 2013, as a baseline security control framework designed to help enterprises assess the risks associated with a cloud provider. It gives a detailed understanding of security concepts and principles that are aligned to the CSA guidance in 13 domains. The CCM has included a risk management domain to ensure that formal risk assessments are aligned with the enterprise-wide framework, planned and scheduled at regular intervals determining the likelihood and impact of identified risks, using qualitative and quantitative methods. Thereby, it facilities transparency and increase trust level between the cloud customer and the cloud in order to make cloud a secure environment to the future of business [26].

## 3 The Review Methodology

This review has been accomplished by reviewing the existing literature regarding security risk assessments in cloud computing environment. The goal is to identify the existing risk assessment methods, categorize them and suggest areas for further investigation.

### 3.1 Question Formalization

The question focus was to identify the most relevant issues in cloud computing which consider security risk and their assessment methodologies. Therefore, the research question addressed by the researchers was: How to identify, analyze and assess security risk in cloud computing? The keywords and related concepts that make up the question were used during the review execution as: cloud security risk, threat identification, threat modeling, vulnerabilities assessment, risk analysis models and risk assessment methods.

### 3.2 Selection of Sources

The reviews is conducted by searching academic gateways, online databases, catalogues, academic journals, conferences and workshops to obtain related information and recent articles while considering authorship, credibility and authenticity. In an attempt to perform an exhaustive search, basically we considered

the following electronic sources because they had published papers on the topic: Institute of Electrical and Electronics Engineers digital library (IEEE Xplore), Association for Computing Machinery digital library (ACM), ScienceDirect, SpringerLink and Google scholar. Once the potentially relevant primary studies have been obtained, we assessed them for their actual relevance. The selection criteria through which we evaluated the sources were based on practical issues such as authors experience and the language, for instance all the included studies were written in English and available on Web. Furthermore, the inclusion and exclusion criteria were based on the research question. Thus, we included studies that contain issues and topics that they consider in security risk assessment in cloud and these studies must described methods or framework for risk assessment.

### 3.3 Review Execution

The review is executed by searching in the defined sources and evaluating the obtained studies based on the defined criteria. Writing this review is after obtaining a set about 100 results which were flirted according to the inclusion criteria to produce a set of 45 relevant studies. This set was filtered again with exclusion criteria to give a set of studies which corresponds with 15 primary studies. Based on the security risk assessment review, several interviews with cloud computing experts were conducted. In these interviews the main questions for cloud provider and cloud customer respectively are: “How would you demonstrate adequate risk management and compliance to your customers”? and “How do you evaluate various cloud providers on their security level?” The interviews conclude that both cloud customers and providers should develop robust information security risk assessment, regardless of the service or deployment model. The assessment should be collaboration between customers and providers to achieve agreed upon goals which support the business mission and information security program.

## 4 Results and Discussion

By reviewing the literature, several methodologies and frameworks for performing risk assessment have been reviewed and suggested. We have classified risk assessment methods into five categories: assessment as a service, quantitative and qualitative, hierarchal, graph analysis and security matrix assessment. Basically, these risk assessment methods have analyzed security risks by using qualitative or/and quantitative approach. For comprehensive risk assessment, risk analysis is accomplished using an integrated method; a combination of qualitative analysis and quantitative analysis. Meanwhile, some studies have used risk inventory as a Knowledge Base (KB) to include facts, scenarios, and reasoning rules that represent security and exploitation related knowledge. In addition to the risk assessment methods that has been reviewed, the CSA leads a number of ongoing research initiatives like security guidance, CCM and STAR to facilitate risk assessment in cloud computing. Despite all these methodologies and initiatives, currently no concise

methodology exists for analyzing and evaluating security risks of cloud based solutions. Thus, the adoption of cloud solutions in a number of industries is prevented. Most of the studies view the problem of assessing security risks either from cloud customer or cloud provider perspectives. The need for a comprehensive, shared and transparent risk assessment methodology that considers both customer and provider is recommended. Such shared assessment enables the cloud provider to prove how the security risks have been managed and mitigated, as well as enabling the cloud consumer to determine the risk tolerance and define security requirements accordingly.

## 5 Conclusion

Due to the obvious cost and convenience benefits of cloud computing, adopting cloud-based solutions is widely accepted. However, the typical decision of cloud adoption taken by management often considers the cloud benefits without any attention or a proper evaluation of the associated cloud risk. Thus, developing a mechanism that facilities and standardize the process of security risk assessment before cloud adoption is critical. It increases transparency, reduces uncertainties and establishes trustworthiness. Meanwhile, several researches and initiatives have been conducted. We have classified the cloud risk assessment methods into five categories: assessment as a service, quantitative and qualitative, hierarchal, graph analysis and security matrix assessment. The main process and components of the risk assessment methods have been identified and considered. However, the characteristics of cloud computing challenge the development of mechanisms and standards that assess security risk of adopting cloud computing in effective and efficient manner.

## 6 Future Work

Security risk assessment in clouds is needed for both customers and cloud providers. The security concerns because cloud customers do not see what happens inside a cloud and how their data is handled. They have to fully trust the cloud providers to act honestly and not breach the confidentiality of data and computations. On the other hand, cloud providers prefer to hide the cloud topology and operational details. Thus, there is a necessity to balance the opposing needs of the providers and customers. As for future work, we are looking to make cloud computing more trustworthy and reliable, by bridging the above gap. We suggest to approach this problem in two directions: (1) by building distributed, collaborative and intelligent risk assessor that guide customer to evaluate the security level of cloud provider and identify the associated risk before the decision of cloud adoption has been taken. (2) By designing a mechanism that will allow the cloud provider to prove the confidentiality and integrity of the data and computation without disclosure of sensitive cloud topology information.

## References

[1] Chandran, S., Angepat, M.: Cloud Computing: Analyzing the risk involved in cloud computing environments. In: Proceedings of Natural Sciences and Engineering, Sweden, pp. 2–4 (2010)
[2] Cloud Security Alliance, Security Guidance for Critical Areas of Focus in Cloud Computing - UPDATED (February 14, 2011)
[3] Cloud Security Alliance, Security guidance for cloud computing. United States: Cloud Security Alliance Guidance (2009)
[4] Djemame, K., et al.: 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 (2011)
[5] Verdon, D., McGraw, G.: Risk Analysis in Software Design. IEEE Security and Privacy, 79–84 (2004)
[6] ENISA, Cloud computing: benefits, risk and recommendations for information security
[7] Zhang, J., Sun, D., Zhai, D.: A research on the indicator system of Cloud Computing Security Risk Assessment. In: 2012 International Conference on Quality, Reliability, Risk, Maintenance, and Safety Engineering (ICQR2MSE), June 15-18, pp. 121–123 (2012)
[8] Johnson, B., Qu, Y.: A Holistic Model for Making Cloud Migration Decision: A Consideration of Security, Architecture and Business Economics. In: 2012 IEEE 10th International Symposium on Parallel and Distributed Processing with Applications (ISPA), July 10-13, pp. 435–441 (2012)
[9] Hale, M.L., Gamble, R.: SecAgreement: Advancing Security Risk Calculations in Cloud Services. In: 2012 IEEE Eighth World Congress on Services (SERVICES), June 24-29, pp. 133–140 (2012)
[10] Hashizume, K., Rosado, D.G., Fernández-Medina, E., Fernandez, E.B.: An analysis of security issues for cloud computing. Journal of Internet Services and Applications (2013)
[11] Kaliski Jr., B.S., Pauley, W.: Toward risk assessment as a service in cloud environments. In: Proceedings of the 2nd USENIX Conference on Hot Topics in Cloud Computing, USENIX Association (2010)
[12] Khan, A.U., Oriol, M., Kiran, M., Jiang, M., Djemame, K.: Security risk and their management in cloud computing. In: 2012 IEEE 4th International Conference on Cloud Computing Technology and Science (CloudCom), December 3-6, pp. 121–128 (2012)
[13] Kiran, M., Jiang, M., Armstrong, D.J., Djemame, K.: Towards a Service Lifecycle Based Methodology for Risk Assessment in Cloud Computing. In: 2011 IEEE Ninth International Conference on Dependable, Autonomic and Secure Computing (DASC), December 12-14, pp. 449–456 (2011)
[14] Free Security Assessment by Trend Micro, Security Assessment Tool
[15] Leitold, F., Hadarics, K.: Measuring security risk in the cloud-enabled enterprise. In: 2012 7th International Conference on Malicious and Unwanted Software (MALWARE), October 16-18, pp. 62–66 (2012)
[16] Lim, C., Suparman, A.: Risk analysis and comparative study of the different cloud computing providers in Indonesia. In: 2012 International Conference on Cloud Computing and Social Networking (ICCCSN). IEEE (2012)
[17] Luna, J., et al.: A security metrics framework for the cloud. In: Proc. of Security and Cryptography, pp. 245–250 (2011)
[18] Okuhara, M., Shiozaki, T., Suzuki, T.: Security Architecture for Cloud Computing. Fujitsu Sci. Tech. J. 46(4), 397–402 (2010)

[19] Onwudebelu, U., Chukuka, B.: Will adoption of cloud computing put the enterprise at risk? In: 2012 IEEE 4th International Conference on Adaptive Science & Technology (ICAST), October 25-27, pp. 82–85 (2012)
[20] Peiyu, L.I.U., Don, L.I.U.: he new risk assessment model for information system in cloud computing environment. Procedia Engineering 15, 3200–3204 (2011)
[21] Wang, P., Lin, W.-H., Kuo, P.-T., Lin, H.-T., Wang, T.C.: Threat risk analysis for cloud security based on Attack-Defense Trees. In: 2012 8th International Conference on Computing Technology and Information Management (ICCM), April 24-26, pp. 106–111 (2012)
[22] Saripalli, P., Walters, B.: QUIRC: A Quantitative Impact and Risk Assessment Framework for Cloud Security. In: 2010 IEEE 3rd International Conference on Cloud Computing (CLOUD), July 5-10, pp. 280–288 (2010)
[23] Tanimoto, S., Hiramoto, M., Iwashita, M., Sato, H., Kanai, A.: Risk Management on the Security Problem in Cloud Computing. In: 2011 First ACIS/JNU International Conference on Computers, Networks, Systems and Industrial Engineering (CNSI), May 23-25, pp. 147–152 (2011)
[24] Zhang, X., Wuwong, N., Li, H., Zhang, X.: Information Security Risk Management Framework for the Cloud Computing Environments. In: 2010 IEEE 10th International Conference on Computer and Information Technology (CIT), pp. 1328–1334 (June 29, 2010)
[25] Zech, P., Felderer, M., Breu, R.: Cloud risk analysis by textual models. In: Proceedings of the 1st International Workshop on Model-Driven Engineering for High Performance and Cloud Computing. ACM (2012)
[26] Cloud Security Alliance, Cloud Control Matrix (September 26, 2013)
[27] Cloud Security Alliance, GRC Stack an Integrated Suite of Four Initiatives (2011)
[28] CSA Security, Trust & Assurance Registry (STAR). Cloud Security Alliance
[29] Security Risk Assessment for Cloud and Web. Cenzic Cloud
[30] Fito, J.O., Macias, M., Guitart, J.: Toward business-driven risk management for Cloud computing. In: 2010 International Conference on Network and Service Management (CNSM), October 25-29, pp. 238–241 (2010)
[31] SecaaS Category 5 Security Assessments Implementation Guidance. Cloud Security Alliance (September 2012)