Cloud Security Audit for Migration and Continuous Monitoring

Umar Mukhtar Ismail[1], Shareeful Islam[1,2]
[1]School of Architecture, Computing & Engineering,
University of East London,UK
[2]SBA Research, Austria
u0852138@uel.ac.uk,shareeful@uel.ac.uk

Haralambos Mouratidis[3]
[3]School of Computing, Engineering, & Mathematics,
University of Brighton,
Brighton UK
H.Mouratidis@brighton.ac.uk

***Abstract* –Security assurance in cloud computing is one of the main barriers for wider cloud adoption. Potential cloud computing consumers like to know whether the controls in cloud environments can adequately protect critical assets migrated into the cloud. We present a cloud security audit approach to enable users' evaluate cloud service provider offerings before migration, as well as monitoring of events after migration. Our approach entails a set of concepts such as actor, goals, monitoring, conditions, evidence and assurance to support security audit activities. These concepts are considered as a language for describing the properties necessary for cloud security audit both before and after migration. Finally, a real cloud migration use case is given to demonstrate the applicability of the security audit approach.**

Keywords: Cloud computing; security; audit; conditions; and evidence.

I. INTRODUCTION

Cloud Computing (CC) offers increased agility for enterprises to easily expand their IT services as business needs evolve, along with significant benefit of cost reduction [1]. Cloud Computing Customers (CSC) are increasingly apprehensive about cloud adoption, with current literatures citing the insufficient implementation of appropriate security controls by Cloud Service Providers (CSP) and the inability of customers to monitor their entities as the two most pressing challenges to adoption. We approach this problem from the outlook of a security audit perspective, which is perceived as an established method for assessment and evaluation process that could successfully facilitate cloud migration decision-making process. Security audit empowers the trail of resources, collection and evaluation of evidence to determine the effectiveness and efficiency of controls in safeguarding assets and achieving organizational objectives [2, 11, 13].

There are approaches from both academia and industry that cover cloud security audit from different perceptions. Some of such works [3,4] consider the task of allowing a third party auditor to verify the integrity of dynamic data stored in the cloud on behalf of the CSC. Others, such as CloudAudit [5] provide an assessment methodology through which the offerings of various CSPs are analyzed. However, there is insufficient consideration for a systematic audit process that uses a set of concepts relevant to user-specific goals and cloud based environment. An audit should assess the completeness of security offerings being provided by a specific CSP that has the potential to fulfill users' requirements. This paper contributes towards this direction by introducing a set of concepts that support the evaluation of CSP offerings. We follow the existing works in literatures such as Goal Oriented Requirements Engineering (GORE) [6] to define the concepts. The concepts enable the definition of users' intentions as the goals for cloud migration, as well as the introduction of conditions so that appropriate evidences can be collected as a prerequisite for fulfilling conditions and cloud adoption. Finally, we implement the concepts in a real organization to demonstrate the relevance of the work.

II. RELATED WORKS

Cloud security audit allows users to understand security status of CSP's infrastructure. The National IT and Telecom Agency [7] introduced the current trends in cloud audit, assurance initiatives and evaluated the feasibility of accessing different security documentations provided by CSPs to determine whether they provide adequate information to meet the customers' risk assessment and be compliant with legislative requirements. [8] proposed Complete-Auditable-Reportable (C.A.RE) approach to help prospective CSCs evaluate the sufficiency of security services offered by CSPs and map those offerings with their internal operational requirements through an assessment process. [9] presented Security-Audit-as-a-Service architecture that uses the concept of utilizing autonomous agents for monitoring a cloud infrastructure. CSA CloudAudit framework attempted to address audit and compliance in cloud services by developing an automated and standardized way to facilitate information gathering regarding the performance and security of cloud services [5].

All the above mentioned efforts introduced essentially relevant concepts to the realm of auditing in CC. However, some of the works are limited to specific cloud models and acknowledge the difficulties of identifying the control objectives that need to be audited in cloud context. There has been a little effort made towards building an auditing approach that could support users in analyzing the security offerings of a CSP based on primary user goals. Our work contributes to develop such an approach and supports business organizations and individuals in identifying goals and sufficiently

assesses cloud offerings for a well-founded decision making.

III. MODELLING CONCEPTS

The proposed approach includes several modeling concepts that serve as a language for describing essential audit properties. As stated before, we follow GORE approach [6] to define the language and extend the methodology with imperative concepts for cloud security audit. Furthermore, we also follow the CSA cloud control matrix (CCM) [5] to define the audit conditions. An overview of the concepts used by the proposed approach is given below:

a. *Actor*. An actor represents an entity that has strategic goals within its organisational setting (6). Based on the layers of CC service models, actors are identified as CSPs and CSCs. CSPs develop applications that are offered and deployed on the CC platform, and also supply infrastructure, network facilities and other computing and storage services needed to run applications within the cloud. CSCs require the services provided by a CSP to attain their business goals, hence resort to patronising computing services from CSPs.

b. *Goals*. A goal represents the overall aims and objectives of an actor that support its business interests. The CSC is the main actor with three goal categories:
   - *Strategic goals* imply the functionalities or services that support a CSC in the attainment of business objectives. It entails other sub-goals. The first sub-goal focuses on transforming business models. Organizational goal is another type of sub-goal aiming at increasing output with efficiency and effectiveness. Another sub-goal in this category involves cost-reduction defined in terms of return on investment (ROI).
   - *Operational goals* are described as non-functional properties that are indirectly related to functionality, but rather specific to adding quality to operating objectives, whose attainment moves an organization towards achieving strategic goals. Operational goals are associated with security, privacy, scalability, optimization, and quality of service in the cloud.
   - *Technical goals* deal with ensuring that technology adequately provides for the technical requirements of the CSC in terms of data, application and management interoperability, portability and compatibility.

*c. Risks***.** A risk is defined as the probable failure of CSP offerings to fulfil goals, or the probability of CSP offerings to obstruct CSC goals. CSPs usually design SLAs to satisfy the generic requirements of the cloud market, some specific requirements that are distinctive to a CSC may not be satisfied by the CSP, hence introducing risks to their goals. For instance, Office 365 usually allows negotiation of goals through SLAs [12]. Therefore, risk mitigation actions cover performing a trade-off between CSC goals and the limitations of the CSP through negotiations that are later included as part of the conditions. The negotiations can either be direct or indirect. Direct negotiation involves unmediated discourse between CSC and the CSP. Indirect negotiation involves using readily available information to assess the service provisions of a CSP.

d. *Conditions*. A condition represents a set of restrictions that prevent specific CSC goals from being achieved unless they are otherwise fulfilled. Aspects of a condition deal with setting essential specifications for ensuring that all specified goals are met; risks mitigated; and the continuous monitoring or auditing of migrated entities is supported by the CSP. We follow CSA's CCM [5] domains to define the necessary conditions. For instance, the domain "*Information Security – Encryption"* in CCM is used to draw a condition associated with end-to-end encryption for ensuring the confidentiality and integrity of CSC entities.

e. *Evidence*. An evidence is defined as a set of information in any form that represents CSP processes, technologies, and operations. The CSP generates evidence(s) as a means of demonstrating how conditions are approached. This is based on a well justified affirmation that desired resources, controls and technologies are sufficiently implemented. From the perspective of our approach, evidence is characterised by evidence criteria and evidence source.
   - Evidence criteria deals with controls in certain areas specified in the condition, which are related to the domains of CCM such as data security & information lifecycle management.
   - The available information documenting CSP service provisions are generated through such sources as: audit reports, SLA, benchmarks (e.g. CSA CloudAudit), observations, and third-party asserted certifications, etc.

f. *Monitoring***.** Monitoring is defined as recording of events to observe the status of migrated objects within the CSP infrastructure. It consolidates several services that enable CSCs to continually monitor and validate the status of security controls of a CSP after migration to the cloud. Particularly, the monitoring focuses on essential areas of cloud operations as (i) security operations and processes, and (ii) alerts on security incidents, and breach of privacy to

entities. The objective of the monitoring concept is to ensure that a set of mechanisms, systems, processes and procedures are deployed in the CC platform to enable CSCs instant reaction to unwarranted changes or events concerning their entities.

g. *Assurance***.** Assurance provides various levels of confidence regarding CSPs ability to fulfil goals. It establishes to what degree a potential CSP's offerings satisfy goals. The ranking is considered to be based on a subjective opinion of an auditor and other CSC stakeholders. In our approach, the assurance is directly defined and represented according to a scale ranking of three levels:
   - *Level 1.* This is the lowest level of assurance attributed to a CSP. It indicates all, or rather, most evidence(s) required for satisfying conditions have not been implemented by a CSP, meaning that services are unreliable and untrustworthy for adoption.
   - *Level 2***.** The evidences required for fulfilling a condition have been moderately or partially implemented to a reasonable degree of satisfaction. This level manifests that CSP offerings are moderately acceptable and sustainable.
   - *Level 3.* This is the highest level of assurance signifying that all evidences required for fulfilling conditions have been optimally implemented with detailed description of applicability. It implies that CSP services are highly trustworthy, reliable and stable.

The metamodel illustrated in Fig.1 shows an overall relationship among the concepts. A CSC actor is represented as having interest in cloud services offered by a CSP. The CSP provides reliable and secure services that also support its users to continually monitor their entities. The CSC may have several goals under multiple categories (such as security and privacy, availability, cost reduction, etc.), and a single or more goals may be the focus of attainment. While concerns are raised regarding risks that may obstruct the fulfillment of goals in CC adoption, how the CSP can fulfill goals, and those risks inherent to CC, conditions for migration are introduced in order to accredit CSP services and mitigate the risks. Conditions represent a description of requirements that need to be fulfilled for certain occurrences to take place. The conditions are drawn from control objectives of CCM particularly on the criteria most relevant to the goal(s), and then they are imposed to the CSP in order for them to provide evidence that fulfill those conditions. Evidence is provided by the CSP as a means of demonstrating the fulfillment of the conditions. It is done through affirmation of the specific criteria relevant to the conditions and substantiating the sources from which information is provided. The evidence also affirms whether security monitoring and incident reporting tools are adequately supported. The validity and efficacy of the evidences generate different levels of assurance to signify the level of satisfaction attributable for the each evidence. All of the assurance levels serve to indicate that the CSP has implemented the necessary technical and nontechnical processes, procedures, technologies, and practices that could fully satisfy, moderately satisfy or not satisfy goals.

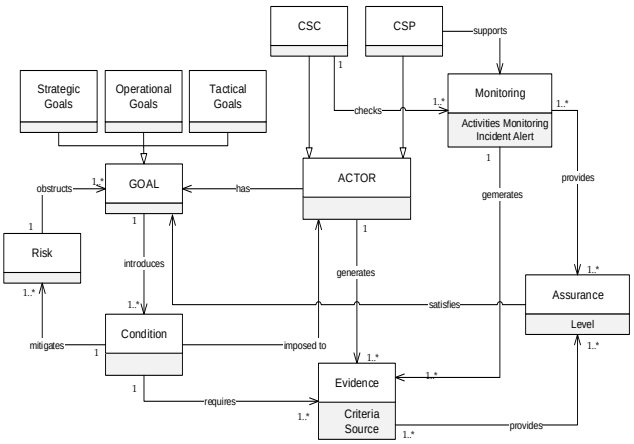

Fig. 1 Metamodel

IV. CASE STUDY

This section presents a case study from a real cloud migration use case to demonstrate the applicability of the proposed approach.

A.Use Case Scenario

The migration use case adopts a London based open-access publishing company. Due to confidentiality reasons, we are restrained from using the publisher's real name and detailed information. The organization provides an affordable open access publishing services of peer-reviewed academic journals, books and data through a network of independent university and society presses. The publishing services provided by the company include anti-plagiarism checking, rigorous peer review, indexing and archiving.

The underlying technology for the open access publication is using a code repository with Python and PH for storing and archiving documents. The code repository is currently used by 25 users. The business process includes: receiving articles from potential researchers, assigning reviewers for the papers, proof reading of the selected papers and final publication. The existing in-house systems use three web servers, and 20Mbps of bandwidth. Generally, there are around thousands of articles published every month. The company has recently decided to adopt cloud for

performing existing operations within tight budget constraints. However, the management likes to know the possible consequences of cloud adoption in terms of benefits and risks, the selection of a suitable CSP and evaluating their commitments to protecting the interests of the company. One of the coauthors, through his personal contact, has the opportunity to perform this task based on the proposed approach.

B. Implementation of the Concepts

Actor

The printing company is identified as the CSC actor that requires the services provided by a CSP to achieve its goals. Another actor is the CSP who specializes in the delivery of cloud models and provisioning of other computing power that could support the company to achieve its goals.

Goals

The management certainly has a set of targets as goals that must be achieved if the migration ever takes place. These goals are classified according to the three categories of sub-goals. Due to space restrictions, we are not considering all the identified goals for further illustration. In particular, we focus only on integrity, availability, and portability goals.

- *Strategic goals.* Supporting 24 users to work with the code and printing services (*organizational goal*); cost minimization to achieve cost efficiency and business sustainability (*cost reduction goal).*
- *Operational goals.* High availability of cloud services, continuous and constant customer service support, and minimum downtime (*availability goal)*; integrity of migrated data and applications (*integrity goal);* the transparency of operations and monitoring of migrated entities *(auditability goal).*
- *Technical goals.* The portability of supporting unlimited number of researchers to access published articles through diverse platforms (*portability goal)*; running the repository from the cloud environment *(interoperability)*; and compatibility of cloud-enabled code repository to host PHP and Python (*compatibility goal).*

Risks

The predictable and undesirable circumstances that could forestall attaining the goals of the company are:

- Security issues associated with the integrity of articles and the code repository in general, such as data breaches, loss and leakage.
- Unavailability of the code repository and open access portal.
- Poor provisioning of customer support by a CSP.
- Lack of monitoring facilities.

The imperative controls and techniques that are desirable in mitigating those risks were discerned and introduced as part of the conditions that must be fulfilled.

Conditions

To satisfy the identified goals, CSA's CCM control objectives were considered. The domains most relevant to ensuring availability, integrity and portability in CC were analyzed, interpreted and translated into conditions that best befit the goals. This means that the conditions aim at ensuring that the prospective CSP satisfies all the goals of the printing company in line with CCM provisions. Table 1 shows the identified conditions needed to satisfy the goals.

TABLE I. GOALS AND CONDITIONS

Goals	Conditions (C)
Availability goals	**C1.**Availability monitoring & management tools. **C2.**BCP & DRP, data backup & redundancy. **C3.** Customer service support.
Integrity goals	**C4.** End-to-end data encryption techniques. **C5.** Access controls integrating identity & access management. **C6.** Certifications & third party attestations.
Portability goal	**C7.** Compatibility, portability and interoperability of data and platforms.

Evidence

In collecting evidences, the service offerings of two reputable IaaS providers were considered from sources of information such as CSP websites, security whitepapers, Request for Information (RfI). We also looked at independent auditor reports to obtain an elaborate overview of all the implemented controls, processes, procedures and technologies in the CSPs environment. Evidences are mapped to the conditions accordingly as shown in Table 2, which forms the basis to perform an audit and establish a reasonable opinion on assurance ranking. For example, encryption mechanisms that ensure the integrity of published articles was introduced as condition 4 (C4). Both CSPs provided evidences in their security whitepapers and websites on the implementation of encryption techniques at several layers of their platform using globally accepted encryption standards. In this paper, nevertheless, we do not intend to provide a detailed insight into how the audit process is applied to the collected evidences as our focus is on the introduction of preliminary stages of the systematic audit.

TABLE II. CSPs EVIDENCES

C	CSP 'A' Evidences	CSP 'B' Evidences
C1	Hardware & software monitoring tools for	• Dedicated monitoring systems that monitor

	acceptable service performance & availability.	services for failure. • Automatic service availability and recovery systems in case of system failure.
C2	• BCP & DRP services and policies for fast recovery of critical IT systems. • Automated backup methods. • Redundancy on multiple devices across multiple locations.	• BCP & DRP services and policies across all data centres in multiple locations. • Entities stored in a redundant environment with robust backup, restore, and failover capabilities for ensuring availability
C3	• Web service support for technical or account issues. • Additional support features provided using voice calls, user guide, and knowledge centres.	• Customer support services provided to users through online help, community forums, online requests, and voice call supports,
C4	• An integrated server-side encryption for data-at-rest is used to store data in encrypted form. • Users are also encouraged to encrypt data at rest, and in transit over the network. • Keys are stored in separate locations from the data for enhanced key management.	• Industry cryptographic standards such as SSL/TLS are used to protect data integrity. • For further data protection, an encryption mechanism using AED is deployed on servers that hold messaging data including emails and IM conversations.
C5	• Identity & access control management that allow the creation and management of multiple users based on credentials & permissions. • A multi factor authentication is also supported as an additional layer of security for accessing data & applications.	• Data and services are secured using identity & access control management at the data center, network, logical, storage and transit levels. • Azure Active Directory is used as the underlying identity platform. Federated identity and single sign-on security provided.
C6	Third party audits and certifications issued by: ISO27001, ISO27018, Safe Harbor, SSAE16, SOC1 Type II, SOC2 Type II, and FISMA	Certified against third party attentions as: FEdRAMP, FIPS 140-2, FISMA & DIACAP, HIPAA, ISO 8001, ISO27001, ITAR, PCI-DSS Level 1, SOC1-3, CSA's CAIQ, and MPAA
C7	Support standards as OGF, CDMI, OCC, OData, DMTF,	Support OGF, CDMI, OCC, OData, and DMTF formats

Monitoring

As a means of ensuring continuous monitoring of research data and code repository by the printing company, the two CSPs enable a significant number of events monitoring techniques in different areas of their services that allow CSCs to monitor resources and applications after migration. One of such technique involves regular penetration testing and vulnerability assessments against their services as part of a move to mitigate evolving threats and new attack patterns, and also on the protection of customer data. Another process adopted involves incident response process and forensic investigations on recorded security incidents. This is demonstrated in the evidences. Our analysis in this regard looks into the techniques for monitoring security operations and processes, and receiving alerts on security incidents and breach of privacy to entities as acclaimed by the CSPs. However, CSP 'B' offers an infrastructure monitoring capability with additional features and flexibilities that monitors the internal working of servers, which checks for information such as security status, system availability and performance, and network usage. It also offers notification flexibilities of defining rules and specifying how and to whom message is sent when an alarm is triggered.

Assurance

The evidences provided by the CSPs were used to determine the level of assurance(s) that can be assigned to the ability of their offerings to satisfy the goals. In determining assurance level, each evidence is compared against the assurance levels defined in the previous section. For instance, condition 3 (C3) requires a customer service support. CSP 'A' fulfilled the condition by generating evidences manifesting the implementation of a web-enabled customer service that support users with technical and account related issues. It also provides additional support features using voice calls, user guide, and knowledge centers. This evidence is ranked with a 'Level 3' assurance because CSP 'A' has a running customer service support that is rendered through various platforms to adequately meet the printing company's requests when the need arises. The same process of ranking is applied to all of the evidences. The table below provides assurance ranking for the respective CSPs.

TABLE III. ASSURANCE RANKING

Condition ID	CSP 'A' ASSURANCE LEVEL	CSP 'B' ASSURANCE LEVEL
C1	Level 2	Level 3
C2	Level 3	Level 3
C3	Level 3	Level 3
C4	Level 3	Level 3
C5	Level 3	Level 3
C6	Level 2	Level 3
C7	Level 3	Level 2

Assurance table III illustrates the various level of assurances accorded to the CSPs. Both CSPs adequately implement and demonstrated evidences to fulfill conditions. This may be due to the fact that we selected two market leading and reputable CSPs. The choice of selection in such scenario remains with the management involved. However, in consideration of the additional monitoring capabilities supported by CSP 'B', we see it as more suitable for adoption.

C. Discussion

A brief description of the use case scenario allows us to exemplify the implementation of the security audit approach. We particularly focused on the applicability of the concepts, while referring to existing CSP offerings. The main contribution of the approach is to support potential cloud users to perform a comprehensive investigation of CSP offerings based on goals and conditions. In other words, it allows users to define specific goals and introduce conditions in relation to the goals in order for prospective CSPs to exhibit the design and strategy in their environments that fulfill user expectations. Furthermore, our work also allows users to closely examine the existence of tools in CSP environment that allows them to continuously monitor security events regarding their entities particularly for internal security and compliance purposes. The case study results revealed that there are adequate evidences from two chosen CSPs to support the goals and conditions of the studied company. Therefore, in most cases assurance is designated at level 3. However, CSP B provides enhanced infrastructure monitoring capabilities as an additional feature to the users that support monitoring after migration. We communicated the studied results to the top management of the company and studying the results, the organization planned to migrate into CSP B.

V. CONCLUSION

Cloud computing is increasingly assuming a prominent and leading role in businesses for the purpose of operational efficiency and cost reduction. In spite of the numerous benefits, users remain anxious about data protection and dependency on CSP for business continuity. We proposed a security audit approach to evaluate offerings of CSPs based on user needs. The approach takes the viewpoint of cloud adoption use case that defines user goals and identifies risks that may likely obstruct the fulfillment of such goals. And based on the goals, conditions (extracted from industry accepted guidelines) are introduced that must be satisfied before cloud services are purchased. Evidences are then collected from CSPs for evaluation and determining the level of assurance that can be assigned to CSP services so that users can feel confident with the migration decision and their ability to monitor their data and applications after migration. The approach also defines an assurance ranking scheme through which collected evidences are compared to a predefined criteria for establishing the strength of CSP environment using the evidences they have provided. Therefore, the underlying concepts by this work allow the user to audit the CSP even before migration decisions are taken. A real-world case study adopted for this approach has shown that the concepts adequately support users to asses CSP offerings. The results generated from the use case also provided a timely support to the management in taking the migration decision and advised on the issues that need adequate attention. It also demonstrates determining the stability, trustworthiness and capability of CSPs. However, the paper did not provide details on how to execute the audit process, hence we need to provide guidelines to users on how the concepts should be used in performing the audit. Therefore, we are planning to develop a systematic process along with guidelines using these concepts to support users with the audit. Furthermore, we also intend to implement our approach to a different case study to generalize findings and refinement of the work.

ACKNOWLEDGMENT

This work was partly supported by the Austrian Science Fund (FWF) project no. P26289-N23.

REFERENCES

[1] B. Halpert “Auditing Cloud Computing: A Security and Privacy Guide”. John Wiley and Sons Inc, Hoboken, New Jersey, 2012.

[2] J. Sinclair “Auditing in Cloud Computing,” SAP Research, CEC Belfast, 2010. Available at: http://www.slideshare.net/jonathansinclair86/cloud-auditing.

[3] Q. Wang, C. Wang, K. Ren, W. Lou, J. Li, , “Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing,” IEEE Transactions on Parallel and Distributed Systems, vol. 22, no. 5, 2011.

[4] M. R. Gohel and B. N. Gohil. “A New Data Integrity Checking Protocol with Public Verifiability in Cloud Storage”, Advances in Information and Communication Technology, Volume 374, 2012.

[5] Cloud Security Alliance. “Cloud Control Matrix”, 2011 Available at https://cloudsecurityalliance.org/research/ccm/.

[6] A. van Lamsweerde. “Goal-Oriented Requirements Engineering: A Roundtrip from Research to Practice”. In Proceedings of 12th IEEE International Requirements Engineering Conference. Kyoto, 2004

[7] National IT and Telecoms Agency, “Cloud Audit and Assurance Initiatives”. The National IT and Telecoms Agency, Denmark 2011. Available at: http://www.digst.dk/~/media/Files/

[8] M. Ouedraogo, H. Mouratidius “Selecting a Cloud Service Provider in the age of cybercrime”. Journal of Computers & Security, 2013.

[9] S. Pearson and G. Yee. “Privacy and Security for Cloud Computing”, Computer Communication and Network, Springer, 2013.

[10] J. Ryoo, S. Rizvi, W. Aiken, and J. Kissell “Cloud Security Auditing: Challenges and Emerging Approaches," IEEE Security and Privacy, vol 12 issue 6, 2014.

[11] S. Islam, E. Weippl, K. Krombholz, A Decision Framework Model for Migration into Cloud:Business, Application, Security and Privacy Perspectives, Proceeding on 16th International Conference on Information Integration and Web-based Applications & Services(iiWAS 2014)

[12] Microsoft Office 365 Dedicated Service Level Agreements, http://www.microsoft.com/en-gb/download/ details.aspx?id=18128

[13] H. Mouratidis, S. Islam, C. Kalloniatis, S. Gritzalis, A framework to support selection of cloud providers based on security and privacy requirements. Journal of Systems and Software, Vol 86, issue 9, 2013 Elsevier,