Cloud security audit – issues and challenges

Livia Maria Brumă
Economic Informatics Doctoral School
The Bucharest University of Economic Studies
Bucharest, Romania
brumalivia@gmail.com

2021 16th International Conference on Computer Science & Education (ICCSE) | 978-1-6654-1468-5/21/$31.00 ©2021 IEEE | DOI: 10.1109/ICCSE51940.2021.9569654

***Abstract*—This paper analyzes the cyber security audit program of services, infrastructure and processes offered through the cloud computing technology. The first part of article presents the importance of performing the process of audit, general concepts of information security audit as well as the limitations of traditional methods for auditing complex systems, such as the cloud computing. In the second part there are presented frameworks for audit planning, that can be used for every cloud model.**

Keywords—cloud computing, security audit, information security, cyber security

I. INTRODUCTION

Cloud technology has become a component part of daily activities in the corporate, industrial, medical, educational and domestic use, evolving from concept to reality. NIST defines cloud computing as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" [1]. The advantages of this new type of technology, such as scalability, elasticity, mobility or reduction of the initial costs dedicated to the infrastructure have led to large-scale adoption, offering solutions that meet current digitalization needs. At the same time, the number and complexity of cyber-attacks on Internet-connected infrastructures have grown exponentially, requiring specialized solutions and methods to respond to threats.

Because in today's society, the most important asset is information, information security and thus cyber security has become one of the main challenges that cloud service providers and users must respond. Security auditing and compliance validation could be a solution to respond these challenges. Regardless of the technologies used, on-premises or off-premises, the main components of information security remain confidentiality, integrity, non-repudiation and availability. The same way, security strategies adopted use the same methods of protection as defense in depth, through different protection layers provided by equipment, layered defense, data and channel encryption or applying of restrictive configurations. These traditional security methods cannot fully respond to current complex threats, requiring new approaches, adapted to cloud technologies.

Depending on the services used, customers may implement various security policies designed to provide the appropriate degree of protection for the data and information processed. The security policies created, regardless of their procedural or technical nature, must create a balance between the security offered and the ability to perform operational tasks. In cloud, one of the most used security models is the *shared responsibility* one, that shares the responsibility related to compliance and security between provider and user without having a common database of information regarding the mechanisms implemented by each entity. These models create difficulties in conducting cyber security audit processes, necessary in the risk management and in choosing the right solutions for securing cloud resources. The importance of the cyber security audit is given by the results obtained after the evaluation of the security controls and the analysis of the systems vulnerability. This article analyzes the Cyber Security audit process of the services offered through the cloud. The first part presents general concepts of information audit as well as the limitations of traditional methods for auditing complex systems, such as cloud computing technology. In the second part there are presented frameworks for audit planning, that can be used for every cloud model.

II. INFORMATION SECURITY AUDIT PROCESS

The main purpose of the cybersecurity audit program within an organization is to verify the operational processes in the area of information technology in order to establish their degree of quality and compliance. This process examines both specific components, such as applications, security equipment used to implement the concept of defense in depth designed to protect the confidentiality, integrity and availability of systems and information, databases, operating systems, and processes that consider the impact of privacy (compliance with laws and standards) [2]. ISO defines the audit as "a systematic and independent examination to determine whether quality activities and related results comply with planned arrangements and whether these arrangements are implemented effectively and are suitable to achieve objectives ". [3]

The challenges of the security audit of cloud technologies are mainly due to the complexity of these systems, the differences between public and private clouds, the disappearance of the concept of perimeter between the cloud and the organization's systems. There are important differences between the high-level recommendations provided in most cloud-specific standards and the low-level logging information currently available in existing cloud infrastructures. In practice, only limited forms of auditing may be performed by CSC administrators, and there exist a few compliance tools with several major limitation [4].

The results obtained provide useful information for understanding and addressing the risks associated with cloud technologies - security, confidentiality and data integrity, business continuity plan, reliability of processes and systems, effectiveness / efficiency of new business processes, compliance with inter-jurisdictional regulations. [5]

Audit methodologies and security methods used so far cannot be fully applied to cloud services because the features that led to the widespread adoption are completely different from traditional technologies. Thus, the virtualization of

resources, the fact that the concept of shared responsibility is used and the inability to audit the equipment that is the responsibility of the service provider make the audit process in the cloud require new methods and processes. It is important to specify that in the case of public cloud architectures, the security audit performed by the client refers to "audit in the cloud", and "audit of the cloud" can be performed only for private clouds. Depending on the chosen cloud service, the security audit process will target the following components, respecting the principle of shared responsibility: [6]

TABLE I Shared Responsibility Model

	IaaS	PaaS	SaaS
CSC	People Data Applications Operating System Virtual Networks	People Data Applications	People Data
CSP	Hypervisors Servers Storage Physical Networks	Operating System Virtual Networks Hypervisors Servers Storage Physical Networks	Applications Operating System Virtual Networks Hypervisors Servers Storage Physical Networks

The simplest model to audit, from a CSC perspective, is the SaaS model because the responsibility of security is only for people and data. In the same time, the CSC who audit only people and data must trust the audit report from CSC because having no responsibility over the other components, cannot conduct a security audit.

The cloud audit process can be classified according to security objectives and requirements, how it is defined as a public, private, internal or external audit with or without the support of a TPA (third-party auditor) [7]

a) internal audit - the role of internal audit is to help manage and assess the security and compliance risks of the services provided by CSP. The whole process is carried out exclusively by the organization, through its own methods and mechanisms, without the support of other entities involved in cloud administration and its key role is to ensure the organization's management that all information security risks are identified.

From an internal audit perspective, other issues arise in determining which part of the cloud stack is audited, such as controls for a system in which services and infrastructure are constantly evolving and changing. Figure 1 illustrates the main challenges faced by the internal audit, like defining the scope, dependence of third party, access to skills and expertise and access to date [8].

b) cloud provider auditing - auditing is performed and conducted by CSP. Giants CSP (like Google Cloud, Azure, IBM) offer certain audit reports that certify compliance with international standards (Cloud Security Alliance Control Matrix, ISO 27001, SOC 2 etc.) and can be accessed via their websites.

c) public audit-TPA - is performed by entities independent of the organization and provides objective results compared to an internal audit or CSP [9]. One of the biggest companies that provides security audit is Delloite who use the following approach [10]

- Testing logical and physical security controls
- Testing IT operations
- Testing disaster recovery procedures
- Testing business continuity

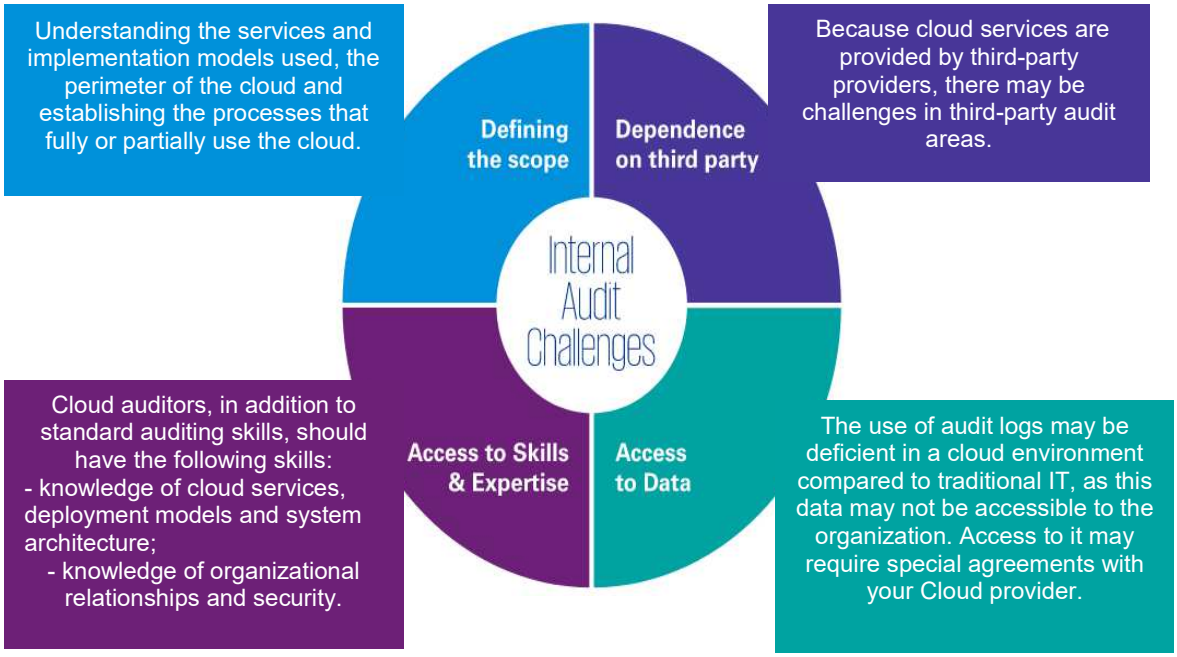

Fig. 1 Cloud Internal Audit Challenges [8]

- Data integrity assessment
- Assessment of controls over critical system platforms, network and physical components, IT infrastructure supporting relevant business processes
- IT strategy preview
- IT organization review
- IT process review (helpdesk, service management, application management oversight).

In Table 2 are presented a series of recommendations for CSP and CSC after going through an audit process, regardless of the audit method used from the three previously presented:

TABLE II Recommendations for CSP and CSC

Cloud Service Consumer	Cloud Service Provider
• communicating the results of the clients' audit in which to be mentioned especially the scope of assessments, which services may fall under the incidence of certain laws and regulations and the clear establishment of the client's responsibilities; • maintaining the certificates of conformity and communicating any change in its status; • providing clients with the necessary audit artifacts that cannot be collected by them.	• Understand compliance obligations before deploying, migrating, or developing in the cloud. - Evaluates CSP attestations and certifications • Try to select auditors with experience in cloud computing, especially if audits and pass-through certifications will be used to manage the client's audit area.

Existing methods for cloud audit are divided into three categories: retroactive, intercept-and-check and proactive auditing [11].

1. Retroactive and Intercept-and-check audit are the traditional methods of conducting the audit process. Retroactive auditing, is based on detection of intrusion and known vulnerabilities using security patches and updates. The same system is subject to the action of input parameters, to see the result of using the patches [12]. There are multiple security solutions for auditing, developed by major cloud technology companies, including Microsoft's SecGuru used to audit network connectivity in Azure data centers, IMB QRadar - SIEM (Security Information and Event Management) IBM has integrated modules, and Amazon offers various web APIs for WS CloudWatch & CloudTrail customers that can be used for auditing [13]. There are also various open-source solutions that can be used in the security audit process, Osquery, an operating system analysis utility created by Facebook, which allows low-level analysis for end-point devices based on SQL queries [14]. CloudSploit ensures the detection of security risks in the cloud infrastructure, returning a series of configuration errors and associated vulnerabilities [14]. Intercept-and-check method perform major verification tasks while holding the event instances blocked [16].

2. Proactive Audit - the proactive approach in conducting the security audit consists of combining the traditional audit methods mentioned in point 1 and the incident management activities [13].

III. INFORMATION SECURITY AUDIT PLANNING

A. Planning the audit

In order to carry out an audit process that provides management structures with feedback-useful for improving processes and activities that can cause damage to information assets, it is necessary for organizations to implement audit policies specific to the type of data used. The planning of an audit activity has in view the establishment of the necessary stages depending on the specifics of the organization. Usually, planning consists in setting audit objectives and purpose:

- audit objectives - the planning phase of this process involves the auditors to form an overview of the organization and the processes carried out. It is necessary to collect information from all audited segments in order to understand the policies, specific internal regulations and the way the organization works [17].
- audit scope - defining the purpose of the audit is done by identifying all components included in the process - personnel, systems, processes. The predominant use of virtualization to allocate resources complicates the audit process because the abstraction of resources makes it difficult to identify all assets for audit purposes. To address this issue, some CSPs provide consumers with audit reports from third-party companies that can confirm whether their infrastructure meets compliance standards [18].

ISACA proposes an audit / assurance program based on 3 steps - planning and scoping the audit, governing the cloud and operating in the cloud. The security of data and information is analyzed with the help of the controls from the third stage, according to table 3:

Table III – ISACA Audit/Assurance Program Step

Category	Description	Step
Incident Response, Notification and Remediation	Incident notifications, responses, and remediation are documented, timely, address the risk of the incident, escalated as necessary and are formally closed	• Incident Response • Service Provider Issue Monitoring • Customer Issue Monitoring
Application Security	Applications are developed with an understanding of the interdependencies inherent in cloud applications, requiring a risk analysis and design of configuration management and provisioning process that will withstand changing application architectures.	• Application Security Architecture • Configuration Management and Provisioning • Compliance • Tools and Services • Application Functionality
Data Security and Integrity	Provides confidentiality, integrity and availability for applications.	• Encryption • Key Management
Identity and Access Management	Identity processes assure only authorized users have access to the data and resources, user	• Identity Provisioning • Authentication

	activities can be audited and analyzed, and the customer has control over access management.	
Virtualization	Virtualization operating systems are hardened to prevent cross-contamination with other customer environments	

B. Cloud auditing standards and frameworks

The standards have the role of providing uniformity in the application of some norms, characteristics and implementation frameworks, having a very important role in the development of the audit processes. The rapid evolution of cloud technologies determines the achievement of standards applicable to all CSPs in order to provide a degree of trust to users. The traditional IT infrastructures, in which all the hardware and software components are in the administration of the organization, allow the development of complex and detailed audit processes that aim at all the components and objectives of Security. There are several organizations that have developed frameworks and standards specific to cloud technologies, among which we can mention CSA - Cloud Controls Matrix, ISACA (Information Systems Audit and Control Association) - Cloud Computing Audit Program, ENISA (European Network and Information Security Agency) etc. The main security guidelines and concepts in these standards are as follow [19]:

1. Cloud-based systems need specific security methods; traditional methods are not enough.

2. Auditors may find that the organization accumulates multiple traditional control mechanisms that are not always justified in cloud systems, representing a waste of resources, and it is necessary to eliminate them.

3. In order to carry out the audit process, it is necessary for the auditors to have detailed knowledge on the new security controls used in the cloud as well as on the basic services, such as log files, identity management, access control.

4. Establishing the purpose of the audit requires solid knowledge of architectures, which is specific to cloud topology, as it includes links to hosted or partner systems and to leased systems.

Although the implementation of standards in the cloud infrastructure is an additional assurance for users, some of the most important security threats need additional security controls. Attacks such as DoS (Denial of Service), Malware injection Attack, Authentication and MiTM Attack can only be stopped by implementing in-depth defense mechanisms and adopting a holistic, unitary security strategy that can meet these challenges.

IV. CONCLUSIONS

Cloud technology has changed the way we use computing resources and has become an integral part of today's society. The increased number of cyber-attacks on organizations that use cloud resources determines the need to carry out risk management processes that provide all the information necessary to choose security controls suitable for the organization. The security audit process is necessary and provides objective feedback on the security status of the organization. The cloud security audit differs from the one performed on traditional technologies due to the characteristics of the cloud. Thus, it is necessary to identify new methods that can respond to the specific elements of the cloud in order to carry out an audit as accurately as possible.

REFERENCES

[1] P.Melland and T.Grance, "The NIST Definition of Cloud Computing," 2011.

[2] D. C. Chou, "Cloud computing risk and audit issues," *Computer Standards & Interfaces,* vol. 42, pp. 137-142, 2015.

[3] [Online]. Available: https://www.iso.org/standard/17940.html.

[4] S. Majumdar, T. Madi, Y. Wang, A. Tabiban, M. Oqaily, A. Alimohammadifar, Y. Jarraya, M. Pourzandi, L. Wang and M. Debbab, in *Cloud Security Auditing*, Springer, 2019.

[5] [Online]. Available: https://www.ucop.edu/ethics-compliance-audit-services/_files/webinars/10-14-16-cloud-computing/cloudcomputing.pdf.

[6] [Online]. Available: https://www.aws.training/Details/eLearning?id=41556.

[7] M. Kolhar, A. Alameen, B. Dhupia, S. Rubab and M. Gulam, "Cloud Computing Data Auditing Algorithm," Notion Press, 2017.

[8] [Online]. Available: https://home.kpmg/be/en/home/insights/2020/11/ta-cloud-computing-and-the-internal-audit-function.html.

[9] F. OGÎGAU-NEAMȚIU, CERCETARI PRIVIND SECURIZAREA INFORMATIEI TN SISTEMELE CLOUD COMPUTING, Brașov, 2018.

[10] [Online]. Available: https://www2.deloitte.com/rs/en/pages/technology/solutions/it_audit_and_information_system_security_deloitte_serbia_technology_services_solutions.html.

[11] M. Ou, L. Wang and H. Xun, "DeaPS: DeepLearning-Based User-Level ProactiveSecurity Auditing for Clouds," in *019 IEEE Global Communications Conference (GLOBECOM)* , 2019.

[12] [Online]. Available: https://people.csail.mit.edu/nickolai/papers/wang-rad.pdf.

[13] S. Majumdar, in *Proactive Security Auditing for Clouds*, Montreal, 2018.

[14] [Online]. Available: https://osquery.readthedocs.io/en/stable/.

[15] [Online]. Available: https://github.com/aquasecurity/cloudsploit.

[16] u. Majumdar, T. Madi, Y. J. M. Pourzandi, L. Wang and M. Debbabi, "Cloud Security Auditing: Major Approaches andExisting Challenges".

[17] G. Fazekas, "Cloud Computing Auditing," 2018.

[18] (ISC)2® CCSP® Certified Cloud Security Professional Official Study Guide.

[19] J. Rissi and S. Sherman, "Cloud-Based IT Audit Process".