УДК 657.633:004.056:[004.383.2:004.738.5]

*L. Khodakivska,*
*PhD in Economics, Associate Professor of the Department of Accounting and Economic Control, Poltava State Agrarian Academy, Poltava*
*ORCID ID: 0000-0002-6758-697X*
*V. Plaksiienko,*
*Doctor of Economic Sciences, Professor,*
*Head of the Department of Accounting and Economic Control,*
*Poltava State Agrarian Academy, Poltava*
*ORCID ID: 0000-0003-0371-1054*
*Y. Hrybovska,*
*PhD in Economics, Associate Professor of the Department of Accounting and Economic Control, Poltava State Agrarian Academy, Poltava*
*ORCID ID: 0000-0001-5205-9045*

DOI: 10.32702/2306-6806.2019.10.26

# INTERNAL AUDIT AND CLOUD INFORMATION SECURITY

*Л. О. Ходаківська,*
*к. е. н., доцент, доцент кафедри бухгалтерського обліку та економічного контролю,*
*Полтавська державна аграрна академія, м. Полтава*
*В. Я. Плаксієнко,*
*д. е. н., професор, завідувач кафедри бухгалтерського обліку та економічного контролю,*
*Полтавська державна аграрна академія, м. Полтава*
*Ю. М. Грибовська,*
*к. е. н., доцент, доцент кафедри бухгалтерського обліку та економічного контролю,*
*Полтавська державна аграрна академія, м. Полтава*

**ВНУТРІШНІЙ АУДИТ І ХМАРНА ІНФОРМАЦІЙНА БЕЗПЕКА**

***In the past decade more and more companies moving their operations to the Cloud. In each case the reason for this decision is different: some are looking for a better ability to streamline the company processes and workloads and gain more robust organization flexibility. Others are after faster applications deployment and an ability to expand in different business areas. On the other hand, some companies just want to standardize their IT-capabilities by providing more unified software solutions across the enterprise. However, there are a few common grounds between all of these companies in their decisions. First, they want to cut cost (on technology infrastructure as well as software licensing). Secondly, they want to become less dependent on the delivery platform at the same time as get easier adaptable to changes in the IT-environments. Third, they want to get closer to their customers by providing new services and marketing programs at the same time as getting that done more efficient and cheaper. Fourth, these companies want to change their capital investment structure by reducing the cost structure. The number of benefits for the companies moving to the Cloud is endless; however, the potential security cost increases significantly as well. By moving to the Cloud, the companies losing one of their most valuable assets: ability to control their underlined infrastructure and create self-governed environments. On the Cloud this responsibility will be fully delegated to the Cloud service provided. In most instances, the space on the Cloud servers will need to be shared across multiple non-related companies, where some of them might have different standard of internal security and create extra, unnecessary traffic to the shared servers. That unrelated traffic might slow down all renters located on this Cloud server. Finally, the companies will expose their data to outside world as never before. That can create an opportunity to the malicious individuals to steal and compromise the information. Without adequate security protocols, established intrusion detection mechanisms, and full understanding of possible risks, decision to move to the Cloud should not be made. But even after the decision is reached, a search for the Cloud service vendor must be done in the very meticulous way. A common determination what data to put on the Cloud and what not must be accepted and verified on all technical and business levels of the company. And finally, an appropriate level of the data security and encryption must be established and enforced. This article will review risks and benefits of the decision to move to the Cloud in more details and address some aspects that companies need to take into consideration before making such type of move.***

***В останнє десятиліття все більше і більше компаній переводять свої операції на Хмару. У кожному випадку причина цього рішення різна: деякі шукають кращу здатність спростити процеси, робочі навантаження компанії і отримати велику гнучкість організації. Деякі — більш швидкого розгортання додатків і можливості розширення в різних сферах бізнесу. З іншого боку, деякі компанії просто хочуть стандартизувати свої IT-можливості, надаючи більш уніфіковані програмні рішення для всього підприємства. Проте є кілька загальних підстав для всіх цих компаній в їх рішеннях. По-перше, вони хочуть скоротити витрати (на технологічну інфраструктуру і ліцензування програмного забезпечення). По-друге, вони хочуть стати менш залежними від платформи доставки і одночасно легше адаптуватися до змін в IT-середовищах. По-третє, вони хочуть стати ближче до своїх клієнтів, пропонуючи нові послуги і маркетингові програми, одночасно роблячи це більш ефективним і дешевшим. По-четверте, ці компанії хочуть змінити свою структуру капіталовкладень, скоротивши структуру витрат. Кількість переваг для компаній, які переходять на Хмару, нескінченна. Проте потенційна вартість безпеки також значно зростає. Перейшовши на Хмару, компанії втрачають один зі своїх найцінніших активів: здатність контролювати свою власну інфраструктуру і створювати самокеровані середовища. На Хмарі ця відповідальність буде повністю делегована компанії, яка надає Хмарні послуги. У більшості випадків простір на Хмарних серверах може бути розподілений між кількома непов'язаними між собою компаніями, де одні з них можуть мати різні стандарти внутрішньої безпеки і створювати додатковий непотрібний трафік для загальних серверів. Цей непов'язаний трафік може уповільнити роботу всіх орендарів, розташованих на цьому хмарному сервері. Нарешті, компанії будуть відкривати свої дані зовнішньому світу, як ніколи раніше. Це може створити можливості зловмисникам вкрасти і скомпрометувати цю інформацію. Без адекватних протоколів безпеки, встановлених механізмів виявлення вторгнень і повного розуміння можливих ризиків, рішення про перехід на Хмару не повинно прийматися. Але, навіть після того, як рішення буде прийнято, пошук постачальника Хмарних послуг повинен бути виконаний дуже ретельно. Загальне визначення того, які дані поміщати на Хмару, а які ні, слід приймати і перевіряти на всіх технічних і бізнес-рівнях компанії. І, нарешті, необхідно встановити і затвердити відповідний рівень безпеки та шифрування даних. У цій статті буде більш докладно розглянуто питання про ризики та переваги рішення про перехід на Хмару і розглянуто деякі аспекти, які необхідно враховувати компаніям, перш ніж робити подібні дії.***

*Key words: Cloud based services, Cloud system management, SaaS, PaaS, IaaS, data security, system vulnerabilities, DevOps.*

*Ключові слова: хмарні сервіси, управління хмарними системами, SaaS, PaaS, IaaS, безпека даних, вразливість системи, DevOps.*

## PROBLEM DEFINITION

Growth of the Cloud based computing platforms forced a significant number of companies around the world to move their applications and services to there. Such type of move can improve the life hood of the company and give it a significant advantage over its competitive. What pros and cons of this decision and how internal auditors can help senior leaderships of the company to make the right decision will be discussed in this article.

## ANALYSIS OF THE LATEST RESEARCHES AND PUBLICATIONS

Researches of the risk and benefits of the migration to the Cloud and possible recommendations on this process were a center points of the publications done by The Dallas Chapter of the Institute of Internal Auditors, Gartner Research, Sandy Pundmann, (U.S. managing partner, Internal Audit) and Clay Young, (partner and U.S. IT Internal Audit practice leader), David Linthicum (Chief Cloud Strategy Officer, Deloitte Consulting).

## TASK DEFINITION

Describe costs and benefits of the decision to move company applications and services to the Cloud and what kind of preventive mechanisms need to be established to make this transition successful and cost effective.

## PRESENTATION OF THE RESEARCH MATERIAL

According to the general definition of the Cloud computing, it is a model that enables on demand availability of the network pool of the shared configurable computer resources (data storage, applications, servers and etc) that do not require direct constant and persistent management by the end users. These Cloud-based resources can be easily provisioned for specific purpose and task by the company that lease them and release after the need for the them is no longer there [1].

The Cloud computing is usually represented in the way of three service models (platforms):

1. Software as a Service (SaaS) — in this model, the company runs application (owned/rented/licensed to the provider) on the infrastructure platform provide by the vendor and these applications accessible from inside (or outside) of the company network on authorized devices. The company that rents the service does not manage nor responsible for the Cloud infrastructure but can be authorized to make application configuration settings that affect user experience of the company employees or customers [1; 8].

2. Platform as a Service (PaaS) — this model allows companies that rent the service to deploy to the Cloud proprietary, self-developed, or licensed to renter company applications that can must by supported by the Cloud service provider. Still, as in the previous model, the company

that lease the service does not have an ability to manage the Cloud infrastructure but can control deployed applications and their settings [1; 8].

3. Infrastructure as a Service (IaaS) — that model gives the company that lease the service the most options, like deploying software package and applications of the company choice on the operation system selected and configured exclusively by the client itself. The company can also manage Cloud storage, networks and Cloud workflow processing. Despite the fact that even in this situation the lease company does not have a direct control of the Cloud infrastructure and OS. However, all other aspects of the network controls are present [1; 8].

What model company choses depends on multiple positions, such as importance of the data that will be store on the Cloud and data privacy issues; ability of the Cloud provide to protect data from unauthorized access; type of application that company plans to move to the Cloud and access level across multiple regions, ability of the Cloud service provide to meet changing demands in service on the rapid basis, and of course, cost of the change compare to the current level of expenditures. The risk of moving to the Cloud will always be there; however, the current adoption rate signifies a notable point where Cloud adoption became a mainstream venue. The numbers below just support that statement:

1. As of end 2019 year the global Cloud computing market is projected to reach $258 billion. According to the forecast, that number will more than double by 2023 and should be reach $623.3 billion [2].

2. As estimated 90 % of small to medium to large companies have their presence on the Cloud already with approximately 60 % of the workload running there. And that number is just going to increase year over year. Considering the numbers above, about 1/3 of the IT budget these companies already designating for the Cloud development [3].

It is worth to mention, however, that small and medium companies with expectation of the rapid growth, are more acceptable to the Cloud move compare to the large organization with large IT departments that tend to stay on the sidelines (to the most part). That is due to the cost of the move (monetary as well as reputations risks because of the possible data breaches), opposition from the upper management due to the upfront investment in the technology, and not definitive cost advantage (as of the current moment), as well as a need to change the established business process. With all of that holds true, the large companies are also moving to the Cloud (on the slower pace) because of the major shift of doing business in the modern digital world.

3. Cloud infrastructure spending is going to reach approximately $80 billion by the beginning of 2019. That is 69 % increase compare just to 2017 where the same spending was $55 billion [4].

However, everything shown above is just an illustration of the trend. The question is: why this trend even exists and what company can gain from moving to the Cloud? First and foremost, the companies are looking for their bottom lines: cost and revenues. Businesses seeing in this migration a huge saving opportunity in outsourcing maintenance and support of data centers, supporting infrastructure, and labor cost. That is alone might save some companies up to 1/3 of their IT budget annually. Other driving force behind the move is software maintenance and rapid deployment of the application packages across the enterprise. In the traditional environment at least 30 % to 40 % of the time and efforts support personal spend on testing, verifying, and installing software patches to different servers and platforms, as well as monitoring ongoing activities and providing infrastructure support. With the Cloud solution, all of that will be transferred to the Cloud service provider. Finally, there is one more aspect that worth to mention: more and more companies want to have not just a content on the Cloud to be distributed to the end user but being able to use this content in combination with different social media platforms, perform data analytical functions, apply elements of artificial intelligence (AI) tools in the their offering as well as data gathering and data manipulation mechanisms in the internal networks. Above all, the Cloud solutions offer companies an easy, fast, and efficient way to communicate with different categories of customers (current and future) and provide a much more targeted marketing campaign [5].

All of the above means one thing: moving to the Cloud will be inevitable action for majority of the small to medium and to some extend for large companies in the next 10 years. The role of the internal audit committees is to evaluate the risks of the adoption and find the best balance between benefits the Cloud platforms offer and potential exposure to the risk factors this new technology poses. To do that correctly internal auditors need to understand a few key factors:

1. Scalability of the Cloud platforms and DevOps development.

One of the main advantages of the Cloud solution is its scalability. In a few words that technology can be explained as on demand increase or decrease of the available resources (capacity) due to the current business needs. That mechanism is a huge selling point for any company to move to the Cloud. In essence, such approach is very expensive to introduce on the in-house networks when all of the infrastructure needs to be bought, configured, and released to production well in advance of the growing demand. That is especially expensive for the companies which cannot predict a demand for their product on the medium to long range. That means a big risk to these companies with investment in the hardware and software that might not even needed. The Cloud solution solves that problem in an instance. The peak demands can be easily met but allocating necessary processing power, storage, and bandwidth on the moment notice. Also, most of the companies do not rely on just one Cloud. They use a hybrid approach where different applications operate on different Clouds. That creates a sort of a guarantee that at no time all of the processing workflows will be offline due to unforeseen circumstances [6].

The other attraction of the Cloud based solution is a DevOps development lifecycle. The Gartner defines it as a method that represents a global change in the IT life cycle development and focusing primarily on "...rapid IT-service delivery through the adoption of agile, lean practices in the context of a system-oriented approach" [10]. This technique put a focus on people, people's culture and cooperation between development teams. The main goal of this technology is to utilize automation tools and put focus on increasing use of the dynamically programmable infrastructure from the view point of the life cycle of the product.

At its core, DevOps is a set of centralized platform tools that allow developers to respond to the business needs very rapidly and without any latency that usually surrounds traditional software development methods. All of that with the lower cost, and shorten development, testing, and deployment cycles, because of its centralized nature. Currently, most of the Cloud service provides support DevOps and its continuous integration and development strategy. That native support of the tool and established integration with the Cloud infrastructure, lowers the development and operational cost of the in-house applications and provides better centralization management of the whole Cloud application environment [9].

However, the same mechanism that makes Cloud solution so attractive can also poses a danger. Misconfigurations, security holes, software and hardware vulnerabilities, data transmission without proper encryption and etc create a honey pod for attackers. Even looking on

something as simple as a password protection between different Clouds, can show what problem is that. In theory, each Cloud and possible even each container within a Cloud should have its own administration management console with specific set of rules, privileges and access level. However, that might not be a case in the fast pace changing environment where driving force is DevOps system. With that many changes happening rapidly on very regular basis, such precautions can be "forgotten" or circumcision. To avoid that, and enforce the security rules, internal auditors must be familiar with this concept and technique first hand [9].

2. Company internal data security rules and regulations.

Regardless of the Cloud company choses (private or public) and the subscription model (SaaS, PaaS, IaaS), the company itself still does not have a full control of the Cloud infrastructure, nor OS this infrastructure operates on, nor the whole security protocols the service provider has. Because of that it is imperative for the internal auditors to understand and enforce strict rules and regulations in regard to the company data usage and access authorization, full understanding of the safeguard mechanisms vendor applies to their assets, level of the security compliance the vendor has and what steps it takes to keep it on the constantly acceptable level [7; 8].

3. Data storage, manipulation, backup, transmission and adequate level protection.

Because of the nature of the Cloud platform, the data will always be saved on the Cloud platform and travel between Clouds, network services, applications, databases and etc. The users will see it on the Application Programming Interfaces (API). That weakness can be exploited by the attackers to get unauthorized access. To establish a satisfiable level security for the data storage, use, and transmission, the following mechanisms need to be established and enforced:

I. Establish organizational access level of the data and classify all of the customer, proprietary, and private data based on the access level.

II. Enforce security of the user and system accounts by enabling complexity level of the passwords and password expiration date of no more that 30 days (system accounts need to use random password generation techniques with the password vault storage approach).

III. Prevent use of the default password on all levels.

IV. Encryption of all of the transmitted data (between the Clouds to the network and back) and keeping customer and private data encrypted in the database as well.

V. Disaster Recovery should at paramount importance to any organization. It is even more critical for organizations saving their data on the Cloud. Before any plans to move to the Cloud will take shape, it is necessary to verify data back up solutions (based on the local network and the changes needed due to the Cloud migration, Also, it would be wise to test a verify a fall over solution if a need to switch between servers and Clouds will ever arise (to prevent interruption of the service). Data recovery benchmark and protocols need to be verify based on the internal security standards, practices and regulations. Each solution needs to be tested again before migration to the Cloud takes place as well as after the migration [7; 8].

1. Company insider thread analytics.

Regardless how good is the outside defense system, the biggest threat can lay from inside, from the company own employees. By using malware or any sort of social engineering tools or any other mechanisms pinpointed to a specific employee or employees sophisticated attackers can bypass all of the layers of security and steal the company secrets and customer private data. To prevent that from happening is very difficult. One of the ways to avert it can be repeatable training exercises of all employees where possible types of social engineering attacks will be explained. That trainings should go hand-by-hand with established powerful identity and access management framework (IAMF) and privilege management set of tools. Each of these mechanisms need to have to very sophisticated log system [8; 11].

2. System Incompatibilities.

In some instances, some applications and tools that work across network enterprise might not function properly on the Cloud platform. Because of that, it is imperative for the internal auditors to identify such type of incompatibilities to prevent inadvertent situations where incorrectly functioning applications create holes in the protection system and allow third parties to access privilege information. Attackers can exploit such misconfiguration to gain access to the system and remain undetected for a long period time. That might have very dare consequences to the company reputation [8].

3. Cloud service provider security.

Even if the company itself (as a renter of the service) does not manage Cloud infrastructure, the internal auditors must understand, verify and enforce a few security aspects of the Cloud infrastructure security and the way how the service provider manages it.

4. Cloud Service Provider Security Protocols.

— Network Segmentation must put in place by the Cloud service provider in any multi-service environments. That segmentation should isolate resources allocated to one instance (the company that lease a resource) from all others. That segmentation needs to include container, application, OS, and other types of separation in order to prevent un-authorized access to the data, verify constant amount of network resources allocated to the company share and to limit exposure to multi-cloud breach attempts.

— Discovery and Onboarding of the new and existing Cloud instances and related assets must me fully automated, grouped into sub-clouds and managed by the lease company or provided to the lease company as service by the Cloud management company. Each of these sub-clouds must have its own security and password management mechanisms, to prevent cross intrusion attempts.

— Identity and Access Management (IAM) system will always need to be in place and operational. Process of the search, verification, and prevention of the for general system vulnerabilities need to happen on the regular basis.

— Presence of the container's (virtual place on the Cloud server that is designated for the company data) account activity monitors. That monitoring should include identification and segregation of the API calls (to prevent unauthorized activities) and logging and verification of use of the management console on the Cloud server (to prevent unauthorized access from the inside the Cloud itself). Such monitoring should also include log file enablement, analyzation, access validation.

— Cloud security network configuration protocols must be presented to the internal auditors of the company that rents the service so that it would be possible to establish full compliance of these protocols to the established industry and government established requirements [8; 11].

5. Cloud Service Provider Intrusion Detection and Activity Monitoring.

Based on the model selected for the service, some of the following activities can be performed by the IT department of the company itself or outsourced the Cloud service provider. If a decision for outsourcing will be made a prior verification of the ongoing processes would be necessary to confirm compliance with the company and industry rules and regulations:

— Verification of the Cloud service provider continues operation of the vulnerability management.

— Verification of the established firewall, thread analytics and identity management.

— Verification of functionality of multiple layer security access protocols.

— Monitoring of the new activity alerts, change or activation of the established service, and modification of the access control list (ACL) or events related to ACL.

— Monitoring of the change or addition to the system policies that govern users access and roles.

— Establishing of the alert mechanisms and reporting system that evaluate daily alerts and reduces alerts that can be false positive.

— Verification of the processes that protect Cloud infrastructure of the Distributed Denial of Service (DDoS) attacks [8].

## CONCLUSION

Migration to the Cloud will continue everywhere in world and the rate of this trend will just accelerate in the very near future. Each company will have its own specific reason for the move, but majority of them can be combine into a few very specific tasks: access to the data regardless of the region; cost of the operation after the move; flexibility, mobility, and scalability of the delivery platform; increased collaboration between the development teams inside the organization as well as outsourced; efficiency in meeting customer demand for new or improve services and etc. However, all of these benefits would not be without cost. The cost will consist of the following: increased compliance regulations in regard to the customer data; legal conflicts on what proprietary applications can and cannot be deployed on the Cloud; lack of visibility and oversite of the solving performance issues (in case if they arise); possible latency on the some of the API due to multitude of the issues related to the Internet connection speed and shared (or private) connection bandwidth; shared disturbance from other clients who use the same provider; and, of course, increased security risks to the data, company business model and the company growth strategy. What strategy is right for a specific company will need to be determine based on that company adaptivity to the changing market situations. However, if a decision will be made to move to the Cloud, qualified internal auditors need to be involved from the very beginning.

References:

1. The Research Committee of the Dallas Chapter of the IIA (2012), "Cloud Computing: A Study of Internal Audit's Preparedness in the Dallas Area", available at: https://na.theiia.org/iiarf/Public%20Documents/IIA%20-Dallas%20Research%20Project%20-%20Final%-20Submission.pdf (Accessed 17 Sept 2019).

2. Liu, Sh. (2018), "Public cloud revenue worldwide from 2016 to 2027, by segment (in billion U.S. dollars)", available at: https://www.statista.com/statistics/477763/public-cloud-segment-revenue-forecast/ (Accessed 17 Sept 2019).

3. 451 Research (2017), "69 % of enterprises will have multi-cloud/hybrid IT environments by 2019, but greater choice brings excessive complexity", available at: https://451research.com/images/Marketing/press_releases/Pre_Re-Invent_2018_press_release_final_11_22.pdf (Accessed 17 Sept 2019).

4. Canalys (2019), "Cloud infrastructure spend grows 46 % in Q42018toexceed US$80 billion for full year", available at: https://www.canalys.com/static/press_release/2019/pr20190204.pdf (Accessed 17 Sept 2019).

5. Protiviti (2012), "Internal Audit's Role in Cloud Computing", available at: https://www.protiviti.com/US-en/insights/wp-internal-audit-role-cloud-computing (Accessed 17 Sept 2019).

6. Pundmann, S. Young, C. Willis, Ch. and Awasthi, D. (2018), "Moving to the Cloud? Engage Internal Audit Upfront", Deloitte Risk and Financial Advisory, Deloitte & Touche LLP, available at: https://deloitte.wsj.com/riskandcompliance/2018/11/26/moving-to-the-cloud-engage-internal-audit-upfront/ (Accessed 17 Sept 2019).

7. Utley, G. (2018), "6 Most Common Cloud Computing Security Issues — CWPS", available at: https://www.cwps.com/blog/cloud-computing-security-issues (Accessed 17 Sept 2019).

8. BeyondTrust (2019), "Cloud Security/Cloud Computing Security", available at: https://www.beyondtrust.com/resources/glossary/cloud-security-cloud-computing-security (Accessed 17 Sept 2019).

9. Linthicum, D. (2019), "DevOps dictates new approach to cloud development", available at: https://techbeacon.com/app-dev-testing/devops-dictates-new-approach-cloud-development (Accessed 17 Sept 2019).

10. Gartner (2019), available at: https://www.gartner.com/it-glossary/devops/ (Accessed 17 Sept 2019).

11. MacDonald, N. (2019), "Market Guide for Cloud Workload Protection Platfor", available at: https://www.gartner.com/doc/reprints?id=1-6JH8ZKN&ct=-190417&st=sb (Accessed 17 Sept 2019).

*Стаття надійшла до редакції 29.09.2019 р.*