DOI: 10.5281/zenodo.4383046

RISKS AND BENEFITS OF ADOPTING CLOUD ACCOUNTING

Daniela MITRAN, PhD Associate Professor
Athenaeum University, Bucharest, Romania
danielamitran@yahoo.com

Abstract: *The current business environment is extremely dynamic and competitive. Elements such as access to information, its transmission speed, quick decision making, mobility, and flexibility have become more and more important for companies operating in the field. Given that information technology has evolved incredibly fast over the past decade, digital technologies such as cloud computing, e-commerce, and mobile applications provide opportunities to improve networking with partners and customers, and new ways to generate value. Cloud applications have gradually gained ground to the detriment of locally operated applications. There are numerous advantages of cloud technology which can no longer be overlooked, especially by small- and medium-sized companies. At company level, regardless of its size or activity, the decision to change the accounting software is critical and may have a major positive impact on the business, nevertheless involving a series of risks that can be largely mitigated.*

Keywords: *Cloud accounting, Cloud computing*
JEL Classification: *M15, M41*

1. Introduction

More and more companies are now considering cloud technology a crucial pillar of their digital transformation, its implementation allowing for business to run safely and more efficiently.

Cloud computing is a distributed system providing computing services, applications, data access and storage, without the user needing to worry about the location and physical configuration of the systems that provide these services.

Companies can rent access to anything from applications to storage from a cloud service provider (CSP). The customer can use CSP services to access and process data from wherever there is internet access, via any kind of terminal, desktop, laptop, tablet, smartphone, etc.

Amid fierce competition among companies, these benefits may just be the key to a successful business.

Cloud computing offers customers more agility, scalability and flexibility. Instead of spending money and resources on outdated IT systems, customers can focus on more strategic activities. Without a large investment in advance, companies can quickly access the computing resources they need, only paying for what they need to use.

Modern cloud solutions help companies face the challenges of the digital era. Instead of managing their IT department, organisations can swiftly address more complex business challenges.

Cloud customers automatically benefit from the newest innovations and emerging technologies integrated by the cloud service provider, including from the use of cutting-edge technologies such as artificial intelligence (AI), chat robots, blockchain and Internet of Things (IoT).

Cloud computing models

There are different Cloud Computing Deployment models (Mell&Grance, 2011):

- ***Public cloud***, in which the entire computing infrastructure is located at the headquarters of the cloud provider, and the customer can access the services via the internet. The customer no longer has to maintain its own IT department and can quickly add more users or computing power, as necessary. The cloud provider hosts several entities that share its IT infrastructure.

The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organisation, or some combination of them.

- ***Community cloud***. "The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy and compliance considerations)". It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.

- ***Private cloud***, used exclusively by a single organisation, which can be hosted at its headquarters or at the cloud provider's data center. A private cloud offers the highest level of security and control.

- ***Hybrid cloud***, which is a combination of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability. In general, the customer hosts the applications essential to the business on its own servers, for higher security and control, while its secondary applications are stored at the cloud provider's location.

The basic cloud computing services are structured into three main categories:

a) ***Infrastructure-as-a-service (IaaS)*** provides internet-based access to storage and computing power, via a public connection, usually the internet.

The computing resource is provided via a subscription and consists in virtualized hardware - or in other words, computing infrastructure.

Tangibly, the set of hardware resources comes from a multitude of servers and networks, usually distributed across numerous data centers, under the management of the cloud provider,

The customer has access to virtualized components in order to create efficient IT solutions that are easily scalable, with management and hardware expenses being outsourced to the cloud service provider.

Infrastructure-as-a-service (IaaS**)** allows customers to access on-demand infrastructure services via the internet. The fundamental benefit is that the cloud provider hosts the infrastructure components, which provide computing, storage and network capabilities, so that subscribers can run their workflow in the cloud. The cloud subscriber is normally responsible for the installing, configuring, securing and maintaining any software in the cloud infrastructure, such as the database, middleware and application software.

For example, companies can use *IaaS* for:

- **Cloud hosting**; hosting websites on virtual servers which are distributed to resources collected from subjacent physical servers. A website hosted on the cloud benefits from the redundancy of a vast network of physical servers and on-demand scalability so as to cope with unexpected requests.
- **Virtual data centres (VDCs)**; a virtualized network of interconnected servers that can be used to provide increased cloud hosting capabilities, IT infrastructure for companies, or to integrate all these functionalities in a private or public cloud.
- **Enterprise infrastructure**; internal IT business networks, such as a private cloud or local virtual networks that use server and centralised

network resources, and can store data and run the applications needed on a day to day basis. Business can be easily expanded by scaling the infrastructure in accordance with rising demands, and private cloud solutions (accessible only in the internal network) can protect the storage and transfer of the company's sensitive data.

b). ***Platform-as-a-service (PaaS)*** is a cloud computing category that offers users a platform and an environment for developing and operating web or mobile applications.

The provider hosts the infrastructure components and middleware, and the client can access these services via a web browser.

PaaS may come with preconfigured features to which customers can subscribe, choosing to use those that meet their requirements and opting out of those they do not need.

Consequently, packages may vary from offering simple point-and-click services which do not require too much experience, to providing infrastructure options for advanced development.

The infrastructure and applications are managed for the customers and there is a technical support service available. Services are updated constantly, upgrading the existing features and including additional features.

PaaS providers can assist developers via an automated mechanism throughout the entire process of developing, testing and implementing original applications.

PaaS services are subscription-based, and customers ultimately pay only for what they use.

In order to boost productivity, Oracle's PaaS solutions offer ready-to-use programming components, which allow developers to create new functionalities in their applications, including such innovative technologies as artificial intelligence (AI), chat robots, block chain and Internet of Things (IoT). These also include solutions for analysts, end users and professional IT administrators, *inter alia* Big Data analyses, content management, database management, and system and security management.

c) Software-as-a-Service (SaaS) is a software provision model in which CPS hosts the customer's applications at its location. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g. web-based email), or a program interface. Instead of paying for the maintenance of its own computing infrastructure, the customer subscribes to the service, paying as it uses it.

Many companies find SaaS to be the perfect solution, as it allows them to quickly become functional, using the most innovative technology available. Automatic updates reduce the burden on internal resources. Customers can scale services to support a fluctuating workload, adding several services or features, as they develop more and more.

A modern cloud suite can include and connect everything from financial services, human resources, acquisitions and supply chains, to solutions for trade, marketing, sales and services.

In response to the challenges of the business environment, a modern SaaS suite can promote modernisation in the entire business by supporting fast innovation, offering superior customer experiences, and facilitating better business decisions with the help of integrated analysis capabilities and a comprehensive view of the business.

Nevertheless, some companies may not agree to use the same SaaS applications as their rivals if they are focused on the need to maintain a competitive advantage and the security of sensitive data.

Companies may opt to use several cloud computing and storage devices in a single architecture. The customer can have a combination of software as a service (SaaS), platform as a service (PaaS) and infrastructure as a service (IaaS).

Although cloud solutions are viewed as generally safe, companies can take additional measures to secure data, ensuring that only authorised individuals can access the system, and by implementing solutions such as VPNs that mask individual internet protocols, they can work to prevent potential cybersecurity issues.

2. Cloud accounting

Traditional accounting software is installed locally, on the company’s hardware. Normally, to use these applications, a licence must be purchased and maintenance (upgrades, troubleshooting, back-up, etc.) must be provided either by their own staff or by the provider (for a fee).

A cloud accounting application is an accounting software that can be accessed from anywhere with an internet connection, without needing to be installed and managed on own servers, and all the data is safely stored on cloud servers. Using all the benefits of cloud technology, cloud accounting software is a real solution for increasing a company’s efficiency and competitiveness. All tasks related to accounting, invoicing, sales and planning can be performed via SaaS.

Cloud applications have gradually gained ground to the detriment of locally operated applications. There are numerous advantages of cloud technology which can no longer be overlooked, especially by small- and medium-sized companies.

2.1. Benefits of Cloud Accounting

Compared to software applications installed on individual computers, cloud accounting technology offers mobility and freedom, as data and applications can be accessed at any time and anywhere there is an internet connection.

Online data centralisation allows fast access to all authorised individuals, regardless of their location, and increases the transparency of document and data movement, as well as the control and authorisation of access to various procedures and files.

Accounting costs are significantly lowered considering that:

- The purchase of licences, servers and other IT equipment can be a very expensive investment, while choosing a cloud-based solution reduces these costs to a minimum.
- The responsibility for the optimal functioning of the applications falls solely on CSPs, thus lowering the costs for server management, update, upgrade, back-up.
- Applications are ready to use at the moment of subscription, with no initial installation costs.
- Cloud accounting services are subscription-based, the amount of fees paid depending on usage.
- Scalability is an important feature of this technology as it allows the management of a larger data volume by supplementing demand for cloud services, at minimal additional costs, thus ensuring higher flexibility, with no further investment in equipment or infrastructure.
- Real-time access to information provides an overview of the company's financial position, as well as access to detailed financial breakdowns, management information and key performance indicator (KPI) metrics.
- The software updates happen automatically as soon as they are available and most of the time they are free for the existing customers.
- Automatic backups are created in order to ensure uninterrupted access to data through recovery in case of accidental data destruction or natural disaster.

- Cloud computing applications can be accessed from various devices connected to the internet, such as laptops, smartphones and tablets.
- In some situations, applications can be customised to better answer customer needs.
- Most cloud accounting service providers offer customer service and technical support, which are very useful for less experienced users, and also ensure higher protection.
- Encryption of data that is to be stored in the cloud provides increased security, in the event of unauthorised access. There are different types of encryption and different standards of safety which can be adopted depending on the nature of the data circulated and the wishes of the cloud service user. An 128-bit SSL (Secure Sockets Layer) encryption can be used for accounting software.

Companies that offer cloud services have strict rules and procedures in place for data security.

2.2. Risks of cloud accounting

Using cloud accounting services also entails a series of risks that may be lower or greater_depending on the size and structure of the company, its internal data security and, last but not least, the CSP chosen.

Main risks of transitioning to cloud accounting:

- **Connectivity risks**

Cloud services' advantage of being accessible any time and from anywhere disappears when the internet connection is not available, unstable, or low speed. In order to reduce this risk, redundant internet connections (e.g. mobile data backup) may be chosen.

The compromising of the APIs (application programming interfaces) used by the customer in managing and interacting with cloud services can pose a significant risk. These application programming interfaces can have a series of software vulnerabilities that can be additionally exploited, given that they are accessible via the internet.Once discovered, these vulnerabilities can turn into attacks on organisation cloud assets or even on other CSP customers.

A **Denial-of-Service (DoS) attack** is an attack aimed at denying legitimate users access to a computer or network. DoS attacks accomplish this by flooding the target with traffic, or sending it information that triggers a crash.

A DDoS (Distributed DoS) attack uses several computers to launch a coordinated DoS attack on one or more targets. Using client/server technology, the attacker can increase the efficiency of the DoS attack by capitalising on the resources of several accomplice computers against their will, using them as attack platforms (Stein, L.D., Stewart, J.N., 2002).

In 2020 H1, there have been 4.83 million DDos attacks at online platforms and services, while the largest monthly number of attacks happened in May, with more than 929,000 DDoS attacks. However, DDoS attack frequency jumped 25% during peak pandemic lockdown months - March through June. (Help net security, 2020).

- **Reduced control and visibility of cloud data**

The loss of data stored in the cloud can occur not only following malicious attacks, but also as a result of a natural disaster, of the customer losing the encryption key used to encrypt the data before uploading it, or of the CSP accidentally deleting the data.

The customer's lack of visibility on how data is stored on different storage devices within the CSP's infrastructure makes it difficult to check the safe deletion of its data. Specifically, data can be incompletely deleted, remaining on various storage devices of the provider and may eventually be available to attackers.

Given the risk of data loss, a series of measures should be considered to ensure data recovery.

- **Security breaches**

Cloud data is accessed through accounts created and managed differently, depending on the service provider. Unauthorised data access is more frequent via password theft. The attacker can gain access not only to the company's data, but also to that of other companies using the same CSP.

Access passwords to cloud systems are most often the weakest points. Data can be accessed on any device connected to the internet, thus strong, unique passwords are necessary so as not to be vulnerable to an attack.

E-mail security is as important given that, in a lot of cases, this is the key password reset mechanism for cloud apps.

- **Insiders abuse authorised access**

One of the most serious threats to an organisation is an insider threat. Insiders, such as staff and administrators for both organisations and CSPs, who abuse their authorised access to the organisation's or CSP's networks, systems, and data are uniquely positioned to cause damage or exfiltrate information.

This threat may involve fraud, theft of confidential or valuable commercial information, theft of intellectual property, or sabotage of IT systems. Threats can come from: ill-intentioned individuals that take advantage of their access to information to damage an organisation, negligent individuals, namely people who make errors and fail to consider security policies, endangering their organisations, and infiltrated individuals, who are external actors that obtain legal access credentials without authorisation.

Over the last two years, there's been a 47% increase in the frequency of incidents involving insider threats. This includes malicious data exfiltration and accidental data loss.

Incidents involving stolen credentials causing the most financial damage. Insiders abusing authorised access can be very expensive, may lead to incidents that expose various customers and are harder to prevent than external attacks. Insider threats are invisible to traditional security solutions like firewalls and intrusion detection systems.

As per a recent survey (Trzeciak, R.F, 2017), 27% of the total cyber crime incidents were supposed to be conducted by insiders, and 30% of respondents specified that the destruction caused by insiders was more severe than the loss caused by external attackers or malicious intent or financial gain.

- **Vendor Lock-In or portability issues to another CSP**.

The risk of bankruptcy of the cloud service provider should also be analysed, and the necessary measures to prevent data loss should be taken.

Changing the cloud service provider can be difficult and involves costs and time, considering the non-standard data formats, non-standard APIs, and reliance on one CSP's proprietary tools and unique APIs.

Each CSP wants to maintain its customers and develops functions and services to set it apart from its competition. Every company must establish if and to what extent it wishes to depend on a sole provider and on the facilities it offers, or if it desires high portability. Using cloud-native applications based on containers and microservices ensures portability between clouds, but does not allow access to all the facilities they offer.

In order to avoid being locked-in to a single CSP and to have more benefits and new services, large companies adopt a multi cloud strategy.

- **A failure to maintain separation among tenants** that use the same infrastructure or applications of the CSP can be used by an attacker to gain access from one organisation's resource to another user's or organisation's assets or data. To reduce this risk, sensitive data can be stored by the CSP on separate physical hardware from other customers, setting up a private cloud or using an API to keep their data onsite while still using the cloud-based application.

- **Increased complexity strains into IT operations.**

Introducing cloud services increases the complexity of IT operations, as it is necessary to have skilled IT staff to ensure the migration of assets and data to the cloud in addition to their current responsibilities for on-premises IT.

If the company's staff uses additional cloud services, unauthorised by the organisation's IT department, it may lead to an increase in malware infections or data exfiltration.

Not knowing the security measures used by the CSP and the responsibility to also ensure own security measures heightens cybersecurity risk.

3. Conclusions

The benefits of cloud services are undeniable, regardless of the size of the organisation and business activity, and are capitalised on by more and more companies in spite of the possible risks involved in using these new IT technologies.

Transitioning to cloud computing entails major changes not only to companies' structure and operation, but also to the mentality and work culture of the managers and the entire staff.

A cloud accounting provider must be chosen after a thorough review of the offers on the market so as to select the best solution for the specific activity and the company's digital architecture, as well as to minimise the risks surrounding this transition.

Integrating cloud computing technology in a company involves the design of a solid digital architecture to integrate, along with cloud based accounting, other cloud services necessary for increasing productivity, improving communication, and boosting innovation.

For small and medium-sized enterprises with underdeveloped IT systems, cloud services can improve their security, and in the case of large companies, the control of cloud services may require additional data security solutions.

Data security risks increase as companies access cloud computing services via devices that are not sufficiently protected or show software vulnerabilities (often run software which can be exploited such as Office, Outlook, Internet Explorer, Flash and Acrobat Reader), which can be taken advantage of by intruders.

References

Attaran, M., (2017). Cloud Computing Technology: Leveraging the Power of The Internet to Improve Business Performance. *Journal of International Technology and Information Management,* 26, 112-137.

Help net security, (2020). *4.83 million DDoS attacks took place in the first half of 2020, a 15% increase. A*vailable at https://www.helpnetsecurity.com/2020/09/30/4-83-million-ddos-attacks-first-half-of-2020/.

Ionescu, B.S., Prichici, C., Tudoran, L., (2014). Cloud Accounting – A Technology that may Change the Accounting Profession in Romania. *Audit Financiar,* no.2/2014.

Marston, Sean & Li, Zhi & Bandyopadhyay, Subhajyoti & Zhang, Julie & Ghalsasi, Anand., (2011). Cloud computing – The business perspective. *Decision Support Systems* 51, pp.176-189. 10.2139/ssrn.1413545.

Mell, P. and Grance, T., (2011). *The NIST Definition of Cloud Computing.* Gaithersburg*:* NIST Special Publication 800-145. Available at http://faculty.winthrop.edu/domanm/csci411/Handouts/NIST.pdf.

Rosenthal, M., (2020). Insider Threat Statistics You Should Know: Updated 2020, *Tessian*. Available at https://www.tessian.com/blog/insider-threat-statistics/.

Saxena, N., Hayes, E., Bertino, E., Ojo, P., Choo, K.-K.R.. Burnap, P., (2020). Impact and Key Challenges of Insider Threats on Organizations and Critical Businesses. *Electronics,* 2020, *9*, 1460. Available online: https://www.mdpi.com/2079-9292/9/9/1460/pdf.

Stein, L.D., Stewart, J.N., (2002). The World Wide WebSecurity FAQ. Available at http://www.w3.org/Security/Faq/.

Trzeciak, R.F., (2017). SEI Cyber Minute: Insider Threats. Available at: http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=496626.