Quarterly Newsletter

CHAIR

iDANAE

INTELLIGENCE · DATA · ANALYSIS · STRATEGY

2Q21

Cloud outsourcing risk management

POLITÉCNICA

UNIVERSIDAD POLITÉCNICA DE MADRID

ManagementSolutions
Making things happen

Introduction

The evolution of computing processes in companies and institutions can be summarized by the occurrence of phases of centralization of data and processes, followed by phases of decentralization. This generates a transformation of organizations with a certain cyclical character. These phases are conditioned by the creation and development of new technologies. In this sense, *cloud computing* can be understood within a centralization phase, where a cloud model is used instead of the traditional *on premise* model. However, this model could be altered: the emergence of 5G and IoT might imply a new decentralization of data and processes. This would require the need to develop a management called HDIM (Hybrid Digital Infrastructure Management), which would make it necessary to think about the so-called *proximity* data centers, or the federation of these centers.

In any case, more and more organizations currently depend on external service providers to run their operations. This has made it essential to analyze and control the risks associated with outsourcing services to third parties. This process is commonly referred to as third-party risk management.

The financial industry has traditionally addressed this type of risk, in part due to industry regulations (e.g., regulations in the US issued by the OCC[1] and the Federal Reserve[2], published in 2013). However, with the rise of digital transformation, and more specifically, of cloud computing, reliance on third parties has increased markedly across industries. According to a Forrester® Research study[3], 1 in 3 respondents reported working with more third-party vendors than two years ago.

In addition, outsourcing services to the cloud has particular characteristics that distinguish it from traditional outsourcing arrangements. Therefore, this newsletter aims to focus on the risk management of outsourcing services to the cloud, providing an overview of this technology and third-party risk management. Consequently, this newsletter addresses the benefits of cloud computing technology and then analyzes the associated risks, focusing on those related to the company's organizational strategy and information security.

[1]OCC, 2013.
[2]Fed, 2013.
[3]Forrester, 2020.

What is Cloud Computing?

Cloud computing is a computing model that enables on-demand remote access to a multitude of resources and services provided by a vendor, through the use of the Internet[4]. These resources can be both hardware and software, and are offered to customers on demand. In other words, the cloud is the resource to use if any type of technology is required, without the need to install any program or application locally, allowing the customer to disengage from the technological infrastructure necessary to meet their particular needs. Thus, this computing model arises in contrast to the concept of on-premise or traditional architecture, under which companies are the owners of all the elements (data centers, storage systems, etc.) and manage them in their own facilities, which tends to be result in a higher cost.

In contrast, cloud services allow, among others, to reduce the costs associated with hardware resources, improve the security levels of the solutions offered, facilitate access to them when and where required, and condense the management of all computing at the same level[5]. In addition, cloud computing allows access to resources at an international level, being multi-location one of the differential aspects of this model when compared to classic service providers. This fact makes it possible for small companies and startups to become more competitive, so that they can compete with other companies of larger size and capitalization. This is known as democratization of access to resources.

In 1999, Salesforce made applications available to its customers via a website, which would lay the foundation for the cloud revolution of the last two decades. Three years later, Amazon launched the first public cloud computing service, AWS, and Google and Microsoft joined in 2009. Since then, the range of possibilities has been growing, and more and more companies are offering solutions of this type to their customers: Oracle, IBM, HP, etc. In turn, this increase in providers has been accompanied by a continuous increase in the use of cloud services by companies over the last few years, which has been reflected in a constant growth of the global cloud computing market and does not seem to cease in the short and medium-term[6]. In this context, three cloud service providers currently stand out, both in terms of market share and services provided: AWS[7], Microsoft Azure[8], and Google Cloud[9], jointly representing 60% of the global market.

[4]INCIBE, 2017.
[5]Salesforce, 2017.
[6]According to the latest Gartner study (Gartner, 2021), worldwide spending on public cloud services is estimated to grow by 23.1% in 2021, reaching $332.3 billion.
[7]The largest cloud-computing provider with a 33% market share.
[8]The second largest cloud-computing provider with a market share of 18%.
[9]The third largest cloud-computing provider with a market share of 9%.

"The cloud provides services to companies of all sizes. The cloud is for everyone. The cloud is democracy."

Marc Benioff | Chief Executive Officer, Salesforce

Characteristics of Cloud Computing

The multiplatform nature of cloud services makes it possible to take advantage of all the benefits that this form of computing can offer by simply having a device with Internet access. In addition to this, the main characteristics[10], that differentiate this way of working from other traditional frameworks are the following:

- **On demand.** The services are 100% adapted to the particular needs of each client. These needs refer to both quantity and timing, being always available for any purpose required.
- **Measured service.** The activity is collected in a precise way to control and monitor at all times the use that is being made of the services provided. This is essential when controlling the associated costs per use, which will be given by the number and type of resources used: pay-as-you-go.
- **Fast flexibility.** The services offered have a high scalability according to the resources required by each client and in each situation.
- **Pooled resources.** Resources are allocated and reallocated according to customer demand. The consumer can disregard the location of the resources provided, achieving a high level of abstraction. In addition, this arrangement of resources in multiple locations favors fault and error tolerance.

Types of Cloud services

- **SaaS – Software as a Service.** A software application is made available to the client through a web server, saving him the task of updating or maintaining the application. E-mail services, videoconferencing applications, or data exchange services are some examples of this Cloud model. It has become one of the preferred options in the recent technological transformation carried out by many companies today.
- **PaaS – Platform as a Service.** It provides all the necessary resources to build a specific application, adapting to its specific requirements. There are multiple benefits of this service, as it allows a considerable reduction in the infrastructure costs of customers or facilitates the scalability of companies according to the demand for their products.
- **IaaS – Infrastructure as a Service.** It provides the hardware required to launch the applications created with the above services. Among the resources included, there are data storage and networking services, allowing customers to use these hardware assets without the need to purchase and manage them[11].

Types of Cloud

- **Public cloud.** These clouds allow simultaneous access by multiple clients through the Internet, regulating their access usually through control mechanisms, which guarantees the security and integrity of the information involved.
- **Private cloud.** Unlike the previous case, this cloud is unique to a particular organization, so no public access points are allowed.
- **Hybrid cloud.** Combination of the two previous ones, allowing the exchange and movement of information between public and private points, depending on the importance of the data or the associated services.
- **Community cloud.** Companies with common interests share a set of services and responsibilities, motivated by achieving a common end goal.

[10]Hernandez, N.L. and Florez-Fuentes, A.S., 2014; Shaw, S.B. and Singh, A.K., 2014.
[111]Gartner, 2017.

Benefits

The popularity of cloud computing has been increasing in recent years thanks to the growing advantages it offers over traditional forms of work. The following are some of the benefits[12] that have encouraged the move from traditional infrastructures to the cloud environment in a multitude of companies of different sizes and industries[13].

- **Access to new technologies.** New value-added products and services, or new technologies can be made available to companies as they emerge (e.g., in the field of Artificial Intelligence), as well as innovation in new hardware (e.g., advances that improve computing capabilities). By doing so, the company can limit its initial investment in innovative technology and, in turn, reduce the time-to-market for its acquisition and implementation.

- **Scalability.** The possibility of accessing certain resources according to the level of use in each specific situation facilitates the task of progressively adapting to the storage or processing requirements, depending on the customer's product demand. It increases the efficiency of companies, since they only invest in what is necessary at any point in time. In addition, a level playing field is created for smaller companies, so that they can compete with products from large companies.

- **Security.** Organizations less developed in security can benefit from the environment offered by the cloud service provider.

- **Mobility.** The mobility of cloud computing offers the possibility of working anytime, anywhere and on any device, as long as you have an Internet connection.

- **Insight**. Many cloud service providers provide services that allow analyzing stored data, giving a panoramic view of the entirety of your data (which was previously inaccessible).

- **Increased collaboration.** Thanks to cloud computing, collaboration becomes simpler, sharing information easily and securely, offering automatic synchronization of stored[14] files and eliminating the need to send files.

- **Disaster recovery.** Although disasters cannot be prevented or anticipated, cloud computing makes it possible to accelerate data recovery in many types of emergency scenarios.

- **Loss prevention.** With cloud computing, stored information remains secure and accessible from any computer, eliminating the risks of data loss inherent in local storage.

- **Automatic software updates.** Cloud service providers take care of the maintenance of the servers, carrying out all the necessary updates[15].

- **Competitive advantage.** Cloud computing provides a competitive advantage to the company through multiple ways: providing the most innovative technology possible, becoming a more agile company, focusing on projects by transferring the responsibility of managing the infrastructure, among others.

- **Sustainability.** The use of cloud services results in a lower carbon footprint, making this technology more environmentally friendly.

Because of these advantages, it is expected that more and more customers will join this way of working in the coming years and that the technological change that this entails will be increasingly reflected more noticeably.

"You don't generate your own power. Why would you generate your own computing?"

Jeff Bezos | CEO and founder of Amazon

[12]The first three can be considered the main advantages offered by cloud computing.
[13]Salesforce, 2016.
[14]Allowing for the maintenance of the coherence of data.
[15]Both software and security.

Risks

In contrast to the benefits described in the previous section, cloud computing poses certain risks that must be identified and managed to outsource services to the cloud correctly.

Risks arising from the use of cloud services vary depending on the service model and the deployment model[16]. However, in general terms, it is possible to differentiate between traditional risks related to outsourcing services and new risks that have appeared with the emergence of this paradigm.

The following are some of the main risks to be taken into account[17], based on various proposed categorizations[18] and current regulations[19].

Organizational risks

These include those risks that affect the organizational strategy of the company, which may lead to non-compliance with the objectives set by the company[20]:

- **Lock-in.** Currently, the portability of services, applications and data between cloud service providers is low, so a customer outsourcing services to a cloud provider may experience serious difficulties if the need arises to migrate the service to another provider or even to an in-house environment.
- **Loss of governance.** By using services, the customer transfers the control of the infrastructure to the cloud provider, as well as of various security-related issues. As a result, the customer's organizational strategy could be affected.
- **Supply chain failure.** A cloud service provider may outsource services to third parties, creating a chain of dependencies that may result in cascading failures.
- **Less control of costs.** The costs associated with the platform, both those related to hardware and products, depend on the pricing of the service provider, as well as the use that the organization makes of them, thus adding uncertainty to cost control, which requires an additional layer of analysis and a prior estimation.

Information security risks

These include vulnerabilities related to unauthorized access, use, disclosure, interruption, modification, or destruction of information and/or information systems[21]. These vulnerabilities are concentrated around four key concepts:

- **Confidentiality.** It refers to unauthorized or improper access to data. When outsourcing services to the cloud, the confidentiality of data can be compromised by accessing them through an Internet connection, which increases exposure to attacks. In addition, failures or errors in shared environments could result in one tenant gaining access to another tenant's resources.
- **Integrity.** It refers to unauthorized modifications and deletions by users. It must be ensured that only authorized users can alter stored information.

  In this line, there is also the risk associated with inefficient data deletion since, given the reduced visibility by clients of the physical location of the data, the client's information may not be deleted in its entirety from the service provider's servers.
- **Availability.** Users must be able to access data whenever and wherever they want, i.e. providers must provide a connection without interruptions or disconnections.

  The location of data has become very important, as the usual lack of knowledge about location makes it difficult to control data storage[22].
- **Authentication.** Outsourcing services to the cloud can amplify the challenge around user authentication, which is a

[16] For example, the same risks are not assumed if a PaaS (Platform as a Service) and SaaS (Software as a Service) service model is used.
[17] Lista no exhaustiva.
[18] Raval, V., 2010, ENISA, 2009 y Shayan, J., Azarnik, A., Chuprat, S., Karamizadeh, S. and Alizadeh, M., 2014.

[19] EBA, 2019, EIOPA, 2020 y ESMA, 2020.
[20] ENISA, 2009.
[21] NIST, 2012.
[22] This acquired importance has been reaffirmed by the publication of regulations on data localization, limiting in several jurisdictions the countries in which data can be stored.

highly related aspect of data integrity.

Thus, in terms of information security, the contracting company must pay special attention to the security measures integrated into the contracted cloud platform.

Management APIs compromise

It refers to possible deficiencies in the APIs provided to the client by the cloud providers to manage and interact with the information systems. These deficiencies in the APIs will lead to a partial loss of services, affecting the availability of the services.

Operational risk

In general terms, operational risk refers to the risk of loss due to the failure of internal processes, people, and systems or external events. The migration of services to the cloud will lead to an increase in operational risk[23], which will have to go alongside the training of professionals in the use of these services to avoid failures because of changes in the company's operations. On the other hand, other operational risks may be the lack of personalized services[24] or less control over both the quality of services and the availability of applications.

Compliance and legal risks

When outsourcing a service, it is necessary to ensure compliance with all legal and regulatory requirements in force. Its non-compliance could result in heavy sanctions and could have a significant impact on the company's reputation. This task can be challenging due to the multiple jurisdictions in which cloud service providers operate and the non-homogeneity of regulatory requirements between different countries. More specifically, these legal issues often arise around data privacy, data ownership, copyrights, data localization, contractual issues, etc.[25, 26].

Reputational risk

It can be defined as the current or future risk to the institution's income, equity or liquidity resulting from damage to its reputation[27]. In this line, customer dissatisfaction, as well as security failures or regulatory violations resulting from the outsourcing of services can significantly damage the reputation of the entity. In addition, any negative public opinion of the cloud service provider can pose a reputational risk for the company.

Business continuity

Outsourcing a service to a third party creates a dependency on the provider's business continuity. In other words, business continuity is partially delegated to the provider. Thus, if the cloud service provider were to suffer an attack, this would also directly affect the contracting organization.

Concentration risk

It arises from over-dependence on a cloud service provider,

[23] Operational risk exposure will be highly influenced by the deployment model.
[24] Not fully suited to the needs of the contracting company.
[25] Moriggi, A., 2018.
[26] For example, in the area of personal data privacy, compliance with the European General Data Protection Regulation (GDPR) should be noted.
[27] EBA, 2018.
[28] Microsoft, 2020.

Cloud outsourcing risk management

As explained in the previous section, the use of cloud services is associated with a series of risks and threats that must be taken into consideration. Therefore, the identification and management of these risks become a key factor to carry out a correct outsourcing of cloud services and obtain the benefits[29] that this delegation of services offers.

Thus, it is possible[30] for the customer to transfer certain risks to the cloud service provider, although not all risks can be transferred. Additionally, it should be taken into account that in these cases the responsibility will be outsourced, but not the accountability obligation[31].

In this sense, several regulators have recently published regulations regarding the management of outsourcing cloud services, with the aim of helping regulated entities to adopt cloud-based solutions.

At the European level, EBA, ESMA and EIOPA have published a series of guidelines[32] that aim to help regulated entities identify, control and address the risks arising from cloud outsourcing contracts, highlighting their alignment.

Consequently, although these guidelines only apply directly to regulated entities, they can be considered as a set of best practices for the proper management of cloud outsourcing. In this way, taking the different guidelines as a reference, the general guides are summarized below.

Governance

Entities must have a defined and updated cloud outsourcing strategy that is consistent with the rest of the entity's strategies and with its internal policies and processes.

Consequently, the entity should have a clear assignment of roles and responsibilities for the management and control of this type of arrangement, ensuring that sufficient resources are being allocated[33].

In addition, entities must maintain an up-to-date record of all cloud outsourcing arrangements.

[29] For more information, see Section 3.
[30] And even recommended in some cases.
[31] ENISA, 2009.
[32] EBA, 2019, EIOPA, 2020 y ESMA, 2021.
[33] Among these functions, it should be noted that the entity must supervise the performance of the service provider.

Risk assessment

Before carrying out the outsourcing of a service to the cloud, a prior analysis must be carried out in which:

- it is assessed whether the functions to be outsourced are critical;
- all relevant risks are identified and evaluated;
- a due diligence of the cloud service provider is carried out
- potential conflicts of interest are identified and evaluated.

As would be expected, the scope of this analysis will depend on the criticality of the function to be analyzed. In addition, if there are changes in the contracted services or in the status of the service provider, these analyses should be performed again.

Contractual terms

Cloud outsourcing agreements should set out in writing the rights and obligations of both parties, and should reflect the possibility for the contracting company to terminate the contract at any time. In addition, the different guidelines specify a series of minimum terms that must be included in cloud outsourcing contracts (start and end date, financial obligations, agreed service levels, etc.).

Information security

As explained in the previous section, information security is one of the main risks in cloud services. Therefore, a series of information security requirements must be established in the company's internal policies and procedures, as well as in the outsourcing contract[34].

The ESMA guidelines are the most detailed in this aspect and specify that in case of critical functions, requirements related to the entity and access management, encryption and key management, network security, integration with APIs, or data location, among others, must be included.

Exit strategy

Contracting entities must ensure that they can exit from cloud outsourcing arrangements without interrupting their activities and services, and without prejudice to compliance with their obligations. To this end, entities should develop exit plans, identify alternative solutions and develop migration plans to remove the outsourced service.

Access and audit rights

Service outsourcing agreements must allow the effective exercise access and audit rights over the service provider or, if this is not possible, agree on alternatives that achieve a similar result[35].

Finally, for regulated entities, competent authorities should assess the risks derived from cloud outsourcing contracts as part of their supervisory process. More specifically, they should assess whether: (1) they have the necessary governance, resources, and operational processes in place to carry out cloud outsourcing arrangements, (2) they identify and manage the relevant risks arising from such arrangements, and (3) they monitor the evolution of concentration risk.

[34]These requirements will be proportional to the criticality of the outsourced function.
[35]In this line, third party certifications or external or internal audit reports could be used.

Conclusions

In recent years, cloud computing has revolutionized the landscape of new technologies and the business world, with many enterprises and companies of all sizes and sectors moving from traditional infrastructures to the cloud environment.

This paradigm shift has been boosted by the numerous advantages of using this type of service (cost reduction, scalability, security, etc.) and, consequently, has led to a marked increase in companies' dependence on third parties.

In this way, third-party risk management highlights the importance of identifying and managing the associated risks to carry out correct outsourcing of cloud services, differentiating between traditional risks related to outsourcing services and new risks associated with this technology.

Authors

Ernestina Menasalvas (UPM)
Alejandro Rodríguez (UPM)
Manuel Ángel Guzmán (Management Solutions)
Segismundo Jiménez (Management Solutions)
Silvia Duque (Management Solutions)

Bibliography

Basel Committee on Banking Supervision (BCBS), 2003. Basel II: The New Basel Capital Accord.

Carroll, M., Van Der Merwe, A. and Kotze, P., 2011. Secure cloud computing: Benefits, risks and controls. In 2011 Information Security for South Africa (pp. 1-9). IEEE.

European Banking Authority (EBA), 2018. EBA/GL/2014/13. Guidelines on common procedures and methodologies for the supervisory review and evaluation process (SREP) and supervisory stress testing.

European Banking Authority (EBA), 2019. Guidelines on outsourcing arrangements.

European Insurance and Occupational Pensions Authority (EIOPA), 2020. Guidelines on outsourcing to cloud service providers.

European Securities and Markets Authority (ESMA), 2021. Guidelines on outsourcing to cloud service providers.

European Union Agency for Cybersecurity (ENISA), 2009. Cloud Computing Risk Assessment.

Federal Reserve (Fed), 2013. Guidance on Managing Outsourcing Risk.

Fitó, J.O. and Guitart Fernández, J., 2010. Introducing risk management into cloud computing.

Forrester, 2020. Rethink Third-Party Risk Management To Promote Innovation Without Sacrificing Customer Trust. Disponible en: https://www.rsa.com/en-us/offers/forrester-rethink-third-party-risk-management

Gartner, 2017. Gartner Says Worldwide Public Cloud Services Market to Grow 18 Percent in 2017. Disponible en: https://www.gartner.com/en/newsroom/press-releases/2017-02-22-gartner-says-worldwide-public-cloud-services-market-to-grow-18-percent-in-2017

Gartner, 2021. Gartner Forecasts Worldwide Public Cloud End-User Spending to Grow 23% in 2021. Disponible en: https://www.gartner.com/en/newsroom/press-releases/2021-04-21-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-grow-23-percent-in-2021

Hernandez, N.L. and Florez-Fuentes, A.S., 2014. Computación en la nube. Mundo Fesc, 4(8), pp.46-51.

Instituto Nacional de Ciberseguridad (INCIBE), 2017. Cloud Computing.

Microsoft, 2020. Concentration Risk: Perspectives from Microsoft.

Moriggi, A., 2018. Legal risks of cloud services.

National Institute of Standards and Technology (NIST), 2012. Guide for Conducting Risk Assessments.

Office of the Comptroller of the Currency (OCC), 2013. Third-Party Relationships: Risk Management Guidance. Disponible en: https://www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html

Raval, V., 2010. Risk landscape of cloud computing. ISACA Journal, 1, p.26.

Salesforce, 2016. 12 Benefits of Cloud Computing.

Salesforce, 2017. ¿Qué es Cloud Computing? Disponible en: https://www.salesforce.com/mx/cloud-computing

Shaw, S.B. and Singh, A.K., 2014. A survey on cloud computing. In 2014 International Conference on Green Computing Communication and Electrical Engineering (ICGCCEE) (pp. 1-6). IEEE.

Shayan, J., Azarnik, A., Chuprat, S., Karamizadeh, S. and Alizadeh, M., 2014. Identifying Benefits and risks associated with utilizing cloud computing.

UNIVERSIDAD POLITÉCNICA DE MADRID

The Universidad Politécnica de Madrid is a public-law organization of a multisectoral and multidisciplinary nature that is engaged in teaching, research, as well as science and technology development activities.

www.upm.es

Management Solutions is an international consulting firm whose core mission is to deliver business, risk, financial, organizational and process-related advisory services, with operations in more than 40 countries and a multidisciplinary team of 2,500 professionals working for over 1,000 clients worldwide.

www.managementsolutions.com

For more information, visit

blogs.upm.es/catedra-idanae/