Related Work: Framework for Evaluating Internal Controls in a Cloud Computing

Vinícius Batista Peçanha[1], Tiago Bittencourt Nazaré[2], Raissa Batista Peçanha[3]
[1]*Student ofInformation Systems, Faculdades Unificadas de Cataguases-DOCTUM*
[2]*Master in Engineering systems management, Universidade Católica de Petrópolis-UCP*
[3]*Bachelor degreeofLanguages, Universidade Federal de Juiz de Fora – UFJF Cataguases/MG, Brazil*

Abstract

Cloud Computing has emerged as a way to save resources by sharing structures in distributed systems. This has improved flexibility and provided on-demand services. This article aims to demonstrate the scenario after the deployment of the cloud environment, focusing on existing functionalities, possible security problems that may be encountered, possible problems when SLAs are celebrated, as well as a range of cryptographic algorithms that can be worked by the provider. With the use of this framework, internal controls were deployed in cloud environments. Case studies and vulnerability analysis were performed to verify security, allowing important results to be obtained, such as: making possible the choice of Amazon AWS and services that have the desired control; create metrics for service monitoring; integrate controls on service contracts and oversee service level agreements.

Keywords: *Cloud Computing, Framework, Internal controls, SLA, Amazon AWS.*

I. INTRODUCTION

With the popularization of Internet access, especially with the increasing expansion of the connection through mobile devices, Cloud Computing is becoming more and more present and necessary, since there is a limitation of storage and processing capacity in these devices.

In this way, using the cloud has made it both advantageous for manufacturers, who can reduce production costs and users, who can have their data always within reach on any device and without the risk of losing everything if a problem occurs devices.

Today's companies are looking to adopt a new computing format that involves greater efficiency, lower operating costs, and multiple options to improve processes, applications, and services with poor management.

For this purpose, Cloud Computing is used, which refers to the use of memory and the storage and calculation capacity of computers and servers shared and interconnected through the Internet, following the principle of grid computing.

Its emergence represented a new paradigm in the area of computing, from the need to offer IT (Information Technology) services on demand, with payment based on usage.

This new standard has made it possible to reduce costs for companies and end users, since it does not require such a large investment in equipment and software.

Following the idea of reducing costs, providing savings with equipment acquisition and program licenses, practicality and less time to use anoperational environment, corporations now outsource various services.

In addition to the above points, companies of any size can, depending on their needs and priorities, pay off the hiring of specialized professionals, previously needed to meet small demands. Therefore, routine tasks of program management, maintenance and updating can be included in a service contract.

On contract, there is still the service level arc (SLA) that commonly represents the availability time of a service. Other benefits of this model would be elasticity, better quality of service, more effective internal resource allocation.

In the present work, we intend to implement a framework so that the relevant internal controls are evaluated so that a cloud environment is created.

Among the objectives of this research are the evaluation and analysis of cloud service structures, define and declare internal control goals, and provide subsidies to manage and monitor service contracts.

For this, this work was carried out in an exploratory way, with a qualitative approach, through the case study, and with bibliographical researches.

II. LITERATURE REVIEW

According to [1] Cloud Computing is a set of easily usable and accessible virtual features such as hardware, development platforms and services. These features can be dynamically reconfigured to fit a variable load, allowing for optimized use. This set is typically exploited through a pay-per-use model with guarantees offered by the provider through Service Level Agreements SLAs.

A. Essential features

The essential features are the advantages that Cloud Computing solutions offer transparently to the user. Fields of technology of great relevance in this convergence are Hardware, with the capacity of virtualization. Internet technologies such as Web 2.0, web services, systems management, such as

autonomic computing and automation of data center management and maintenance; in addition to distributed computing. These characteristics include:

Self-Service on Demand: According to [2], the user can unilaterally acquire computational resources, such as processing time on the server or storage on the network as needed and without requiring human interaction with the providers of each service.

Broad network access: According to [2], resources are available through the network and are accessed through mechanisms that promote the pattern used by heterogeneous platforms (cell phones, laptops, and PDAs).

Resource pooling: According to [3] resource pooling is the providers organized in a pool to serve multiple users.

Fast elasticity: According to [2], resources can be acquired quickly and elastically, in some cases automatically, if there is a need to scale with increasing demand, and released, in the retraction of this demand.

Measured Service - Cloud systems automatically control and optimize resource utilization, leveraging measurement capability at some level of abstraction appropriate to the type of service (eg, storage, processing, bandwidth, and active user accounts).

B. Services Models

In its composition, there are the three basic layers for the operation, which are the lower layer, intermediate layer and the upper layer.

The lower layer, known as Infrastructure as a Service (Iaas), is responsible for providing the infrastructure itself, the intermediary layer known as Plataform as a Service (Paas), is responsible for providing the platform where the necessary software and systems will be implemented organizations, and the top layer known as Software as a Service (Saas), is responsible for delivering the software or systems that will be used by organizations.

C. Implementation Models

Cloud computing offers four basic models for deployment. The definition of the model that best suits the particularities of each company depends on the business process, the type of information and the desired level of vision.

Public cloud: According to [4], in the public deployment model, cloud infrastructure is made available to the public and can be accessed by any user.

Private cloud: According to [5], private clouds are those built exclusively for a single user (a company, for example). Unlike a virtual private data center, the infrastructure used belongs to the user, and therefore has full control over how applications will be implemented. A private cloud is generally built on a private data center.

Community cloud or community: According to [6], the infrastructure of this model is shared by several organizations that usually have common interests, such as security requirements, policies, flexibility and / or compatibility issues.

Hybrid Cloud: According to [7], a Cloud computing framework is considered hybrid when it comes to a combination of public and private clouds. These clouds would typically be created by the company and management responsibilities would be split between the company and the public cloud provider. The hybrid cloud uses services that are in the public and private space.

D. Security & Encryption

When the subject is related to the risks associated with Cloud Computing, issues related to the privacy and security of the resident information surround it. Despite the concerns, the risk debate often ignores the importance of creating contingency plans and SLAs aimed at ensuring reliability and the certainty that business will not suffer major crashes in the event of an incident.

According to [8], the term Cryptography arose from the fusion of the Greek words "Kryptós" and "gráphein", which means "occult" and "to write", respectively. It is a set of rules that aim to encode the information in a way that only the sender and the receiver can decipher it. For this purpose several techniques are used, and over time modified and improved, among them:

Symmetric Key (or Secret Key) Encryption: According to [9], it is characterized by having a single key to encrypt and decrypt. For this reason, the sender and recipient of the message must necessarily know the key.

Asymmetric (or Public Key) Cryptography: This is a technique that uses the public key system, in which the key used to open (decrypt) a message is different from the key used to close it, and if it has a higher level of security.

According to [10], it says that it characterizes by using two distinct keys.

Digital Certificate: According to [11], with the public key system, key management has two new aspects: first, one must first locate the public key of any person with whom one wishes to communicate, and second, you can obtain a guarantee that the public key found is from that person.

III. RELATED WORKS

As soon as a software, hardware, server, or service asset is in the cloud, there needs to be a way to provide the security of the trafficked information itself.

It becomes a complicated task in public environments in which data is not controlled by its owners to keep the constant assessment of all controls inherent to the environment imported to a third party environment.

In private or community clouds there is the possibility of greater control over assets and

information, however, it should be remembered that critical or sensitive data must be restricted, according to policies or standards, between departments or organizations.

In order to obtain more confidence and consequent success in the processes of implementing an environment based on business requirements and information security, a process framework was used, which describes a set of internal controls based on [12].

In addition, based on the framework, the internal controls inherent to the environment were raised so that they can be evaluated.

The basis for creating the framework was the need to implement processes to help mitigate possible risks associated with the environment imported into the cloud.

A. Controls for Amazon AWS service level agreements

In order to meet stakeholders' needs, we analysed the internal controls raised during the framework, comparing whether Amazon's AWS service has the necessary requirements for its planning and security.

B. Amazon Web Services (AWS)

Amazon Web Services, also known as AWS, is a cloud computing services platform that forms a computing platform offered by Amazon.com.

It offers a broad set of global cloud products such as computing, storage, databases, analytics, networks, mobile devices, developer tools, management tools, IoT security and enterprise applications. These services help companies move faster, lower IT costs, and scale.

Amazon EC2: Amazon EC2 is a web service that provides secure and scalable computing power in the cloud. It was designed to facilitate web-scale computing for developers.

Amazon S3: S3 is an object store created to store and retrieve any amount of data from any location: mobile sites and applications, corporate applications, and sensor data or IoT devices. The service is designed to provide resilience of 99.999999999%.

Amazon KMS: AWMS Key Management Service (KMS) is a managed service that facilitates the creation and control of encryption keys used to encrypt data and uses validated hardware security modules to protect key security.

Signature 4: Signature version 4 is the process for adding authentication information to AWS requests.

Amazon Virtual Private Cloud (VPC): Is a commercial cloud computing service that provides users with a virtual private cloud, providing a logically isolated section.

Amazon Redshift: Is a fast and scalable data warehouse that allows you to analyse all data warehouses and data lakes data simply and economically.

C. Checking Controls

The results obtained through Amazon AWS were exposed in tables identified according to the family or control domain.

All the checks were subdivided into their respective groups, these being:

- Essential cloud features;
- Service Models;
- Implementation Models;
- Security and Encryption.

The structure used by them follows the following convention:

Control: Identifier of the control based on the listing addressed in the theoretical framework.

OK: Shows whether the control is attended or not, or is partially answered.

Remarks: It explains what Amazon AWS performs around each topic.

Table 1: Controls Check for Amazon AWS

Control	Ok	Remarks
Essential Cloud Features		
Self-Service onDemand	Yes	Maintenance details such as backup and maintenance windows are indicated on the control panel and also if minor version updates can be applied. AWS Amazon S3 service has on-demand Self-Service requirements.
Broad network access	Yes	Because users can be managed by the client, including permissions and authorizations, minimal privileges can be defined. The AWS service, Amazon S3, has broad network access requirements.
Poolingresources	Yes	Amazon has resource pooling, so transparent to the user.

Fastelasticity	Yes	The AWS service Amazon S3 has a fast elasticity. Backup and recovery procedures can be documented by the client. In addition, the client can configure autonomous and independent routines, and can provide more alternatives in the business continuity plan.
Measuredservice	Yes	Control of roles, users and identity can normally be done by the client.
	Yes	Recovery strategy on isolated instances can be retrieved to validate AWS-produced backup files. In addition, if it is in the customer's interest, copy and recovery procedures can also be performed regardless of the cloud.
	Yes	Recovery procedures can be scheduled regularly by the customer.
	Yes	Document recovery procedures can be reviewed and regularly performed by the customer.
	Yes	The service level agreement regarding availability time can be found on Amazon's website. The client can request a chargeback of 10% of the values, if the monthly availability is less than 99.95% and greater than 99%, that is, if the instances are unavailable between 21.56 minutes and 7.2 hours per month. In case of unavailability of more than 7:12, the refund will be 25%.
	Yes	Upon contractual termination, Amazon will not delete the data for 30 days, if payment is made separately. The contract can be concluded by both parties and the migration can be done by the client using the mysqldump tool. No information was found on deleting or retaining customer data on Amazon servers, after the agreement between the parties has been finalized.
Service Models		
Software as a Service (Saas)	Yes	AWS has a Saas partner program. It offers APN technology partners support to create, launch and extend Saas solutions.
Plataform as a Service (Paas)	Yes	The Amazon AWS cloud computing platform provides the flexibility to create your application mode regardless of the use case. Amazon AWS provides Amazon EC2 with infrastructure, it is responsible for the application, and for data, choosing the instance (OS, patch) and AWS is responsible for storage, networking, servers and virtualization.
Infrastructure as a Service (Iaas)	Yes	Amazon AWS provides Amazon EC2 with infrastructure, it is responsible for the application, and for data, choosing the instance (OS, patch) and AWS is responsible for storage, networking, servers and virtualization.

Implementation Models		
Publiccloud	Yes	Amazon AWS allows the user to create an account, offering the possibility of building a 100% public environment.
Private cloud	Partial	Amazon Virtual Private Cloud (Amazon VPC) enables you to provision a logically isolated section of the AWS cloud in which you can run AWS resources on a virtual network that you define yourself. There is complete control over the virtual network environment, including selecting your own IP address range, creating subnets, and configuring network route and gateway tables.
Communitycloudorcommunity	Yes	Amazon AWS has services designed exclusively for community clouds or community, providing data security, advanced auditing controls, and private and isolated resources if necessary.
HybridCloud	Yes	AWS has developed a suite of industry-first hybrid capabilities that span storage, networking, security, and application deployment and management tools to facilitate cloud integration as an extension of today's investments. Strategic partnerships have been established with the provision of local platforms such as VMware, Intel, Microsoft, SAP, among others to enable the execution of current AWS applications with full compatibility and high performance.
Security andEncryption		
Basic security	Yes	The exchange of passwords between servers and clients can be done.
	Yes	According to Amazon, all network traffic entering or exiting through IPSec VPN connections can be inspected by the client's own IDS / IPS tools.
	Yes	Network devices, including hardware, are used to monitor and control external and internal communications. No antivirus information was found, however, it can also be deployed to VPN with IPSec to filter files before they are inserted into the channel.
	Yes	VPNs with IPSec can be configured.
	Yes	The default port 3306 is configured for the connections and can only be changed at base creation time.
	Yes	The connection between servers and clients can be made using cryptography through public keys.
Conceptual Cryptography	Yes	AWS provides security and encryption of network connections.
Symmetric key cryptography (or secret key cryptography)	Yes	For encryption of transmitted data, Amazon provides the KMS service in AWS.
Asymmetric (or Public Key) Cryptography	Yes	The use of public keys is associated with authentication to encrypt connections.
	Yes	Amazon EC2 uses public-key encryption to encrypt and decrypt login

		information.
Digital certificate	Yes	AWS Certificate Manager is a service that enables you to easily provision, manage, and deploy certificates (SSL) / (TLS) for use with AWS services and connected internal resources.

Table 2: Results Obtained

Digital signature	Yes	Through Signature 4 AWS provides the ability to perform digital signature.
EncryptedIPSecProtocols	Yes	Amazon AWS supports IPsec VPN connections.
SSL / TLS encryptedprotocols	Yes	Amazon AWS Certificate Manager enables the deployment of SSL and TLS. AWS Certificate Manager eliminates time-consuming manual processes such as purchasing, uploading, and renewing SSL / TLS certificates.
PGP encryptedprotocols	Yes	Amazon AWS works with the PGP key in the ASC table.
S/MIME EncryptedProtocols	Partial	The Amazon WorkMail web application client is not supported. However, if you need to use the protocol, you can use services such as Windows Outlook.
SET encryptedprotocols	No	Notcompatiblewithprotocol.
CryptoCloud	No	Even though there is a lot of documentation on cloud cryptography, there is no adoption of the term Crypto Cloud in AWS.

IV. RESULTS AND DISCUSSION

In this work, it was proposed the creation of an internal control framework capable of assisting in choosing a cloud service with necessary security. This framework provides greater direction in the analysis of service contracts (SLA) and provides

Support for oversight of the contract concluded between clients and providers.

The choice of the cloud provider by the customer must take into account the requirements of your business, which controls will prioritize and which ones are covered.

In the framework, we used the topics raised in the literature review as a basis for evaluation of the existing controls: Essential characteristics of the cloud; Service Models; Implementation and Security Models and Cryptography.

Amazon AWS was used as the basis to be evaluated following the control families mentioned

above and the theoretical reference.

Amazon AWS had a great return on the evaluations carried out; the data below is as follows:

FeaturedTopics	Yes	Partial	NO	Total Assessed
Essentials CloudFeatures	10	0	0	10
Service Models	3	0	0	3
ImplementationModels	3	1	0	4
Security andEncryption	15	1	2	18
Total	31	2	2	35

In total, 35 internal controls were evaluated, of which 35, 10 belong to the Essential Characteristics of the cloud; three are Service Models; 4 of Implementation Models and 18 of Security and Encryption.

The top rated items are the Essential Cloud Features and Service Models topics in which all the evaluated controls have had a positive return on Amazon AWS.

The implementation model had the four controls evaluated only the private cloud as the only one that

Amazon was not fully met, even the company providing services for the private environment use.

In Security and Encryption, 18 controls were evaluated, and an S / MIME control is partially satisfactory, since Amazon AWS does not provide a configurable client for the protocol. However, it allows other applications to be possible to use and two controls that do not have in Amazon AWS, these are protocols and cryptographic algorithms SET and the concept of Crypto Cloud.

In total, of the 35 internal controls evaluated, 31 obtained a positive return in Amazon AWS; two partial and 2 are not possible in the web services of Amazon.

V. CONCLUSIONS

This work on the security of a migrated environment in the cloud presented the construction of a conceptual framework (similar to COBIT) based on families of internal controls that supports the analysis of service contracts following the SLA definition. The research focused on key points of verification essential to a cloud environment. Defined internal controls were verified by testing a test account in cloud environments.

In the public and private cloud environment, it was considered the Amazon AWS provider. As the main conclusions and contributions, it can be mentioned that a framework of internal controls:

- It is suitable for ascertaining the security of the information in data trafficked in the cloud, vulnerability analysis were applied in the verification;
- It is appropriate to monitor levels and service contracts: there are specific controls for contract analysis and service levels;
- Provides support for creating metrics for service monitoring;
- Can be integrated with service contracts to give more transparency to service rules;
- Supports all essential cloud features, service models, thesis of almost all deployment models, and a range of encrypted protocols and algorithms.

There are several other solutions besides the framework proposed in this work so that after migrating an environment to the cloud, it is possible to obtain security, integrity, scalability and complete contractual apparatus with the providers, in order to obtain the maximum of the contract without major future problems.

REFERENCES

[1] Vaquero, L. et al. A break in the clouds: towards a cloud definition. SIGCOMM, 2008.

[2] Ruschel, H. CloudComputing. Especialização em Redes e Segurança de Sistemas. Curitiba, PR: Pontifícia Universidade Católica do Paraná (PUC), 2010. 117p.

[3] NIST. The NIST Definition of Cloud Computing. 2011. Disponível em: <https://csrc.nist.gov/publications/detail/sp/800-145/final>. AcessedOctober 11, 2018.

[4] Sousa, F. R. C.; Moreira, L. O.; Machado, J. C. CloudComputing: Conceitos, Tecnologias, Aplicações e Desafios. ERCEMAPI, Parnaíba, 2009. Disponível em: <http://www.ufpi.br/subsiteFiles/ercemapi/arquivos/files/minicurso/mc7.pdf>. AcessedNovember 26, 2018.

[5] Veras, Manoel. CloudComputing: nova Arquitetura da TI. Rio de Janeiro: Brasport Livros e Multimídia Ltda., 2012. 240 p. Disponível em: <https://books.google.com.br/books?id=yiggoX2aoC8C&printsec=frontcover&hl =pt-BR&source=gbs_ge_summary_r&cad=0#v=onepage&q&f; =false>. AcessedNovember 20, 2018.

[6] Martins, Rômulo. Os modelos de CloudComputing. 2013. Disponível em: <https://www.qinetwork.com.br/publica-privada-comunidade-ou-hibrida-conheca-os-modelos-de-cloud-computing/>. AcessedNovember 29, 2018.

[7] Amrhein, D.; Quint, S. CloudComputing para a empresa: Parte 1: Capturando a nuvem. 2009. Disponível em: <http://www.ibm.com/developerworks/br/websphere/techjournal/0904_amrhein/0904_amrhein.html>. AcessedNovember 23, 2018.

[8] Stanoyevitch, Alexander. Introduction to Cryptography with Mathematical Foundations and Computer Implementations CRC Press, California State University Carson, California, USA. 2010.

[9] Wenzel, Maira. Serviços criptográficos. 1. 2017. Disponível em: <https://docs.microsoft.com/pt-br/dotnet/standard/security/cryptographic-services>. AcessedNovember 16, 2018.

[10] Stallings, William. Cryptography and Network Security: Principles and Practice, International Edition: Principles and Practice Stallings William Pearson Education, 2014.

[11] Rezende Oliveira, Ronielton. Os principais algoritmos de cifragem. Criptografia simétrica e assimétrica, Belo Horizonte - MG, v. 1, n. 1, p. 3-8, fev. 2012. Disponível em: <http://www.ronielton.eti.br/publicacoes/artigorevistasegurancadigital2012.pdf>. AcessedNovember 17, 2018.

[12] COBIT, 5. COBIT Focus Volume 2: abril de 2014. 5. 2014. Disponível em: <http://www.isaca.org/Knowledge-Center/cobit/cobit-focus/Pages/COBIT-Focus-Volume-2-Abril-de-2014.aspx>. AcessedOctober 15, 2018.