IT Security and Audit in the Clouds

Abstract

Companies are fast adopting IT Public Cloud services due to the many advantages inherent to them. But speed and simplicity of adoption often lead to forget other issues like security of information and in general IT security of data and processing. These issues often become more complex to manage in the Clouds to the point that in some cases the investment in IT Public Cloud services eventually turns out not to be so convenient.

IT Cloud services are becoming increasingly popular not only among consumers but also with companies. In the last years IT Cloud services have matured both in quality and in completeness of the offering to the point that many companies, if not the grand majority of companies, has adopted or is seriously considering adopting such services.

From a company point of view, IT Cloud services are a new incarnation of the IT Outsourcing business model which has been known since the beginning of IT. So it should not be strange that companies look and adopt it in large numbers.

There are many similarities between IT Outsourcing and IT Cloud services, but there are also some striking differences which are seldom considered, at least at first. This can lead to major "misunderstandings" and the possibility of failure of projects to adopt or migrate to IT Cloud services.

IT Public Cloud services

IT Cloud services are usually classified in 3 types (see refs. [3 – 5]):

- Infrastructure as a Service (**IaaS**): the service offered is a virtual infrastructure which allows to easily build services like virtual machines, network nodes etc.
- Platform as a Service (**PaaS**): the service offered is a virtual platform which allows to easily build applications
- Software as a Service (**SaaS**): the service offered is a full application

and 4 fruition models:

- **Public**: the service is accessible by anyone on Internet
- **Private**: the service is internal to a company
- **Hybrid**: part of the service is Public, part is Private[1]
- **Community**: the service is specialised for a community like for example for development, research, education etc.

Usually when IT Clouds are mentioned, people refer to "IT Public Cloud services", independently of the 3 types (SaaS, PaaS or IaaS).

IT Public Cloud services have a number of positive sides which are easy to list:

- Low cost
- Service ready
- Huge scalability
- Pay per use
- always up-to-date and with the latest features
- OPEX (Operating expenditures) without (or with little)[2] CAPEX (Capital expenditures).

The business model of a provider of IT Public Cloud services, is to make capital investments in the IT infrastructure and applications to provide to many customers the same, really identical service at a low price (by realising scale economies), immediately ready and with the possibility of large scaling of performances. This allows the customer to invest the capital in its own business services, paying at the same time just what it is used of the IT services.

So far nothing new for this business model, it was once called "Outsourcing".

As in outsourcing contracts, also in this case it is necessary to understand the responsibilities and duties of customer and supplier. Many IT Outsourcing projects failed miserably because of the lack of clarification of "who does what" and "who is responsible for what".

In the case of IT Public Cloud services, the risk is even greater because of the ease of access to the services: most of the time it is enough just a click of the mouse, and no one reads the terms of service written in small, and then the service is paid by credit card (whatever this means). In the

---

1 For example the development environments are Public clouds but the production environments are Private clouds.

2 Quite often to access Public IT Cloud services a company needs to invest on some internal IT infrastructure components to connect the internal IT systems to the Clouds.

case of a traditional outsourcing, there was at least a paper contract that someone had to read and sign, maybe requiring before an opinion by the legal office. For IT Public Cloud services contractual terms protect mostly the service provider and have generic customer protection clauses. This is inevitable since customers are different with different needs but the service is identical for all of them.

IT Public Cloud services are really "**One size fits all**".

Even if this sounds obvious, in practice this concept is never really well understood by the customer who expects a level of personalisation that IT Public Cloud services will never provide.

An IT Public Cloud service is never a complete (and just cheaper) substitute for a personalised private or outsourced service.

Data Ownership and Security

In an IT Public Cloud service, data is processed, managed, archived by/on the service provider's systems. After all, it's just what it is the purpose of the service, so we can not marvel. The main point is that the same data that previously resided exclusively on company internal IT systems, it is now present on the provider's systems. In the case of a traditional Outsourcing service, the external systems where the data resides are in a nearby location, which is possible to access and visit by the customer, on dedicated servers, and the data path between the company headquarters and that of the provider is known.

For an IT Public Cloud service, all of this is not valid: for example an Application service (SaaS) provider in turn uses Public PaaS and IaaS services (from SaaS to PaaS to IaaS), and each of them uses redundant servers in multiple data-centers to ensure high reliability and lower costs since they are placed in economically cheaper locations.

Then business data is often handled, managed and archived on systems of multiple service providers (often not known by the customer) and distributed around the world.

This is what allows services to be low-cost and high-performance, but how can security measures be implemented so to protect the information managed by IT Public Cloud services?

First of all, who is the owner of the data and information?

Here there is quite a difference between consumers and companies. For a consumer very often the rules is that the data (information) "belongs" to the service provider (aka "all your data belong to us"), but it has to be considered that the services are usually provided for free. For companies, which pay the services, the responsibilities on data and information is vice-versa all on the company.

The typical contracts regulating IT Public Cloud services, often state that it is up to the customer to decide if the service provides enough security features to protect that specific company's information, and that if something happens to the information, it is not in the responsibility of the service provider.

It is then necessary to evaluate how realistic is the following scenario and which could be the consequences: for any reason, all the company data in an IT Public Cloud service is at some point made truly public, that is, anyone can access it via Internet, or others can access it and use it without the company being able to prevent it.

What consequences would this event have for the company?

This question is crucial and should not only be made, but it should also be given the right answer.

Notice that security features to protect data and information are often also required by legislation and international standards. In many situations, it is difficult to prove compliance to legislations and international standards when the service managing the information is in Public Cloud.

IT Cloud providers usually deliver “certified” services, but obviously the certification covers the providing of the service, not the actual managing of the specific data and information of a particular company.

Data protection

It is not easy to implement protection measures for IT data managed by system which cannot be personalised and offer only standard features.

The first step is to decide which data can be managed by IT Public Cloud services and which data cannot. This often has some unexpected consequences. A typical case is that of a business process which should be based on a IT Public Cloud application (eg. SaaS) and for which, based on IT Risk and Security or compliance requirements, some of the data cannot be managed in Public Cloud. It is then necessary to integrate the Public Cloud application with an on-premises application which manages in parallel the higher risk data. But this creates a new risk since the two applications should exchange information at least so that they are synchronised on the state of the business process. This opens up the company's internal IT system to a flux of data with a Public, eg. Internet, service and the associated security risks.

In these cases, what looked initially as a cheap and very simple way of implementing an IT service, turns out to be more expensive than expected and much more complicated to implement and to use. Thus at the end the benefits of the adopting a IT Public Cloud service are less than what desired.

A similar scenario is the one in which the company decides to implement a IT Public Cloud IaaS

service. This can be practically equivalent to build a new virtual data-center which should be populated with all the typical data-center infrastructure and application services, only that now they are provided as service instances in this novel environment.

But setting up and starting a virtual machine is one thing, another is setting up an entire virtual data-center with all its components like: different environments for production and development, network segmentation and access control, (virtual) routing and switching, firewalls, IPS, management and accounting systems and so on.

At the end, having all the management, accounting, security etc. devices and functionalities in place can end up to be equivalent to the effort of really building a new physical data-center. On top there is the added burden to manage two data-centers, the physical one internal to the company and the virtual one in the IT Public Cloud. Moreover the two data-centers often adopt, at least in part, different technologies and solutions, and thus require different competences to manage them.

Also in this case the positive sides of adopting an IT Public Cloud service can be, at least partially, reduced by these extra requirements.

For what concerns the data protection, our starting point, it would seem that in a virtual data-center everything can be managed and protected as in the data-center internal to the company. But also in this case there are differences which must be considered.

The main issues which should be considered also in the case of IaaS (and PaaS) IT Public Cloud, is where the data physically resides.

Obviously the data resides on the hardware infrastructure of the Cloud provider and, unless specific limits are agreed, it can be in any system, anywhere in the world in the provider business locations. Moreover the company's data and services share the hardware with all the other data of the other customers of the provider. This has two possible threats:

- access to company's data and information by the provider's personnel as for example doing backups (eg. snapshots of virtual machines) or accessing systems for maintenance;
- access to company's data and information by other customers either due to errors or bugs in the virtualisation system or due to a deliberate attack.

A simple approach which gives a first protection against these threats is to:

- encrypt all traffic between any system ;
- encrypt all data at rest on file-systems, databases etc.

where the encryption keys are managed by the company and care is taken to guarantee that the

provider cannot access them. If the encryption keys are correctly managed (and this can be a not so trivial task) implementing these types of encryption protect data and information at rest (including backups, snapshots etc.) and in transit. But this does not protect data during elaboration, which as today can not be encrypted.[3] This implies that the previous two threats remain even in presence of data encryption in transit and at rest, albeit reduced as follows:

- access to company's data and information during elaboration by the provider's personnel when accessing and managing live systems;
- access to company's data and information during elaboration by other customers typically abusing the virtualisation systems in a deliberate attack when sharing the same hardware.

Implementing these and many other security measures (for example we did not consider here access management or data integrity and availability, as in backups) in IT Public Cloud services, even IaaS, can be challenging and can require different or new solutions with respect to the ones adopted in an internal company data-center or in a traditional outsourcing service for example with dedicated hardware.

Auditing in the Public Cloud

Finally we consider auditing but from a quite technical point of view. Which information does an IT auditor need to be able to perform an IT or an IT security audit on a IT Public Cloud service?

Since the service is outsourced to an external provider, the first check should be on the contract for the service with the provider. But in the contract the auditor usually finds clearly described what are the responsibilities of the provider, the SLAs etc. but little or nothing on compliance to the company's procedures, to the international standards adopted by the company and to the legislation that the company must comply with.

Morevover, the company should have amended its own IT policies, procedures etc. adding particular measures for managing the services by IT Public Cloud providers. The auditor should also be able to verify that the internal IT policies and procedures and the extra requirements for IT Public Cloud services are fulfilled.

This requires that systems and services are classified, managed and monitored by the company, not only by the IT Public Cloud provider. As simple and obvious as this seems, it is not always as easy or immediate to implement. For example, since the provider obviously can have most of this information and should be able to provide it with little effort, companies often do not bother to look

---

3 Homomorphic encryption allows to perform some computation on data without the need to decrypt first the data itself. Even if big steps have been done in the last few years in homomorphic encryption, still it can be applied only to very few computations and applications.

in to this issue just to discover when the information is needed that the information collected by the provider and that the provider is willing to share does not satisfy all the internal requirements.

Setting up the needed processes to make the Cloud service compliant, requires often to align the management of the IT Public Cloud services to the internal ones, which includes access policies and rights, data management, security and management policies etc. Only if it is possible to enforce the policies and to trace their application, then an IT Public Cloud service can be compliant and pass an audit.

To this purpose, a new class of security services called "Cloud Access Security Broker (CASB)" [6] can turn out to be very useful since their purpose is to enforce security policies and monitor all activities of Cloud service users and Cloud applications.

References

[1] ENISA, "*Cloud Computing Security Risk Assessment: Benefits, Risks and Recommendations for Information Security*", 2009

[2] Cloud Security Alliance (CSA), "*Top Threats to Cloud Computing*", 2017

[3] NIST, "*The NIST Definition of Cloud Computing*", 800-145, 2011

[4] NIST, "*Cloud Computing Synopsis and Recommendation*", 800-146, 2012

[5] NIST, "*Guidelines on Security and Privacy in Public Cloud Computing*", 800-144, 2011

[6] Gartner, "*Cloud Access Security Brokers*", 2016

Andrea Pasquinucci (PhD CISA CISSP)