cigref
A network
for large companies

PROMOTING DIGITAL CULTURE AS A SOURCE
OF INFORMATION AND PERFORMANCE

Cloud Computing basics

Large companies' perspective

June 2013

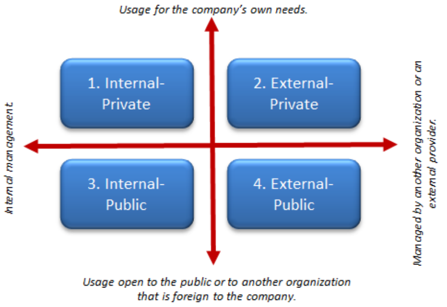
Overview

CIGREF's previous works had highlighted several disagreements in the understanding of SaaS and Cloud Computing. The main one was a lack of a clear definition of these concepts. CIGREF's working group therefore focused on Cloud Computing basics. It revised and redefined them according to the way they were understood and used in companies and not according to offers from the IT ecosystem market.

The working group identified four elements characterizing a Cloud:

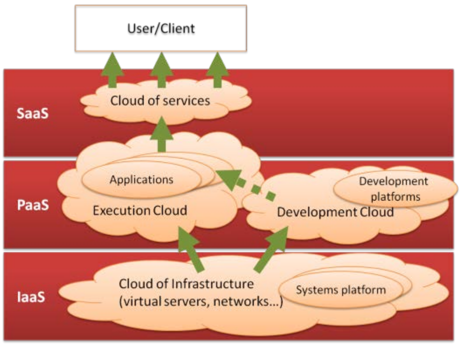
1. A Cloud is always a virtual space,
2. containing fragmented information,
3. These fragments are always duplicated and spread within this virtual space, which can be on one or several physical devices
4. which has a "restitution console" allowing to restore information.

The working group also described and explained in greater details the four Cloud Computing typologies that can be found in organizations that are members of CIGREF. Each of them has been defined and weighted against the service model (SaaS, PaaS, IaaS).


Usage for the company's own needs.
1. Internal-Private
2. External-Private
3. Internal-Public
4. External-Public
Internal management
Managed by another organization or an external provider.
Usage open to the public or to another organization that is foreign to the company.

Source CIGREF

During discussions and experience sharing, much advice was given and best practices were expressed. The group brought together information and sorted it according to the four Cloud typologies, providing a list of priorities for any company interested in Cloud Computing.



Source CIGREF

CIGREF, Network of Large Companies, was created in 1970. It brings together more than one hundred very large French and European companies and organizations from all sectors (bank, insurance retail, industry, services…). CIGREF's aims at « ..*Promoting Digital Culture as a source of innovation and performance…* »

Report Title: *Cloud Computing Basics* – Large companies' perspective

CIGREF team

Jean-François PÉPIN – General Manager
Sophie BOUTEILLER – Mission Manager
Anne-Sophie BOISARD – Mission Manager
Josette WATRINEL – Executive Secretary

Frédéric LAU – Mission Manager
Matthieu BOUTIN – Operations Manager
Marie-Pierre LACROIX – Information Manager
Josette LEMAN – Executive Assistant

Acknowledgements :

We would like to offer our sincerest gratitude to Gérard RUSSEIL, CHOREGIE's CIO, who led this discussion.

We also thank the members of the working group who took part in this study:

Michel BENARD - GROUPEMENT DES MOUSQUETAIRES - INTERMARCHÉ
Cyril BARTOLO - LAGARDÈRE
Éric BARNIER - AÉROPORTS DE PARIS
Laurent BIEBER - SNCF
Thierry CHAMPEROUX - MAIF
Jean-Yves CHOURAQUI - L ORÉAL
Cédric SIBEN - MINISTÈRE DE L'ÉCONOMIE, DES FINANCES ET DU COMMERCE EXTÉRIEUR
Léon DE SAHB - STEF
Luc DEBRAY - AGIRC ARRCO
André DELEVAQUE - NEXTER GROUP
Jean-Pierre DELHEAU - RTE
Jean-Yves DROUGLAZET - MAIF
Bernard DUVERNEUIL - ESSILOR
Marie-Hélène FAGARD - EUROPCAR
Jean-Louis GHIGLIONE - RENAULT
Stéphane HUIGNARD - LACTALIS
Hervé JEGO - GENERALI
Sylvie LABETOULLE - GEODIS
Régis LACOUR - INSERM
Gérard LAGO - RTE
Hervé LAMBERT - GENERALI

Arnaud LE CONTE - GROUPEMENT DES MOUSQUETAIRES - INTERMARCHÉ
Philippe LEBAS - ELIOR
Mina LEJAMBLE - AGIRC ARRCO
Guillaume LIBET - CNES
Christel LOITRON - OCP - GEHIS
Annelise MASSIERA - DISIC
Marc MEYER - MINISTÈRE DE L'ÉCONOMIE, DES FINANCES ET DU COMMERCE EXTÉRIEUR
Hélène MONIN - MANPOWER
Alain MOUSTARD - BOUYGUES TELECOM
Bernard PARMENTIER - AIR LIQUIDE
Jean-Luc PAULIN - AMADEUS
Alain PERONNET - RENAULT
Jean-Luc RAFFAELLI - LA POSTE
Claude ROUCHE - SAUR
Thierry SABLE - TOTAL
Caroline SANDLER-ROSENTAL - CLUB MÉDITERRANÉE
Pierre DE LAJARTE - RÉSEAU FERRÉ DE FRANCE
Grégory SILVAIN - EURO DISNEY
Pierre TOMIAK - CNES
Christian VALIN - LACTALIS
André-Gilles VITTEK - EDF

CIGREF publications related to this report:

2013 - Cloud and data protection: how-to book for the attention of operational and senior managements
2012 – Which infrastructure policy for the digital company?
2011 – SaaS understanding by large companies
2010 – CIGREF's position on Cloud Computing
2010 – Impact of Cloud Computing on the IT function and its ecosystem
2010 – Files of Sales Club – Cloud Computing

For more information regarding this report please contact CIGREF:

CIGREF, a network for large companies - 21, avenue de Messine 75008 Paris, France
Tel.: + 33.1.56.59.70.00 Email: contact@cigref.fr Website: http://www.cigref.fr/

TABLE OF CONTENTS

FIGURES

INTRODUCTION

It has been three years now since CIGREF took an interest in Cloud Computing and in service models.

In 2010 the Cloud Computing offer was already part of IT services and the panel of solutions. CIGREF defined it at that time as **a new way for companies to buy and consume services linked to IT worldwide and through the Internet**. At that time though, we spoke more of SaaS[1] because the market was still structuring itself.

The offer met some needs quite well (transverse application) and some others more badly (especially transactional aspects and ERP), and was rather seen as **a solution to be combined with existing ones**. Resource sharing, pay-per-use, modularity and standardization of proposed duties were the main identified characteristics.

However, the work of CIGREF working groups in 2010[2] and 2011[3] on Cloud[4] and SaaS highlighted **strains regarding the understanding of SaaS between user companies and the IT ecosystem**. Discussions especially showed the positioning gap between suppliers and user companies, in particular regarding the interoperability of solutions and the reversibility of data.

Discussions showed as well **SaaS and Cloud Computing potentials regarding innovation processes**: solutions flexibility, deployment rapidity, lower short term investment. They highlighted too the **need for a guiding of businesses by the IT Department during the acquisition of SaaS solutions**.

Nowadays, some elements have become clear:

- SaaS is seen as a very good way to **help business units in their needs in terms of applications** and thus to **provide them** with **innovative services and applications**.

- It is also a way to **meet the need for flexibility** by rapidly adapting infrastructures or architectures to **occasional and variable needs**.

[1] SaaS: Software as a Service

[2] « CIGREF's position on Cloud Computing »: http://www.cigref.fr/position-du-cigref-sur-le-cloud-computing
« Impact of Cloud Computing on the IT function and its ecosystem»: http://www.cigref.fr/impact-du-cloud-computing-sur-la-fonction-si-et-son-ecosysteme

[3] « SaaS understanding by large companies»: http://www.cigref.fr/la-comprehension-du-SaaS-par-les-grandes-entreprises

[4] The word Cloud will be used indistinctly to speak of a project of Cloud Computing or to speak of Cloud as a tool. This term will also be used for the (technological, economical) models that the concept conveys.

- SaaS can help to **reduce development and integration costs** of application jobs. But the offer is still weak and solutions in service mode are so far quite specific and autonomous: **there is still little integration possible**.

- In the 2010 definition, CIGREF revealed: “Regardless of the method adopted by the client company, the originality of Cloud Computing lies in its pay-as-you-use model, and thus in its readability, its variability and the predictability of its costs”. Nowadays, **costs predictability is not guaranteed more than three or four years. Cloud Computing guarantees, however, the “flexibility” of solutions**, for instance, in case of changing volumes.

- **The concept of consumption prevails over the concept of use**: you buy a subscription, a consumption authorization but not a license to use. SaaS offers to **move from budgetary logic of investment to operating logic**, with a reduction in acquisition and maintenance costs.

- While users used to have no idea of what was set up and consumed, Cloud Computing also permits to **add value to an immediate vision of financial consumption per use**.

- **SaaS applications** provide a **functional standardization** (the same application services are available for all users, without particular development); while **traditional applications are specific** and often adapted to the use of one or several target populations.

- The high economic disparity between suppliers leads to difficulties in comparison. Business Models are not yet well set up and standardized. Hence**, it is difficult to assess the possible TCO[5] of the different offers**.

- In the case of a Cloud, technical solutions of suppliers are not enough: client companies **need to have internal competences and resources** to set it up at its best regarding its use (same as ERP in the early 2000s). A **new job** is maybe coming into existence: setting parameters of Cloud (as setting parameters of ERP already exists)

[5] TCO: Total Cost of Ownership

So, offers have developed and uses have become clear. But during discussions, it appeared that **there is not any real common understanding**. Everyone has his own definition of SaaS, PaaS[6], IaaS[7] and Cloud, and **these definitions evolve over time**.

Hence, during group meetings, CIGREF has expressed the desire to pool knowledge and experience that its member firms had of Cloud Computing, in order **to describe in a representative way their experience of Cloud projects and their use of it**.

LET US REVISIT THE DEFINITION OF A CLOUD

All companies attending the CIGREF working group **have a Cloud Computing project currently going on**. Some of them have already implemented their own Cloud internally. Therefore, most of them know what a Cloud is. Throughout the various discussions however, it rapidly became clear that the concept of "Cloud Computing" could be explained with **different definitions that evolve differently according to the person using it**. User companies, like those of the IT ecosystem, use terms that are more linked to their own business strategy than employed in a spirit of clarification.

In order to **speak with one voice and have a common understanding**, the working group has wished to first work on a shared definition of Cloud Computing.

This definition rests of a couple of simple facts:

- A Cloud is initially a **technological solution**, but its definition depends above all on **the use one makes of it**. Some Clouds are Clouds of service, that offer application based solutions that directly affect final users. Others are Clouds of infrastructure that affect production and exploitation centers by dealing more with the virtualization required to provide infrastructures of servers or networks.

- While **access** to a Cloud requires a **service model**[8], the opposite is not true. Indeed, many applications "as a Service" are not Clouds: they are simple "classical" applications that rely on a traditional infrastructure of web servers, DMS servers or on an ERP. Even nowadays, such confusion is maintained by many for marketing reasons.

[6] PaaS: Platform as a Service

[7] IaaS: Infrastructure as a Service

[8] A model of service allows fully externalizing an element (function or application) of an organization's information system and assimilating it to an operating cost rather than an investment. Thus we speak of an element "as a service".

- The Cloud Computing model is **able to equally process** the three layers commonly used of the model of service.
    - The **IaaS**: Infrastructure as a Service
    - The **PaaS**: Platform as a Service
    - The **SaaS**: Software as a Service

    This is the strength of Cloud Computing: it can either go through all these layers, or relate specifically to each of them.

For the CIGREF working group and even if it may sound basic, a Cloud is above all a **solution for data**[9] **storage** (in the broadest sense of the term: databases structured or not, software, images, etc.) in one or several machines which do not have any **specific functional attribution: they can replace each other**.

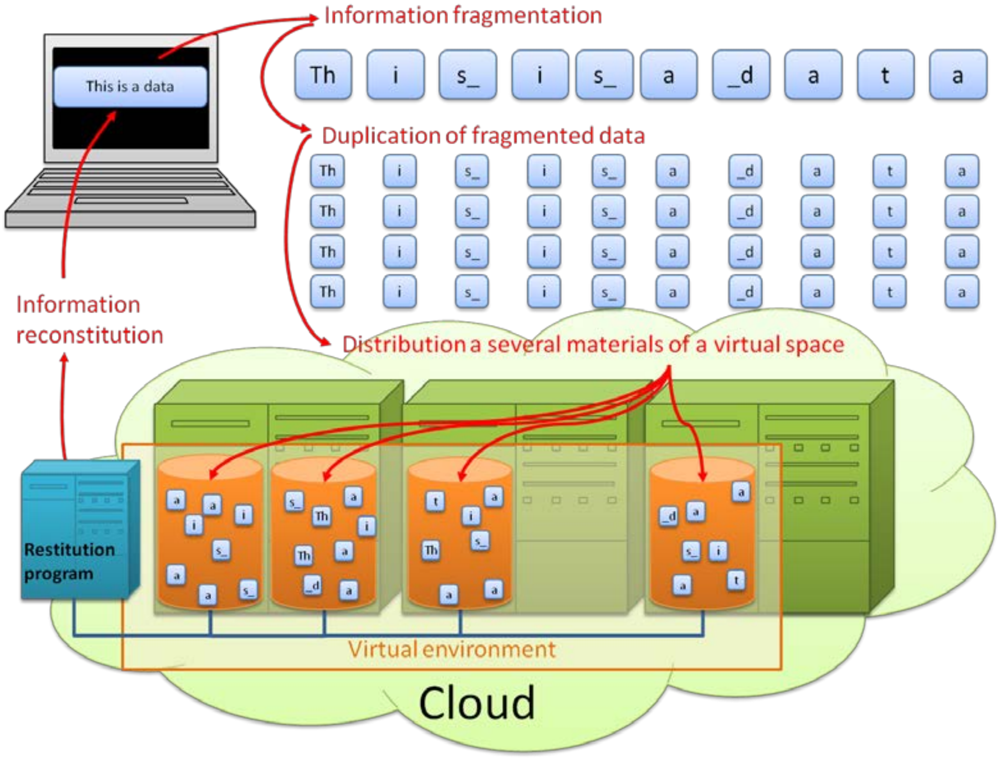
A Cloud **focuses on the data independently from the medium and is able to transmit it independently from its localization**.

In its quest for a definition, the working group identified four elements characterizing a Cloud:

- Point 1: A Cloud is always a **virtual place**,
- Point 2: A Cloud contains **fragmented data**,
- Point 3: These **fragments of data** of a Cloud are always **duplicated** and **spread** in this virtual space that can be on **one or several physical media**.
- Point 4: A Cloud has a "**restitution function**" allowing **restoring data**. This function can be part of the management of the Cloud or moved on the application that provides the service.

If one of those four conditions is not met, one is not in the presence of a Cloud

[9] A « data » is a piece of information, especially facts or numbers, collected to be examined and considered and used to help decision-making, or information in an electronic form that can be stored and used by a computer (Cambridge Dictionaries).


Information fragmentation
This is a data
Th i s_ i s_ a _d a t a
Duplication of fragmented data
Information reconstitution
Distribution a several materials of a virtual space
Restitution program
Virtual environment
Cloud

(Source CIGREF 2013)

Figure 1 : The four points allowing the identification of a Cloud

In addition to these required conditions, these works show:

- That **it is not possible to know the whereabouts of a particular piece of information** (that is why it is called "Cloud"). Indeed, the fragments of data that constitute it are spread on all media/devices that make up the Cloud, and only one "restitution application" can localize them in order to restore data and provide entire information.

  This ability to distribute data allows the extension of a Cloud to several datacenters located in places that are geographically far away from each other and connected through high-speed networks. However, many Cloud offers are limited to a distribution on a collection of servers in a single datacenter.

- That **the fragmentation granularity is significant**.
  - Indeed, if the **fragments are too significant**, it will be possible to **read their contents** but there will be **greater processing – for a larger fragmentation**.
  - If fragments are **too small (beyond the safety requirements)**, the **number of accesses** required to restore information data could be the limiting factor of performances.

Anyhow, **data fragmentation increases reliability and security but can reduce their aggregation**. In that case, the network quality is a significant factor, especially in the case of a Cloud which relies on several datacenters connected between each other.

- That **data restoration** for information delivery, the running of an application or the access to a function **form the "service" provided**.

- **That this definition can be applied regardless of the service model** implemented: IaaS, PaaS or SaaS.

In terms of implementation, infrastructure and security, it is then possible to deduct several significant elements from the four points above.

- **The loss** of a part of a Cloud (a device for instance) **has no impact on information** as it is duplicated and spread over several devices or over several places. Therefore, a piece of data is stored in multiples places. In that case, is the back-up of Cloud servers always necessary?

- Likewise, if a Cloud should run out of resources in existing servers**, it would then be possible to add extra devices**[10]. A Cloud adapts to the required volume, **it is scalable.** In particular, this characteristic can help optimize available space: in a Cloud, data "fills" the available space instead of being "allocated" to defined spaces. Some CIGREF members, moving from classical datacenters to a Cloud, have significantly reduced the amount of servers used.

- In addition, **theft (or delivery) of data of a server** or group of servers **does not make it possible to read information** stored in it, as each piece of information only contains fragments of data. The only program of information restitution ("restitution console") is able to make the link between fragments. In addition, if data has been encrypted (with an RSA key for instance) before being fragmented, it becomes almost impossible to read the fragments directly. However, this last point depends on the level of data fragmentation: large fragments will be more significant and will make it possible to read more information.

- In terms of protection and security, the **critical component** is not the Cloud itself with its data servers but the **"restitution application (or console)"** that allows

[10] Mainly servers. But, in and of itself, it is possible to use disk spaces available in any device (server, desktop, laptop, etc.) that is connected to a network.

restoring required data for service delivery. **It is this application that has to be protected**. It is especially necessary to take into account its geographical location and the legislation it depends on (for instance in the framework of a Cloud of a service provider).

PROJECTION ON MODELS OF SERVICE

So Cloud Computing is a solution that provides a space where it is possible to place, in a virtual manner, server infrastructures or network, development or execution platforms, service catalogs, etc. Therefore, a Cloud is **able to process the various layers of the model « as a service »** from the infrastructure to the user.

CLOUD & IAAS - INFRASTRUCTURE AS A SERVICE

There should be no confusion between a Cloud infrastructure and a Cloud of infrastructure:

- A Cloud infrastructure corresponds to all software and material resources required in **the formation of a Cloud**. This infrastructure is very much needed when a company sets up its own Cloud internally.
- A Cloud of infrastructure is **the service provided by the Cloud**: a virtual infrastructure on which it is possible to build, for instance, an application based solution. That is what is provided to a company in the case of a Cloud of external infrastructure.

The IaaS essentially relates **to Clouds of infrastructure**.

They provide according to demand a set of “low” level services, which are servers, networks, etc. Thus, it allows a client company **to benefit occasionally from the power of an infrastructure without having to invest much**.

When there is a **certainty about high load variations** or **uncertainty regarding the ability of an infrastructure to deliver a service**, Cloud Computing is then an appropriate solution: for instance, for needs such as wages, messaging service or document editing (massive and occasional document creation). Moreover, the Cloud can allow maximizing benefits from hardware sharing (processor, disc, etc.).

In a Cloud of infrastructure, the users or the client companies manage its virtual environment and can install in it everything they want. Many, for instance, offer to install virtual servers, which can be configured on demand and on which applications can be run.

Note:

The CIGREF working group points out that **it is essential to find the right player able to guide the client.** In addition, it tells that the task is not easy as the player will need to wear two hats: **infrastructure** as well as **service** and **use** in order to help teams in managing and implementing the solution.

Nowadays, regarding IaaS, a new offer essentially coming from manufacturers, operators and web host providers is currently coming into existence.

CLOUD & PAAS - PLATFORM AS A SERVICE

If SaaS essentially relates to production and exploitation, Cloud at a PaaS level **relates to applications developers and producers**, which are two levels of service: platforms development and applications that provide the service from the upper level (SaaS).

PaaS allows, for instance, provisions for developers with a **development framework** that meets their needs.

It allows permits providing applications with an **implementation framework** that will produce SaaS services (such as Salesforce).

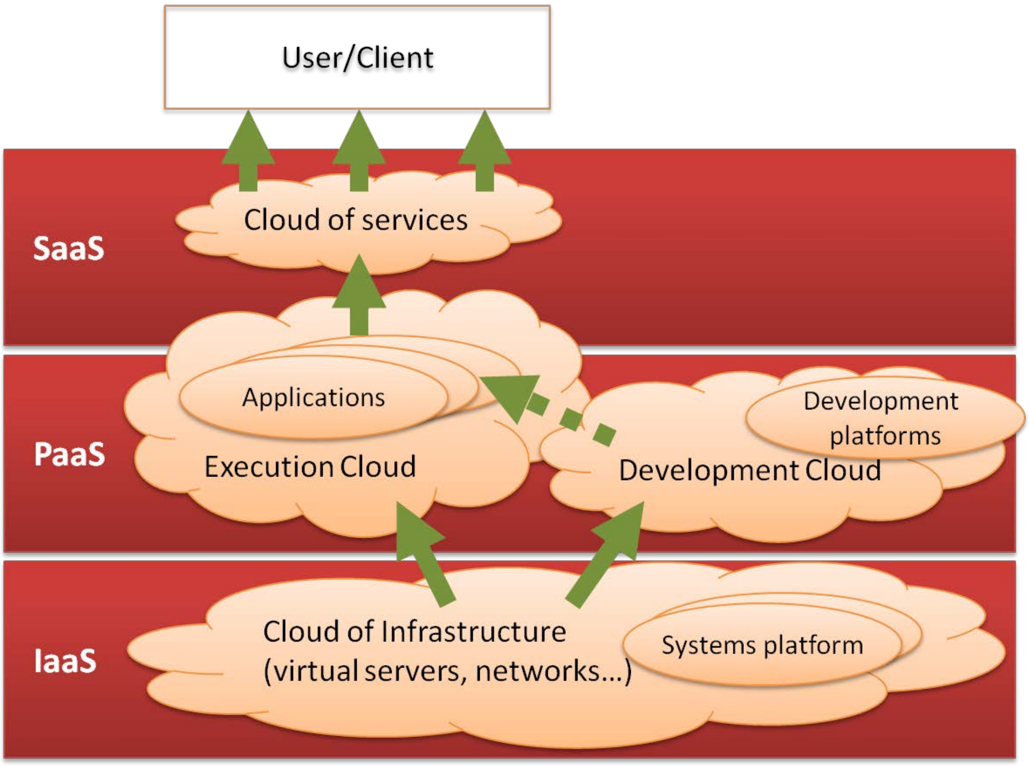
Note:

Please note that required resources for an application in PaaS mode can depend on the significant number of clients that have access to it in SaaS mode (for instance in the case of bandwidth consumption). In that case**, the service of supplying a platform can be charged by some operators as a classical production platform**, which means per number of users and not with an overall subscription to the service.

CLOUD & SAAS - SOFTWARE AS A SERVICE

Cloud at a SaaS level presents most of the time a **catalog of applications that are accessible in service mode for users or final clients**.

In SaaS mode, **use prevails over solutions**: we are dealing with messaging services, CMS, purchase service in online stores, library access service, etc. The application is already built and operational, there is **no real development but rather a parameter setting**. Hence, this model of service is successful: it affects everyone and puts in anyone’s reach a set of services that can be easily shaped and customized.



(Source CIGREF 2013)

Figure 2 : Structuration of the different Clouds compared to the service model

It can be **of particular relevance** for a company to use a Cloud in SaaS mode **during modeling or prototyping phases** because it allows in a very short period and at a reduced cost the assess to a solution, to be able to test it without implementing its own resources, and then, in the case of a conclusive result, to internalize it.

It is this ease of use that appeals to business units. This kind of solutions allows them to approve a concept (such as marketing) and even test a few of them, make "business" choices regardless of the information system of the company. They have the possibility to directly involve other players (clients, partners) in their thought. Moreover, they do not need the endorsement of the IT Department.

It is this ease of use that worries the IT Department, because it can lead to choices that do not correspond to the IT strategy of the company, especially in terms of integration and security.

« AS A SERVICE » MODEL VS. « ASP » MODEL

Please note that one may confuse « as a Service » with what used to be called the ASP (Application Service Provider). While the concepts may seem close to each other, there are some noteworthy differences:

- **Applications** that are based on the **“as a Service”** model were initially created for the Web and use **a “multi-tenant[11]” architecture**.
  - In the **« as a Service » mode, the production environment is shared and virtualized**: there is only one instance for all clients. On the contrary **in the ASP mode, there is one instance per client**.
  - In **ASP** mode, **customization** is possible but requires **specific developments**. **In SaaS mode**, **customization** is only possible through **parameters setting** because there is only one standard for all.
- **Version upgrades in ASP mode**, for the reasons mentioned above, are **much more complex**, problematic (and so costly) than in the “as a Service » mode, especially if the application has experienced specific developments for some clients.
- To illustrate the difference between these two modes one can cite, for instance, two leading solutions in the purchase application market that have totally different models: Ariba (100% SaaS) and Synertrade (100% ASP).

CLOUD COMPUTING TYPOLOGIES

Nowadays, it is not always easy to have a simple description of a Cloud and a clear explanation of typologies that are related to suppliers’ offers. All it takes to be convinced is to ask during an event “what is a Cloud and what are its typologies?”. The clarity of offers though, must contribute to guaranteeing the quality of services offered by the IT Department to clients Business Units.

The CIGREF working group has thus considered the **different typologies of Cloud Computing** that can be implemented. Reflection evolved around two notions:

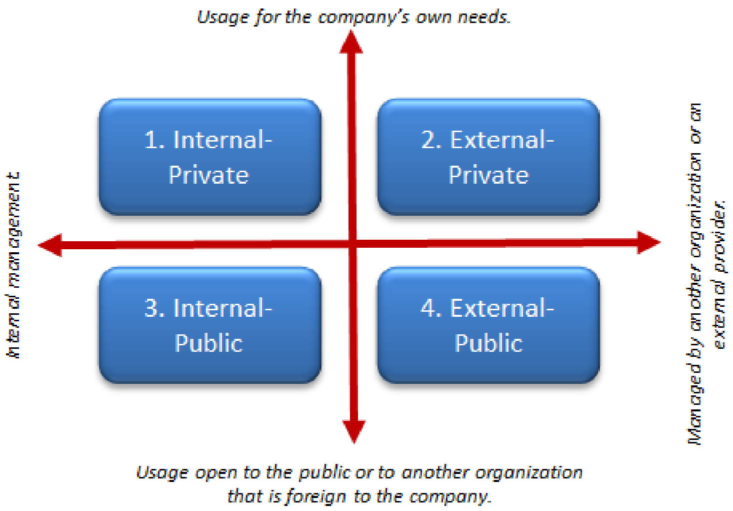
1. « **Who manages the Cloud?** »: the company itself or a Cloud operator?
   The group decided to use the following terms:
   - « **Internal** Cloud» in those cases where it is **the company that manages the Cloud** with its own resources.
   - « **External** Cloud» in those cases where **the management of the Cloud is controlled by a service provider that is Cloud operator**.

[11] A multi-tenant architecture implements a single application instance but that can be used by a large set of clients of different types.

2. « **Who is the client of the service offered by the Cloud**? »: the company itself or an external organization (supplier, partner, subsidiary, etc.), or even the general public (the company's clients for instance)?
   The working group decided to use the following terms:
   - « **Private** Cloud» when it is **dedicated to the company's own needs**.
   - « **Open** Cloud» when it is **open to the general public** or to another **organization external to the company** (supplier, partner, subsidiary, etc.)

Eventually, **four typologies were identified**. Each of them does not affect all companies but they are typical of what an IT Department can be leaded up to consider.

Typologies can also be mixed. For instance an EIG can manage an internal Cloud and offer private services for the company and public ones for other companies. Moreover, an internal Cloud may need to extend occasionally and thus spill over into an external Cloud: this is called **hybrid Cloud**.


Usage for the company's own needs.
1. Internal-Private
2. External-Private
3. Internal-Public
4. External-Public
Internal management
Managed by another organization or an external provider.
Usage open to the public or to another organization that is foreign to the company.

(Source CIGREF 2013)

Figure 3 : Cloud Computing Typologies

1. CLOUDS INTERNALLY MANAGED AND FOR PRIVATE USE

These are **solutions that are totally managed by the IT Department**. The IT Department might appeal to a service provider (such as a facilities manager) but it has total control over the solution.

Solutions of internal and private Cloud facilitate the provision of a catalog of internal services and **establish themselves as an operational alternative to existing services on Internet**.

They allow **better agility and greater service quality**, at the cost maybe of specific developments that are no longer possible[12]. However, as the company has control over it, it is always possible to manage some clients' features by customizing the settings of instances.

Feedbacks have also revealed that the implementation of an internal Cloud can allow **optimizing the use of** a datacenter's **resources** and **making perpetual an infrastructure**.

In terms of security, all large groups have defined a security strategy that is part of the IT governance. Servers related to an internal Cloud must abide by this security strategy. Therefore, there is no further action required.

Here are some examples of internal Clouds for private use for each layer of service affected :

- SaaS : internal collaborative spaces
- PaaS : platforms of development servers on demand (Web development : ViFiB)
- IaaS : deployment of virtual servers on demand (ViFiB, VMware, EMC, IBM, HP, …)

Notes:

1. **There has been a debate within the CIGREF working group regarding the point of implementing an internal Cloud for private use** for the company. While many participants understand in their context the interesting aspect of a Cloud, others see a marketing concept without real added value compared to traditional infrastructures. For them, the interest of Cloud Computing rests on its role as an external solution for the company.

2. Some members of the working group believe that **a minimal size** (for all layers of the model of service) is required **for the Cloud to be useful and efficient**:
   - for instance, a certain number of servers for a IaaS ;
   - a sufficient application scope for a PaaS platform ;
   - a catalog that is filled enough with services for the SaaS.

   However, no quantitative element has been given.

[12] A Cloud provides its clients with a generic service.

2. CLOUDS EXTERNALLY MANAGED AND FOR PRIVATE USE

These are solutions that **save** the IT Department **from investing in a specific infrastructure**, which implies processes guiding its implementation and having required skills. It still requires a minimal number of studies and developments that are essential in terms of integration with what already exists[13].

The **choice of investing** in the implementation of an internal Cloud versus the rent of services in an external Cloud **is linked to a long term or short term strategy of the company**, to its size, and to the number of users.

It this typology, the relationship with the supplier evolves. **New issues appear** in terms of data localization, system interoperability and reversibility of applications. Particular attention must be paid to contractualization with the service provider. **Generally, "one does no longer buy a license to use, one subscribes to a service"**.

Several members of the working group agree that **services rental** is **economically attractive for periods of a couple of weeks or months but not on the long run**. When the licensing model is possible, ROI[14] seems to be higher in the long run. However, as technologies, uses and especially companies' strategy develop; **it is not possible to anticipate the future more than three to four years**. Hence, subscription prevails successfully.

In terms of security, problems related to external Cloud are different from those of internal Cloud: the security policy of the supplier is not controlled by the client. Yet, in this particular case, **the supplier must be able to guarantee the security of its client's data**. It must have governance that is shaped to the client; otherwise, there is a risk of allegiance to the supplier's policy. The question is **how to influence a Cloud supplier so that the contract is not totally generic, especially regarding issues of data protection**[15].

The use of an external and private Cloud implies as well to clearly **define the scope of expected services**. This perimeter must extend **beyond software and technical services**. It must contain job expertise in order to be efficient and relevant in the phases of setting, training, and change management. While these services can be the subject of a contract with a consulting company, it would be better to **make the solution provider aware of his responsibilities** by entrusting him with the role of project manager with an obligation to perform.

[13] The legacy

[14] ROI: Return On Investment

[15] In this regard, more information can be found in the report (coming soon) CIGREF/AFAI/IFACI "Cloud Computing and data protection. Practical guide destined for senior and operational management".

Finally, a grey area remains regarding the layers model: **the service provider commits to the layer affected by the contract, but what about inferior layers[16]?** No answer has been found so far among the various offers.

Here are <u>some examples</u> of external Clouds for private use for each layer of service affected:

- SaaS: Online office suites (Google Apps, Office 365), CRM (Salesforce), online sales services (Amazon)
- PaaS: Development environments (Oracle PaaS, Salesforce, ViFiB,…)
- IaaS: Virtual infrastructures rental (OVH, Amazon, Numergy, CloudWatt, Cheops Technology, Intrinsec,…)

3. Clouds internally managed and for open use

This typology mostly relates to organizations (such as EIG[17]) that offer internal services to the company and external ones to clients. **The company is thus itself a "Cloud operator"**.

In that case, constraints and notes previously identified regarding an external Cloud for private use are still ongoing but inversely:

- Be able to address the issues of data localization, system interoperability and reversibility of applications.
- Make the right choice regarding the economical model: license or subscription.
- Rely on and communicate about one's own security governance in order to guarantee the data security of one's client.
- Define the scope of the offered services.
- Bring an answer to the commitment on the layers of service that are inferior to the layer affected by the offered service.

Here are <u>some examples</u> of internal Clouds for open use for each layer of service affected:

- SaaS: turnkey website of type CMS for a franchised business
- PaaS: offer of on demand development platforms (Free Cloud Alliance, …), parameters setting of virtual configuration (VMWare,…)
- IaaS: offer of virtualized servers (VMWare, IBM, HP, Free Cloud Alliance, …)

[16] Except IaaS that is the lowest layer.

[17] EIG: Economic Interest Group.

4. CLOUDS EXTERNALLY MANAGED AND FOR OPEN USE

This typology corresponds for instance to the case of Business Units, that directly appeal to service operators to implement a Cloud of service for populations that are external to the company, such as clients or partners.

This situation, recognized by many member companies, is thus **particular** because it allows Business Units to, *a priori*, be independent from the IT Department. This typology allows as well often Business Units to **challenge the IT Department in its ability to offer a similar service** in terms of uses, costs, period and performance.

Beyond the essential communication between the IT Department and Business Units, the role of the IT Department is thus to advise the client in his choice of the Cloud that meets his need. Its role is also to prevent redundancy with the ongoing information system, or to prevent unexpected holes in the security due to « wild » link with the company's information system.

Here are some examples of external Clouds for open use for each layer of service affected :

- SaaS: public or professional social networks (Facebook, Google+, LinkedIn), publication or uploading of products in online stores (AppleStore, Amazon)
- PaaS: platforms for development of mobile applications (Kawet), parameters setting of virtual configurations (VMware), or applications hosting (Windows Azure), Web development (ViFiB)
- IaaS: data storage spaces (iCloud, SkyDrive, Google Drive, DropBox, CloudWatt, Numergy, telecoms operators: Orange, SFR, Bouygues Telecoms…)

ADVICES AND GOOD PRACTICES

The following tables present a range of advice and good practices regarding the four Cloud typologies. This list is not exhaustive and stems from numerous discussions and feedback that took place during the working group meetings of the working.

This advice and good practices have been divided into five categories:

A. Legal
B. Security and risks
C. HR and skills
D. Data and audit
E. Infrastructures

1. Internal – Private Cloud *The company manages a Cloud for its internal use*	2. External – Private Cloud *The company uses a Cloud managed by an external operator for its internal use*
A. LEGAL	
CONTRACT	
- Keep watch over contracts with editors and manufacturers (especially the license pricing structure and dependency on the infrastructure) for software introduced in the internal Cloud. - Establish an internal « service offer » to supervise services and commitments to internal users.	- Keep watch over contracts with Cloud operators, and especially make sure that the operator provides differentiated service levels (SLA). - Contractualize a commitment to assistance from the supplier for data recovery (in case of bankruptcy, end of contract…). - Keep watch over license agreements for software introduced in the Cloud. Please note that a "SaaS" or "ASP" contracts are rather complex to write because it must relates to obligations that fall within different kinds of contracts (license agreement, TMA, information management, hosting, technical assistance…). - If the SaaS solution provider uses application modules that do not belong to him, one must make sure that the modules supplier(s) are contractually engaged over the whole period of his own contract.

<table>
<tr><th><b>1. Internal – Private Cloud</b>
<i>The company manages a Cloud for its internal use</i></th><th><b>2. External – Private Cloud</b>
<i>The company uses a Cloud managed by an external operator for its internal use</i></th></tr>
<tr><td colspan="2">RESPONSIBILITY</td></tr>
<tr><td>• Cover the risks of data misuse (for example: IT charter internal to the company, specific annex in contractual conditions of service purchase).
• Define means to identify responsibilities in case of data loss or alteration (traceability, control, audit…).</td><td>• Obtain guarantees from the operator or at least actions implemented to cover the risk of data misuse.
• Demand that responsibilities could be determined in case of data loss or alteration.</td></tr>
<tr><td colspan="2">PRICE</td></tr>
<tr><td colspan="2">• Make sure that prices/conditions are guaranteed over time (especially in case of the acquisition of the supplier by another…)
• Make sure that prices are based on an « on demand » use, which means that one can reduce the number of users and, as a result, costs (monthly, annually) if the activities justify it.</td></tr>
<tr><td colspan="2">REVERSIBILITY</td></tr>
<tr><td></td><td>• Formalize reversibility conditions</td></tr>
<tr><td colspan="2">PROPERTY</td></tr>
<tr><td></td><td>• Make sure of intellectual property of business processes and company's data in the Cloud.
• Have guarantees on property and data localization (in terms of country for aspects of regulation).
• Assess the impact of the Patriot Act in the case of an American service provider.</td></tr>
</table>

1. Internal – Private Cloud ***The company manages a Cloud for its internal use***	**2. External – Private Cloud** ***The company uses a Cloud managed by an external operator for its internal use***
B. SÉCURITY & RISKS	
DRP/BCP	
• Rethink and adapt DRP/BCP business processes internal to the company.	• Plan the DRP tests. • Rethink and adapt opening and flows synchronization processes as well as BCP job procedures internal to the company. • Note: Checking that a DRP/BCP can be implemented implies making sure beforehand that this is possible with the offered external solution.
GUARANTEES	
	• Have guarantees on closed flows reconstruction periods for externalized applications. • Reexamine constraints and recommendations from the CNIL regarding the externalized environment.
CONSTRAINS REGARDING THE SERVICE PROVIDER	
	• Demand that the service provider be certified ISO 27001 or label SAS 70 type II in order to guarantee users that all security requirements are respected. • Require from the service provider the list of all data storage spaces including back-up sites.

1. Internal – Private Cloud *The company manages a Cloud for its internal use*	**2. External – Private Cloud** *The company uses a Cloud managed by an external operator for its internal use*
C. HUMAN RESOURCES	
SKILLS	
• Need for rather technical, support and virtualization skills. Some skills can evolve from a technical operator profile to an analyst or automations developer profile. • Have business skills that allow understanding and anticipating needs and uses related to a Cloud, in order for instance not to appeal to an external Cloud.	• Even if technical and operations support skills are needed, a core of technical expertise must remain, especially in the framework of reversibility or of the beginning of DRP/BCP. • Reinforce skills in terms of contract, purchase and legal. • Focus on the business activities while keeping the key technical skills volume internal to manage remaining internal infrastructures and to ensure the interoperability between the external and the internal. • The involvement and especially the availability of users are essential during phases of parameter settings, acceptance testing and data migration. The deployment of a SaaS project without rallying clients that use the tool is doomed to fail. • In particular, the success of an SaaS solution deployment is proportionate to the commitment made in change management (information, training, communication, coaching…). • A supplier of a SaaS solution must have business skills related to the provided application, that is the real added value. The supplier must not only make a tool available to the client, he must as well bring « business » value allowing the client to automate and optimize processes. In some cases, the SaaS solution with added value (accompanied with services) can even meet

1. Internal – Private Cloud *The company manages a Cloud for its internal use*	**2. External – Private Cloud** *The company uses a Cloud managed by an external operator for its internal use*
	the needs of Business Process Outsourcing (BPO) for companies that wish to externalize all or a part of their business units (Finance, HR, Purchase,…). • Business skills of the service provider are very important in the phase of the tool parameter settings. This phase must not be neglected because it is the phase of the tool « design ». During this phase, it can be very useful to work on rationalization, standardization, or even optimization of existing business processes before rushing headlong into parameters setting.
ORGANIZATION	
• Please note that some Cloud solutions gather technical and financial responsibilities: a change in the Cloud can then immediately trigger a financial commitment. • Users' mobility is made possible by the services of a Cloud. It can affect employment contracts.	

1. Internal – Private Cloud ***The company manages a Cloud for its internal use***	**2. External – Private Cloud** ***The company uses a Cloud managed by an external operator for its internal use***
D. DATA & AUDIT	
Audit	
• No particular change compared to a traditional internal use.	• Plan conditions of security and service audit. • Plan in the contract a clause of technical audit and access to the service provider's premises.
Localization	
	• The Cloud operator must be able to provide information regarding data localization in the datacenters. • The operator must be able to guarantee risks of data misuse.
Responsability	
	• The operator must be able to determine responsibilities in case of data loss or alteration.
Data	
	• Make sure that the operator can guarantee the client company the preservation of intellectual property on business processes and client's data. • If personal data is managed in the supplier's servers, the client must act according to his obligations in the framework of the law of January 1978 entitled « Informatique & Liberté ». CNIL licenses are therefore essentials

1. Internal – Private Cloud *The company manages a Cloud for its internal use*	**2. External – Private Cloud** *The company uses a Cloud managed by an external operator for its internal use*
	(even in the case of an external private Cloud). • In those cases where data is stored in servers that are in countries outside the European Union, a specific license of data transfer must be requested to the CNIL. • Data migration: prepare data to be migrated but leave to the service provider the migration responsibility. "The devil is in the details "; and when it comes to migration, it is all about details.
E. INFRASTRUCTURES	
• The solution rests on the company's network. • The company must retain control of the Cloud solution integration in the existing infrastructure. • The company must retain control of the license pricing structure of the tools that constitute the Cloud.	• Keep watch over the IT network that gives access to the Cloud supplier: service quality, availability, measures… • Be able to cope with infrastructure upgrades that remained internalized, due to technical developments of the external Cloud (in particular regarding workstations). • Check to see who manages the Cloud infrastructure: the operator itself or one of his subcontractor. In the last case, ask for information regarding the contract between them.

3. Internal – Open Cloud *The company manages a Cloud open to external organisations or the general public*	**4. External – Open Cloud** *The company uses a Cloud managed by an external operator for a use regarding external organisations or the general public*
A. LEGAL	
CONTRACT	
• As the company offers a Cloud service, it has to wonder about the conditions of the service it offers. Are they part of a global offer or can they be negotiated?	• The conditions of the contract depend on the supply offer. They are difficulty negotiable. • The multi-device offer (especially regarding mobile tools) is often present to meet the needs of the market but it is not guaranteed that it is really part of the contract.
RESPONSABILITY	
• Detail the commitment of the company in terms of DRP. • Define properly the Cloud client's scope of responsibility in case of BRP/BCP. • During the negotiation of a SLA with the client, define, where required, the scope of the client's functional administration. • Define the publication conditions of the company's technical roadmap in order to allow clients to prepare and implement adaptations, where required.	• Providing a BRP/BCP implies making sure that it is possible with the offered solution. • As the company does not control the platform development, it has to be kept informed of the solution's roadmap in order to inform its clients.

3. Internal – Open Cloud *The company manages a Cloud open to external organisations or the general public*	**4. External – Open Cloud** *The company uses a Cloud managed by an external operator for a use regarding external organisations or the general public*
REVERSIBILITY	
• Define the supported formats for data restitution.	• Define the supported formats for data restitution. • Ensuring the client data reversibility implies making sure beforehand that it is possible with the external solution offered.
INTEROPERABILITY	
• Platform interoperability depends on choices regarding architecture internal to the company and must adapt to clients' needs. • The implementation of Open source solution in an internal Cloud requires defining an IT process, toward clients, in the licenses.	• Platform interoperability depends on the selected solution. • For an external Cloud, it is difficult to know whether Open source modules are implemented, which one they are, and what their license modes are. As a result, it is difficult to foresee impacts on clients.
PRICE	
• The company can define its pricing according to controlled criteria (investment, use, volume, service level, clients' needs etc.) but be aware of the pricing dependency with some supplier, especially editors of softwares containing the Cloud.	• The company that uses an external open Cloud is dependent on the prices of its Cloud operator. In the case where it offers an external service to the company, it may need to charge for it. Its price range will have to follow the one of its operator.

3. Internal – Open Cloud *The company manages a Cloud open to external organisations or the general public*	**4. External – Open Cloud** *The company uses a Cloud managed by an external operator for a use regarding external organisations or the general public*
B. SECURITY & RISKS	
AUDIT	
• An internal solution has to be auditable and submitted to intrusion tests.	
DATA	
• French law requires companies offering data storage space to know the data localization. • Wonder about the possibility of assuring the client that his data can only be reconstituted by him (to prevent access of a third person). • Traceability, archiving and reversibility must be ensured in terms of security. • Make sure of the compliance with regulations to the CNIL. • Guarantees that have to be offered to a client are those that would be required by the company if it relied on an external Cloud operator.	• French law requires companies offering data storage space to know the data localization. But when the solution is not provided by a French operator, data localization is not guaranteed. • The external solution must address the constraints of the CNIL. • The guarantee of the company access to the reconstitution of its data (to prevent access of a third person) depends on the selected solution. • Traceability, archiving and reversibility depend on the selected solution. It is difficult for a company offering the service to ensure them. • An external solution can be submitted to intrusion tests but is hardly auditable because data localization is hardly possible.

3. Internal – Open Cloud ***The company manages a Cloud open to external organisations or the general public***	**4. External – Open Cloud** ***The company uses a Cloud managed by an external operator for a use regarding external organisations or the general public***
C. HUMAN RESOURCES	
SKILLS	
• For an internal Cloud, skills are rather technical, support and virtualization. • Some skills can evolve from a technical operator profile to an analyst or automations developer profile. • Users' mobility is made possible by the services of a Cloud. It can affect contracts of employment.	• For an external Cloud, skills cover technical and support aspects, as well as purchase and legal.
D. AUDIT & DATA	
DATA	
• The company must be able to provide information regarding data (geographical) localization in its own datacenters. • Cover the risks of data misuse.	• Get information on (geographical) localization of data. • The company has to get information regarding means of action on the solution in case of data misuse.

3. Internal – Open Cloud ***The company manages a Cloud open to external organisations or the general public***	**4. External – Open Cloud** ***The company uses a Cloud managed by an external operator for a use regarding external organisations or the general public***
RESPONSIBILITY	
• The company is responsible in case of data loss or alteration. • Male sure of the conservation of intellectual property of the client's business processes and data.	• Get information on the company's responsibility in case of data loss or alteration. • Study the impact of the Patriot Act in the case of an American service provider. • Make sure of the conservation of intellectual property of the client's business processes and data.
E. INFRASTRUCTURES	
• Platform interoperability depends on choices regarding architecture intern to the company and may adapt to clients' needs. However, one must make sure to meet the simple standards of the market in term of access or exchange. • The multi-device offer (especially for mobile tools) is not easy to implement because it must be developed (there are many different devices and new ones regularly appear) and maintained over time (devices evolve very quickly).	

CONCLUSION

Cloud Computing is nowadays a key element in companies' digital transformation. It allows them to be cleared of technical constraints and gain agility and service adaptation to business needs. It also allows to efficiently address mobility's issue by providing an access to information and service everywhere.

Beyond the various definitions identified by the working group, which are essentials to exchange and facilitate understanding between the various stakeholders, the challenge of the IT Department is to know how to match the four typologies of Cloud Computing described in this report. Indeed, companies will have to, if it is not already the case, combine internal and external, close and open solutions.

In this patchwork of solutions which settle in the IT of the company, the added value of the IT Department is to introduce consistency into it, to architect services and to ensure a service quality that is both steady and similar externally and internally. It is also about perpetuating the IT infrastructure and architecture by developing it in order to cope with the evolution of the company's strategy and with its specific environment.

In this context, the IT Department role could move toward a role of « broker » that offers its own internal services and also encapsulate external services in order to integrate them and offer them internally. The difficulty lies in, by relying on relationships with even more matured jobs, how to foresee needs (a watch with Business Units is essential) in order to provide and integrate, if relevant, services while controlling security, interoperability, etc.

The challenge includes as well the establishment of a contract that, whilst protecting the IT and the company regarding its suppliers, ensures the preservation of the service on access, quality and data as well as reversibility; and this, beyond the contractual period (in the case of a change in the agreement, data must always be reachable as long as migration has not totally be done).

> *« … The emergence of cloud computing and its associated services constitutes a step-change that will deliver different economic models and new offers, which in turn will have a major impact on the information service ecosystem for companies… Cloud computing is a solution that must be integrated with existing Information System solutions. The IT function plays an ultimate integration role, uniting business processes with the other solutions comprising the IT application portfolio of the company as a whole. Cloud computing offers must therefore be interoperable, reversible and based on open standards. They must be an opportunity for companies to innovate, in terms of funding, sourcing, architecture, and above all, differentiated services… »*

The New Path to Digital Business – *Corporate Strategies and Culture (December 2010)* cigref

A network for large companies

CIGREF

21 avenue de Messine
75008 PARIS

FRANCE

Tel.: +33 1 56 59 70 00
Fax: +33 1 56 59 70 01

cigref@cigref.fr
www.cigref.fr