Cloud deployments through a tailored Multicloud Strategy
1.0 Summary

Cloud computing is much more than just a technological trend that is changing IT sourcing strategies. It is not only changing the way the corporations consume IT but also how they define their IT systems and even how they develop their software.

Since the outset cloud computing has been surrounded by buzzwords such as Software-Defined-Datacenter (SDDC) and Everything as a Service (XaaS). Providers offer their services according to different models, with the three standard models defined by NIST being: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). These models offer increasing abstraction; and as such, they are often portrayed as different layers in a stack: infrastructure, platform and application services.

In addition to this, depending upon the ownership and the exclusivity of the cloud usage, there are different deployment models:

- **Public cloud**: when the services are offered on a multi-tenant shared platform and rendered over a network.
- **Private cloud**: is cloud infrastructure operated solely for a single organization, whether managed internally or by a third-party, and hosted either internally or externally.
- **Hybrid cloud**: is a composition of two or more clouds (private and public) that remain distinct entities but are bound together, offering the benefits of multiple deployment models.

Enterprises want to avoid “vendor lock-in” and using different IaaS public services to meet the needs of different users. That is the reason why most enterprises use more than one cloud as strategy, what is now known as:

- **Multicloud**: is the use of multiple cloud computing services in a single heterogeneous architecture to reduce reliance on single vendors, increase flexibility through choice and mitigate against disasters. It
differs from hybrid cloud in that it includes multiple public cloud providers, rather than multiple deployment modes (public, private).

A key aspect to be considered when defining a cloud strategy is how the users will securely reach the different IT environments allocated in different clouds and how different environments interact in a reliable way. A combination of private communication services to public clouds and co-allocation of clouds must be considered in order to achieve the goal of having a truly hybrid or multicloud environment.

This paper focuses on how a cloud deployment through a tailored multicloud strategy can generate value to areas of the organization, that deploy applications in IaaS environments.

2.0 Cloud deployments through a tailored multicloud strategy

Market transformation, globalization, and the digital era are generating new business models and new ways of increasing the productivity of enterprises. Infrastructure as a Service has radically changed the way companies consume IT infrastructure, creating great opportunities for them but also bringing big challenges that will be discussed later in section 2.4.

IaaS cloud services has become a fundamental piece of the 21st century enterprise. Technology and Services are moving at a colossal speed and gathering internal knowledge and continuous adaptation has paramount importance.

2.1 The IaaS cloud journey

The origin of the term cloud computing is not clearly identified. But in the 1990s, telecommunications companies, who previously offered primarily dedicated point-to-point data circuits, began offering virtual private network (VPN) services with comparable quality of service, but at a lower cost. By switching traffic and securely sharing network elements, they could use overall network bandwidth more effectively. They began to use the cloud symbol to denote the demarcation point between what the provider was responsible for (shared infrastructure) and what users were responsible for.

In August 2006 Amazon Web Services (AWS) introduced its Elastic Compute Cloud and was the first cloud computing public service available. Microsoft Azure announced as “Azure” in October 2008 and was released on 1 February 2010 as Windows Azure, before being renamed to Microsoft Azure on 25 March 2014.

Users started using public cloud because they were looking mainly for faster time to market, cost reduction, scalability and flexibility.

Some years earlier, in 2003, and mainly targeting corporations that required a virtualization platform, VMware launched VMware Virtual Center, the VMotion, and Virtual SMP technology. That was the seed of the first corporate private clouds. Some providers started launching several IaaS services over VMware platforms during 2007 and 2008 to compete with the AWS offering.

Large corporations started to build their own private clouds looking for cost reduction vs traditional IT architectures, and more security, governance, performance and customization over public clouds.
When cloud computing first began to move from the cutting edge to the mainstream, business leaders were typically faced with two options: the private cloud or the public cloud. Initially, private cloud was the preferred choice in corporations, due largely to its superior perception of security capabilities. As time passed, organizations became more comfortable with the notion of the public cloud and its attendant cost-efficiency benefits.

**From public and private to hybrid cloud**

The term “hybrid cloud” is used loosely by vendors and providers and covers many different implementation models and architectures. Gartner defines hybrid cloud computing as “policy-based and coordinated service provisioning, use and management across a mixture of internal and external cloud services.” (Survey Analysis: Technology Trends in Workforce Management Applications, Sam Grinter, Ron Hanscome, Ranadip Chandra, November 2016)

Before designing hybrid architecture, an enterprise needs to ask themselves: “What capabilities do we need for integration across these different clouds?” It is obvious that having the same technology in the public and private cloud helps a lot (VMware, Openstack, Azure and Azure Stack, etc.), but the answer to this question is that there are many desired hybrid capabilities that you can take into account. Here are some examples:

- Single pane of glass management
- Network connectivity
- Workload motion across clouds
- Cloud storage/archive
- Identity federation
- Workload bursting
- Backup and disaster recovery
- API integration
The problem that business leaders face in this area is the simple fact that hybrid cloud environments are more complex than infrastructure strategies that rely solely on on-premise, private cloud or public cloud solutions.

**Figure 1**
Hybrid Cloud Concept

Source: Telefonica
**Multicloud strategy**

As customers began to consume services from different public cloud service providers, most organizations found that they were not able to properly manage it. Management became more complex, including governance, procurement, performance and cost management.

Therefore, it is crucial to start the multicloud journey by clearly defining the main objectives, rather than being blinded by new fancy features (which are not quite real today). Although there are several tools in the market that allow users to manage the main hyper-scalers and private cloud technologies, it is still an incipient and complex market with many features that have great potential, but are difficult to fully exploit in the current cloud arena:

- Single pane of glass management
- Image motion across clouds
- Identity federation
- Application catalog independent of the underlying infrastructure.
- Backup and disaster recovery enabler
- API integration
- Cost optimization
- Cloud brokering

**2.2 The cloud strategy benefits**

The adoption of cloud technology has firmly risen over the last decade. The discussion is no longer should it be cloud or not, but rather, “which cloud model should we adopt?” Businesses that want to use cloud computing have a choice to select a public or private cloud, a mixture of the two in the form of a “hybrid” cloud or go ahead with the next logical step adding a multicloud Strategy to their cloud deployment models.

Below we outline the most important benefits of each of them:
2.2.1 Public cloud

- **Faster time to market:** time to market is one of the features business managers are asking CIOs to tackle. As IaaS provides instant provision of its services, organizations can get the job done much more quickly.

- **Cost savings:** An obvious benefit of moving to the public cloud are the lower infrastructure costs. Large scales generate lower IT costs and that's why the IaaS providers can offer a competitive cost per virtual machine and per GByte. The pay-as-you-go model also provides significant cost savings. Consumption is metered and organizations only pay for the capacity needed at any given time. This method also allows them to avoid large fixed monthly or annual fees for services they may not use. The public cloud standard model demands no upfront charges, bandwidth utilization fees or minimum term commitments.

- **Scalability and flexibility:** One of the greatest benefits of IaaS is the ability to scale up and down quickly in response to an enterprise's requirements. IaaS providers have spare storage, servers and networking technology to accommodate the needs of their customers. This on-demand scalability provides added flexibility and greater agility to respond to changing opportunities and requirements. This is especially helpful in building and dismantling test and development environments, which greatly benefit from this increased speed and agility.

- **Support for DR, BC and high availability:** Whilst every enterprise has some type of disaster recovery plan, the technology behind those plans is often expensive and unwieldy. IaaS provides a pay-as-you-go disaster recovery infrastructure that is only chargeable if it is used.

In a nut-shell, public cloud is the most well-known and evenly-spread type of cloud computing, with the best economies of scale. It is typically a pay-per-usage model and the only costs incurred are based on the capacity that is consumed.

2.2.2 Private cloud

- **Costs reduction over legacy IT:** Using a cloud platform allows sharing IT infrastructure between several users/applications and so the cost of running a virtual server is much lower than a physical one. The main reason is to avoid capacity (CPU and Memory) vacancy.

- **Total Control:** Private clouds can be hosted either in-house or on in a third-party datacenter, giving organizations better control of data, users and information assets and allowing their IT department to intervene rapidly when changes are needed.

- **Enhanced Security:** As the cloud belongs to a single tenant, the infrastructure and systems can be configured to provide the levels of security needed by the owner of the private cloud. For example, in the case of a data breach, it may be almost impossible to access the internal logs from a public cloud.

- **Improved Performance:** Normally private clouds have customized oversubscription ratios which ensures the performance the user needs. All the resources are at the disposal of your organization alone.

- **High Customization Level:** A remarkable benefit is the level of customization that private cloud may offer. The hardware and software resources can be customized easily suit the variety of technical and business requirement according to the organization characteristics. For instance, you can choose a specific storage configuration, so that the system meets your individual needs.

We believe private cloud is here to stay, especially in large enterprises that have the human and economic resources needed to manage it. For some organizations, TCO can be more cost-effective in the long run than in public cloud usage. In addition, private cloud deployments may be used to achieve higher levels of performance and customization so may be suited to organizations with elevated concerns about security and control.

2.2.3 Hybrid cloud

- **Scalable and Cost-Effective:** Occasionally, applications demand peaks of additional resources that only occur from time to time. Instead of forcing organizations to invest in additional servers to withstand occasional bursts, organizations can leverage public cloud environments to offload these peaks, only paying for what they need, even if it is just a couple hours of cloud bursting. With less money spent on infrastructure, more IT budget can be used to other business critical concerns, instead of holding it back.

- **Architectural Flexibility:** Hybrid cloud allows customers to organize workloads as the situation mandates. This deployment style, with the mixture of public and private cloud gives customers the chance to explore the flexibility and scalability of the public cloud before selecting the best solution for them. Basically, customers are buying time until they find the best cloud solutions for their new applications.

- **Increased Compliance & Security over Public Cloud:** If there is institutional hesitancy about security concerns or the requirement to meet regulatory data handling standard in the cloud, hybrid cloud allows for specified workloads or sensitive data to be
isolated and secured on private cloud. This data can only be accessed on-premise or over a private network communication, whilst general purpose workloads or non-sensitive data can be publicly accessed through Internet.

- **Enabler for Disaster Recovery, Business Continuity and High Availability:** Public cloud provides a pay-as-you-go disaster recovery infrastructure that generates costs just when you use it, so a hybrid cloud implementation offers those capabilities too, addressing strategies not cloud capable but still reaping the benefits of the both worlds.

In summary, hybrid cloud solutions offer numerous benefits over purely private or public deployments. Foremost, hybrid cloud allows organizations to take advantage of the best aspects of each of these both worlds – the flexibility and cost-efficiency of public cloud, combined with the compliance, security, control and customization of private cloud.

### 2.2.4 Cloud deployments within a multicloud strategy

- **Avoid Vendor Lock-In:** The vendor lock-in problem in cloud computing is where customers are dependent on a single cloud provider and cannot easily move to a different vendor without high costs, technical incompatibilities or legal issues. With multicloud, customers operate with several providers mitigating the effects of vendor lock-in, to avoid being trapped when a provider changes prices, SLAs or even worst, goes out of the business.

- **Overcoming latency:** Latency is often reduced because the public cloud provider solutions are served from geographically disparate locations. Bringing the connectivity point closer to final users or the company core business IT systems acts as the most effective way to reduce the latency problem. For instance, an application that has different user access points located
in Latin America and Europe could have separate instances that serve those regions. In that case, selecting the right cloud for each geography might be the best approach, because the less distance your data has to travel, the better the user experience will be.

• **Risk mitigation**: An effective multicloud strategy allows customers to spread not only critical workloads, but also risk across multiple cloud environments. This includes accessible redundancy, improved disaster recovery options and fewer single points of failure. Every action counts against downtime, application outages and data loss, as well as data breaches and attacks. While outages do not occur often, they can cause major disruptions when they do. A multicloud strategy can help you mitigate it by not putting all of your eggs into the same “cloud” basket.

• **More choices and flexibility**: It is clear that every cloud provider has different features, strengths and weakness. From a technology point of view, some align better to particular customer needs than others. Customers may opt for a multicloud strategy in order to leverage the best-of-breed advantages of each provider and avoid the weakness of a particular one. To ensure that you have the very best services that will maximize the performance of your application, using multiple cloud providers may be the best course of action...

A properly adopted multicloud strategy delivers a mix of benefits that enables companies to create the best cloud solution for their business. It can be a facilitator to minimize vendor lock-in, a manner to avoid single points of failure and downtime, or simply a mechanism for consuming unique innovations and features from multiple vendors taking advantage of the best of what each cloud offers.

In conclusion, The beauty of cloud deployments through a tailored multicloud strategy is that there are
many combinations to choose from, meaning every customer can find a solution that meets their specific needs taking the advantages of private deployments and the particular strengths of each public cloud service provider.

Table 1 – Benefits Summary

<table>
<thead>
<tr>
<th>Benefits</th>
<th>Public Cloud</th>
<th>Private Cloud</th>
<th>Hybrid Cloud</th>
<th>Cloud Deployments within a Multi-Cloud strategy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Faster time to market</td>
<td>Costs reduction over traditional IT</td>
<td>Scalable and Cost-Effective Architectural Flexibility</td>
<td>Avoid Vendor Lock-in</td>
<td></td>
</tr>
<tr>
<td>Cost savings</td>
<td>Total Control</td>
<td>Increased Compliance &amp; Security vs. Public</td>
<td>Overcoming latency</td>
<td></td>
</tr>
<tr>
<td>Scalability and flexibility</td>
<td>Enhanced Security</td>
<td>Enabler for DR, BC and high availability</td>
<td>Risk mitigation</td>
<td></td>
</tr>
<tr>
<td>Support for DR, BC and high availability</td>
<td>Improved Performance</td>
<td></td>
<td>More Choices and Flexibility</td>
<td></td>
</tr>
<tr>
<td></td>
<td>High Customization Level</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>


2.3 Architectures

Customers have at their disposal various options available to select their cloud architectures. Organizations must design smart architectures, with applications hosted and interconnected in a hybrid mesh of public and private cloud services. The first question arises: “What is the best option for our organization?” There is not one simple answer. It depends upon the workload characteristics, business needs and grade of maturity of their cloud computing journey.

There are 4 essential components in any multicloud architecture:

• Technology silos to host every particular application and data.
• Integration levels across technology silos.
• Mechanism to interconnect the different silos.
• Management requirements to access, measure and control the silos.

Gartner defines “technology silos” as different locations where applications, services and data can be hosted (Hybrid Architectures for Cloud Computing, Alan D Waite, June 2016). Depending on the individual workload requirements, organizations must select either one silo or a combination of them:

Once the selection is made, the next question for designing the architecture is: “What are the appropriate integration levels across these silos?” There are 3 different levels of integration between the silos: Infrastructure/utilities level, virtualization level and application/data level.

Figure 3
Integration Levels

Each one of them includes hybrid capabilities that allow users to successfully achieve the integrations between the silos such as: APIs or Data Integration in the Application layer, workload bursting and container/VM orchestration in the virtualization layer or network connectivity and Identity/Access in the infrastructure layer.

Thus, network connectivity is also considered an integration capability at the hardware level, but because of its special importance, it is worth treating it separately. This leads to the next question: “What interconnection mechanism should we use across these silos, user locations and company facilities?” The answer to this question is dependent upon the individual customer needs.

Organizations could have different needs in terms of communications systems across their assets such as: security, performance or bandwidth elasticity. So, it would be necessary to select the “interconnection mechanism” in any case.

Basic Connectivity Services, as VPN MPLS, are still an option but they were not created with cloud connectivity in mind and may not always provide all the required features. For example, functionalities specifically designed for the cloud world like bandwidth on demand, the feature making it possible for a customer to adapt the bandwidth of its VPN service in real-time, is a must-have characteristic of a VPN service used to connect to any cloud.

Nevertheless, we must not forget that this basic connectivity is the pillar that enables Advanced Connectivity Services and new value-added services that bring organizations closer to the cloud world.

Other network services can be grouped under the term Advanced Connectivity, each being able to be deployed on top of the physical network, such as:
• **WAN-to-Cloud**, to obtain a fast and secure private connectivity to cloud-based platforms and business applications. Cloud service providers offer APIs to integrate the delivery and some management features with the telcos WAN-to-Cloud services. In the near future, the Wan-to-Cloud services will offer APIs too and the customer will be able to manage all these services and integrations with an unprecedented flexibility.

• **Software-defined WAN (SD-WAN)**, running as an overlay service over any available basic connectivity services or physical infrastructure. This way, it is possible to deploy virtual paths between the branches of a corporation with just an IP link.

• **Virtual Remote Access (vRAS)**, providing a secure extension of the corporate WAN on a public network, granting a protected access.

Last but not least, **Value-Add Connectivity Services** improve capacity, flexibility, security and cost-effectiveness. These services range from network features customization, like Bandwidth on Demand (BoD) to Virtual Network Functions (VNF). With Bandwidth on Demand, bandwidth for a given branch is changed by the user, specifying its increase and duration. In addition, typical VNFs are, for instance: Clean Pipes as a virtual next generation firewall, provides whole threat protection over internet access services or Virtual WAN Optimization Service (vWOS).

IT departments in big enterprises usually base their strategy around security, cloud/platforms and network/connectivity. While this kind of organization has been successful in the past, the explosion of cloud and new network services require a more holistic approach that takes into account the whole picture; there are three main reasons behind this:

• Cloud is part of the network. Applications are no longer at the customer’s datacenter; almost all companies have moved some or all applications to the cloud that have changed the flow of traffic. It is estimated, that at least 50% of MPLS networks traffic has internet as its destiny.

• Security requires an end-to-end approach. Security has not been simplified to isolated elements; it requires a whole approach that embraces private network, public network and cloud to identify the potential risks. Moving to an automated ecosystem can take advantage of consistent security policies across the whole solution.

• Having the visibility end-to-end of all communications and cloud services and the self-management of those services at the tip of your fingers is definite ‘must-have’ a XXI century CIO. This new approach creates an interesting ecosystem that could help to maintain consistency across the entire company through API integration.

The last question that arises here is: “What are the management options available across these silos?”

---

**Figure 4**

**Interconnection Mechanisms**

![Interconnection Mechanisms](source: telefonica)
In an early stage of multicloud adoption, organizations began to consume services from each cloud provider and manage every silo with each provider’s tools. So, in this scenario the management layer sat individually over each silo.

At this point, organizations realized that operating multiple technology silos, involves facing new operational challenges regarding controlling cloud deployments and monitoring cloud consumption. As such, some organizations are evolving their multicloud strategy and deciding to embrace sophisticated cloud management platforms (CMP). This gives them the ability to see the entire functionality of the cloud provider and helps to manage each cloud service without the need for multiple tools for the different cloud services within a “single pane of glass”.

However, it is a well-known fact that multicloud tools cannot totally address all of the features of the detailed management for each cloud. There may also be capability gaps to certain silos that must be managed manually, meaning the individual provider tools are usually still in use as well.

### 2.4 Main challenges for enterprises in the cloud world

We have seen the array of benefits that cloud deployments through a suited multicloud strategy can provide to today’s enterprises, but there are also some challenges to be faced during this transformation journey:

- The proliferation of hyperscale IaaS offerings are generating competition and a cost reduction and time-to-market pressure to internal IT services.
- Some internal users are purchasing IaaS services with a credit card without any control by the IT Department (shadow IT). This generates security challenges and also hinders an efficient management of the IaaS providers.
- The location and communication services used to reach the public clouds are key aspects that have to be considered in order to avoid legal problems and strategic issues. Enterprises should know which legal and strategic requirements their IT systems require to be able to choose the best cloud option for them.
- Some legacy systems cannot be moved to the cloud because of their technical architecture. In those cases cloud users need to co-locate these legacy systems as close as possible to the clouds they need them to interact with.
Employees with a deep knowledge in different technologies are needed to manage these complex multicloud and hybrid IaaS environments. There are Cloud Management Platforms (CMP) available on the market which help to manage different clouds from a single plane of glass, but it is not easy to find or hire the employees with the knowledge needed to manage those multicloud and hybrid environments.

And the obvious questions are:

- How should we manage this transition?
- Should we do it by ourselves or look for a partner?
- Is it better to have a single partner or lots of them?

There are no specific answers to these questions and it is only once an enterprise has a deep understanding of their internal capabilities and limitations that these questions can be properly answered.

2.5 Managing the hybrid-multicloud

Whilst using multiple clouds is attractive, initializing the solution and managing such an environment can be challenging. It is crucial to ensure organizations not only use the best of breed Cloud Management Platforms (CMP) but also they use them in the right way without increasing the management complexity and cost.

A Cloud Management Platform is a suite of integrated tools that provide automated management of private and public clouds. They are fast becoming the critical component for successfully leveraging multicloud strategy.

In reality, however, only a few vendors can deliver a comprehensive functionality. Having good cloud partners with knowledge of the different pieces of the cloud architectures, will help to reduce the challenges and increase the multicloud strategy benefits. Therefore, many organizations are turning to a managed cloud services provider to assist them with their multicloud solution.

2.6 Use cases for public, private and hybrid clouds

Enterprises must determine the IT solution that suits each application: on-premises, private cloud, public cloud, or hybrid cloud. Below we outline some basic considerations and cloud comparisons, as well as best practices for how to integrate and manage these complex deployments.

Applications that are especially well suited to the public cloud:

- Any IT system that is sporadic or highly seasonal.
- Any new application whose demand is uncertain, especially for microsites or other interactive properties for marketing and ad campaigns.
- Test environments, due to the fact that it is so much easier to spin up and down instances for load testing.
- Cloud native applications developed specifically to be run in a cloud.
- Long-term storage, including tape storage, which has significantly more cost-effective solutions in object storage services.

But in some cases there are indicators that your application would be a good candidate to remain in a private cloud:

- If there are any regulations that do not allow you to move data to a public cloud (in some cases there is no public cloud node in the country you are based in).
- You are using any software that requires (by technical or licensing reasons) dedicated infrastructure for compliance.
- You need high and predictable performance.
- The application has very predictable usage patterns and low infrastructure costs.
So far we have reviewed separately the most common use cases for both private and public cloud. But which ones are more appropriate for a hybrid cloud deployment? Here are the most common:

• Using the public cloud as a disaster recovery platform of the private cloud.

• Implementing high availability solutions using public and private clouds.

• Test and development environments (allocated in public clouds) with high flexibility needs of instances running on private clouds.

• Private cloud applications with bursting demand that can move load to public clouds.

Adding a multicloud strategy to a cloud deployment generates advantages in some cases:

• When it is a requirement to use and manage different public cloud services from a single pane of glass.

• Environments with elements that run better or at lower costs in different public cloud providers.

• You want to manage and reduce cloud costs with cloud brokering actions.

Finally, sometimes no cloud fits the use case. Here are some situations where on-premises legacy infrastructure might work best for your application:

• The cost savings of cloud resources do not significantly outweigh the costs in on-premise solutions.

• Your application already sees high performance and high availability from current infrastructure.

• An application is poorly written and infrequently used, and therefore not worth the effort of migrating to any cloud.

### Figure 7
**Suitable Use Cases**

<table>
<thead>
<tr>
<th>TECHNICAL AND ARCHITECTURAL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specialty Hardware or Configuration Requirements</td>
</tr>
<tr>
<td>Low Latency</td>
</tr>
<tr>
<td>Workloads with High Availability and Disaster Recovery</td>
</tr>
<tr>
<td>Tier Deployment (Front End - Backend)</td>
</tr>
<tr>
<td>Supplementing private cloud resources</td>
</tr>
<tr>
<td>Cloud bursting</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>APPLICATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical Applications possible to scale</td>
</tr>
<tr>
<td>High performance and availability to meet demanding SLAs</td>
</tr>
<tr>
<td>Cloud Native applications</td>
</tr>
<tr>
<td>Legacy Applications</td>
</tr>
<tr>
<td>Single application development and testing</td>
</tr>
<tr>
<td>Life-Cycle deployment (across clouds)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SECURITY AND COMPLIANCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ease auditing (performance, configuration, operational and billing data)</td>
</tr>
<tr>
<td>Governance or Regulatory Requirements</td>
</tr>
<tr>
<td>Makes resources available across multiple business units that need isolation</td>
</tr>
</tbody>
</table>

Source: Telefonica

### 2.7 How Telefonica can help enterprises with a multicloud strategy

A multi-cloud strategy presents both opportunities and challenges for all businesses. Having a clear and complete multicloud strategy means matching the existing IT systems to the different clouds available to the enterprise, define how they will interact and plan how the business will reach that end goal.

Historically, the main issues around exploiting the benefits of public cloud were security concerns and the interoperability with private or legacy systems. Being able to collocate the private environments as close as possible (in terms of latency) to the public clouds is possible through some providers today, but alone it is not enough. Enterprises need to connect to hyper-scale public providers (with no colocation services in the same datacenter) and also to connect to their on-premise datacenters, branches and headquarters. That's why a Telco operator, with a complete cloud offering combined with cloud-ready comms services, is the perfect partner to offer an end-to-end multicloud solution to any business.

Telefonica, with a powerful cloud presence in Spain and Latam plays a key role in being able to offer an end-to-end multicloud strategy proposal to our customers. We offer hosting services where customers can allocate their private clouds and legacy systems; in which any of our datacenters has at least one public cloud IaaS offering (Openstack and/or VMware based) and can be hybridized with a customer’s own private cloud. In our portfolio we also have the Azure and AWS IaaS services with design and migration functions that can be included in a multicloud service with a single-pane-of-glass customer portal. And as a Telco operator, it is able to connect all of these pieces to a customer’s private network safely and reliably.

Source: Telefonica
After 10 years, confusion still exists regarding cloud computing. This guide will help CIOs understand why and how cloud as a style of computing should be exploited and why they need a cloud strategy.

**Foundational Document**

This research is reviewed periodically for accuracy. Last reviewed on 27 June 2017.

## Key Challenges

- After 10 years, cloud computing is still perplexing to many CIOs; thus, it is not being exploited for its maximum benefit.

- While cloud computing is a foundation for digital business, we estimate less than one-third of enterprises have a documented cloud strategy.

- Pursuing cloud computing as a style of computing without optimizing application design, management and governance can result in sprawl and cost overruns.

- Many CIOs lack a decision framework to prioritize legacy applications movement to an optimized cloud style of computing.

- No standards address migration between cloud computing suppliers; CIOs that desire reduced lock-in to cloud service providers must explicitly include it as part of the cloud strategy and execution.
Recommendations

• Leverage your digital business strategy to justify your cloud strategy and investments.

• Exploit and optimize a cloud style of computing for new applications, and identify which legacy applications should move to an optimized cloud style of computing.

• Invest in architecture/standards and cloud infrastructure/platform product management roles/skills to succeed with cloud computing and achieve your agility, speed, innovation and cost goals.

• Productize application and infrastructure functionality to enable internal consumers of cloud services to help themselves to IT (through self-service), while reducing associated risks through application of standards, policies and embedded management/security.

• Develop a cloud strategy so that decisions do not have to be re-evaluated and analyzed with every new project/product, thus increasing enterprise agility and productivity.

Introduction

Even 10 years after the introduction of public cloud computing services, and five-plus years of private cloud services, confusion remains over where and how to exploit these services. This document provides guidance to CIOs on the development of a cloud strategy and how to maximize the benefits of cloud computing for your enterprise.

The Multiple Faces of Cloud Computing

CIOs should recognize that we are in a period of slow migration of value from on-premises data centers to the public cloud. While public cloud spending today is a relatively small 5% as a proportion of total IT spend, it will grow at an average compound annual growth rate (CAGR) of 15.8% through 2020, which is much higher than IT budget growth. Public cloud growth is due to new initiatives as well as migration of existing legacy systems.

A key benefit of public cloud infrastructure as a service (IaaS) and platform as a service (PaaS) is to place applications closer to customers to enable better user experience. This is particularly important for enterprises with worldwide customers that have consolidated their data centers in a
few locations to save money. As a result, much of the new customer-facing cloud-style applications being built are for the public cloud. Enterprises with a high need for private cloud computing are making greater use of colocation facilities for the same reasons.

Additional reasons for the rise in public cloud computing are:

- Offloading existing highly customized and expensive-to-operate applications to SaaS can concentrate limited or constrained IT skills on more differentiated services and capabilities.

- Public cloud providers are increasingly abstracting and making it easier and faster to build new application functionality, which makes public cloud providers attractive to leverage for digital business opportunities. At the same time, it is more difficult to build the same type of capability internally with the same level of innovation.

- New application development, especially if it’s experimental or has unspecified demand or an unknown knowledge of success, will often be performed in the public cloud. This is due to lack of desire to invest capital in an unpredictable project. Once the endeavor becomes predictable and productized, decisions on public versus private cloud can be re-evaluated.

- Some IT organizations seek to replatform as much as possible to the public cloud in their effort to divest something they see as commodity: data centers, racking/cabling infrastructure, etc. This enables the limited or constrained IT skills to focus on higher-order delivery closer to business value. Private cloud computing is also being exploited, especially where intellectual property (and the desire not to share infrastructure), control, regulatory or compliance concerns, security, performance, and cost of service delivery are differentiated. In those cases, private clouds that run on-premises, in colocation facilities or at provider facilities can offer some of the same benefits as public cloud computing. It should be noted that enterprises with successful self-built private cloud computing are highly skilled and tend to be Type A enterprises. In addition, distinctions about public versus private cloud are increasingly becoming blurred as public cloud providers have added a portfolio of virtual private cloud options with more isolation and dedicated resources at higher costs.

*Private cloud computing is also being exploited, especially where intellectual property (and the desire not to share infrastructure), control, regulatory or compliance concerns, security, performance, and cost of service delivery are differentiated. In those cases, private clouds that run on-premises, in colocation facilities or at provider facilities can offer some of the same benefits as public cloud computing. It should be noted that enterprises with successful self-built private cloud computing are highly skilled and tend to be Type A enterprises. In addition, distinctions about public versus private cloud are increasingly becoming blurred as public cloud providers have added a portfolio of virtual private cloud options with more isolation and dedicated resources at higher costs.*

*Private to public cloud is a gray spectrum of choices, with a range of isolation options for internal or external delivery. Ultimately, value will be derived from selecting the appropriate style of cloud computing that works for each given organization.*

Gartner defines hybrid cloud computing as the coordinated use of cloud services across provider boundaries among public, private and community cloud service providers. Hybrid cloud computing implies significant integration between the internal and external (or two or more external) environments at the data, process, management or security layers. Nearly all enterprises will exploit public, private and hybrid cloud computing, especially for their digital business needs. As they expand cloud usage, many will engage in the use of managed service providers/cloud service brokers that will help them to aggregate, integrate and customize cloud services, and serve as an intermediary between cloud providers.

**Analysis**

**Justify Your Cloud Strategy and Investments Based on Your Digital Business Strategy**

Digital business requires speed and agility, both to trial and advance new ideas, but also to continually enhance digital business products and services. A cloud style of computing provides speed and agility through the use of cloud services — which become available to a broader set of users (also called cloud consumers) through a self-service interface. As users “help themselves” to these cloud services, it has the effect of democratizing IT, which in turn spurs creativity and innovation. Examples of cloud services that can be self-requested include applications (SaaS), platforms (PaaS) and infrastructure (IaaS).

Before cloud computing became available as a style of service, most users were required to make specific requests to the IT organization to access computing resources (applications, platforms and infrastructure). This often took days to months, depending on the complexity of the request and the number of handoffs required to complete the request. With cloud services, however, users can have access and get resources immediately.

Cloud computing further increases the speed of development and time to market because cloud services are available through APIs, which enable developers to programmatically access cloud services for even faster and more repetitive access. Moreover, these APIs support continuous integration and delivery, the foundation of agile methodology and DevOps methods commonly used for digital business and most new software development. Even if you use...
packaged applications, your vendors (of both SaaS and on-premises software) have or are enabling API access so your developers can more easily integrate functionality and data through APIs.

Gartner has written about the economics of connections that will increasingly define new business models that are more ecosystem- and platform-based. Exploiting these new business models requires the ability to reuse not just your own application and data assets but those of others in your ecosystem. Marketplaces will be established to sell and source various assets (such as data, analytics, functionality and events). Sourcing these assets offers connection to them via APIs that have defined functionality and SLAs, and have been written in the cloud style of computing so the APIs accessing the functionality can scale with increasing demand.

As a result of these benefits, cloud computing is the foundation of digital business initiatives. Yet in our most recent 3Q15 cloud survey, 42% of the more than 6,700 responses indicated their organizations hadn’t used or planned to use any form of cloud services by year-end 2015 (see Figure 1 and Note 1).

**Recommendations:**

- Educate your CEO and board of directors about the need to invest in cloud computing as a style of computing that drives greater speed, agility and innovation through the democratization of IT. It’s not a “keep the lights on” play.

- Use your digital business strategy to justify the investments needed for cloud computing. In our latest CEO survey, CEOs expected 46% of their revenue to come from digital business by 2019.

- If you are not using cloud computing (as 42% were not in our latest cloud survey — see Note 1) you’ll need to experiment with public, private and hybrid cloud services. Experimentation is required so that you get a better understanding of the value cloud computing can provide to your organization, which is an important aspect of the future development of your cloud strategy. Engaging managed service providers/cloud service brokers can extend your skills and reach, and reduce the time to take advantage of cloud services.

**Using Cloud Services Is Not Enough: You Must Optimize Your Application Design**

Cloud services drive speed and innovation through broad and easy accessibility. Offering cloud services make your developers more productive and can improve time to market. But the way you use cloud services matters: Developing your applications in a “Wild West” style where “anything goes” can result in costly sprawl, lack of leverage and high cost maintenance, resulting in significant technical and architectural debt. This is true for all types of cloud

---

**Figure 1**

Cloud Survey Results: 58% Use or Planned to Use Cloud Services by Year-End 2015

<table>
<thead>
<tr>
<th>Has your organization deployed or does it have plans to deploy any cloud service?</th>
</tr>
</thead>
<tbody>
<tr>
<td>n = 6,723</td>
</tr>
</tbody>
</table>

58% Using cloud services by end of 2015

- Plans to deploy by year-end 2017: 13%
- Currently uses cloud services: 35%
- Plans to deploy by year-end 2015: 23%
- Plans to deploy beyond 24 months: 6%
- Does not have plans: 23%
- Still has no plans to use cloud services: 23%

Source: Gartner (July 2016)
services in use. In other words, cloud services can enable agility, but you don’t get it unless you optimize your applications for cloud computing with the explicit purpose of getting the most value (speed, agility) at the lowest effective cost. What does this mean?

**Optimized Cloud-Based Applications Leverage “Service-Oriented Architecture (SOA) on Steroids”:**

Most new applications are being built with cloud as a style of computing through the use of IaaS and/or PaaS, such that they share computing resources, and have the opportunity to be scalable and elastic. But there is something more. First, to reach the level of agility desired by product teams, as much functionality as possible needs to be reused. Of course we have been talking about and implementing SOA for years, but a cloud style of computing is “SOA on steroids.” Cloud computing makes development of new applications more composable, from existing components/functions. As a result, they can be more quickly prototyped and developed, usually at a lower cost, and the teams can be more productive by focusing on new functionality and leveraging existing functionality. This encourages reuse.

*Without reuse, cloud-style applications would be just one more method to generate architectural and technical debt, thus reducing productivity, increasing costs and slowing innovation and releases.*

**Cloud-Based Application Composability Requires Standards:**

To get the maximum reuse with optimized service delivery costs requires standard configurations of software infrastructure components. Without such standards, your cloud-based applications would end up in a similar situation to that of most legacy applications — hundreds or thousands of applications each with different nonstandard components resulting in high costs and low reuse — ultimately reducing, not increasing agility. To get the agility promised by cloud services requires a focus on enterprise architecture and standards.
Cloud-Based Application Design Is Different:

- Cloud-style applications are stateless, meaning they can fail and restart easily, and they can scale dynamically based on increasing or decreasing demand (often called elasticity), thus automatically achieving service levels at reduced cost of operation. (For more information, see Note 2.)

- The cloud style of applications requires the solution architects to design the application to accommodate and respond to failing infrastructure. Resiliency must be explicitly designed by the solution/product teams or embedded in infrastructure policies, which are abstracted from the developers/engineers and applied automatically, driving greater productivity for the product teams.

- Optimized cloud-based application design embeds manageability and security in the application itself rather than performing most of it on the outside and after the fact — as most traditionally built applications do. There is a greater attempt to monitor, analyze, test and forecast potential missed SLAs with dynamic actions taken for correction. For example, monitoring is embedded and linked directly with autoscaling (to scale up or down the resources to meet SLAs). Replication and backups are also embedded, and typically based on policy determined by the type of application, criticality and regulations. Even patching is often done differently, based on an update of the image or configuration, and the orchestrated removal/replacement of the nodes (because they are stateless), rather than applying patch changes online.

The net effect of these design changes, if well-executed, is that cloud computing brings more than agility: It can also lower the cost of building and operating cloud-based applications, assuming the proper operations principles are applied. If you lack optimized cloud service operational and security management skills, managed service providers/cloud service brokers can help to fill the void and encourage good tenant practices, such as turning off cloud instances when they are not in use to reduce undue cost and waste.

**Reuse of standard functionality and infrastructure, embedding manageability and security, and applying greater automation of the build and run processes, offers both agility and cost optimization benefits.**

**Recommendations:**

- Establish a cloud strategy and architecture group with a multidisciplinary focus, including lines of business, enterprise architecture, cloud subject matter experts, sourcing, and infrastructure and operations (I&O), to develop cloud-optimized application design principles and standards.

- Productize application and infrastructure functionality, easily enabling cloud consumers to help themselves to IT (through self-service) and simultaneously encourage reuse, but reducing associated risks through application of standards, policies and embedded management/security. This will require new roles/skills in cloud product management for the various components that will be offered as productized cloud services.

- When establishing architecture standards for cloud-based applications, be sure to establish management and security standards that can be included in every initiative, which will have the effect of reducing risk and increasing product development productivity.

- Consider contracting for managed services/cloud service brokerage capabilities to enable skills transfer and shorten time to value for optimized application design for cloud computing.

**Use a Pace-Layered Application Strategy as Input to Your Cloud Strategy**

CIOs need to determine where and how to leverage cloud computing for business benefit. A different cloud strategy is often made for existing (legacy) applications versus newly developed applications. Gartner’s Pace-Layered Application Strategy and bimodal research can be used to help guide your cloud strategy (see Figure 2).

Driving innovation associated with digital business is a key requirement for today’s CIOs. Much of these innovation initiatives will require shorter cycle times to develop many prototypes for testing, but with fewer resulting developed capabilities (because many prototypes will fail to meet business needs). Most innovation initiatives and their associated software development are exploratory in nature and require a different work style, and a differentiated approach to governance that reflects a different set of risks and a need to manage higher uncertainty but with faster speed. We call this work style and associated governance Mode 2. As a rule of thumb, the applications associated with innovation initiatives will be developed with an optimized cloud style of computing as the new architecture (see Figure 2). Often, these “greenfield” applications are being developed in the public cloud (for reasons cited earlier in the introduction).

Where justified, existing systems of record applications (for example, longer-lived transactional applications) are also getting partially or fully refactored or replaced for an optimized cloud style of computing to
support the digital business strategy. Doing your own refactoring (versus replacing the applications with SaaS or an optimized release from your packaged application vendor) can take a considerable amount of time and money, especially for complex and monolithic applications. Assessing what to do with systems of record such that they have the flexibility needed to collaborate on digital business initiatives is a core requirement for CIOs and enterprise architects to address.

For most organizations, only a portion of legacy will be refactored. Existing applications that are not moving to SaaS often get onboarded to the private cloud because of their intense integration with other applications. With systems of innovation often in the public cloud and systems of record often in the private cloud, most enterprises will pursue hybrid application integration strategies.

**Replace and Refactor Systems of Record to Ready Your Digital Business Platform**

It will make sense for some existing applications to be replaced, through SaaS or the acquisition of packaged software capabilities to modernize the applications and lay the foundation for the digital business platform. However, not all applications can or will be acquired on the open market; some custom applications will need to be refactored for the cloud style of computing to enable them to participate in the digital business platform. Prime candidates are those that require increased change frequency or the need to integrate with new systems of innovation and differentiation to drive digital business initiatives. Another consideration is their variability in demand. If the variability is great, then it makes sense to refactor the application so that it can use the resources it requires to meet the SLA, rather than require extra resources applied round the clock whether needed or not. Refactoring an application with high variability in demand will have the effect of reducing the cost.

- In the public cloud, refactoring such applications enables elasticity, applying just the right amount of infrastructure resources to meet the demand, which reduces direct operational costs because you pay for what you use. If you move your monolithic applications “as is,” you will have to size them for peak demand in the public cloud and therefore incur significantly higher costs. That said, sometimes migration to the public cloud is justified as a form of consolidation, after which the refactoring can be accomplished. Depending on your cloud strategy, you may continue to operate the new cloud optimized application at the chosen public cloud provider, or migrate to a different provider or to private cloud providers.

- In the private cloud, refactoring such applications in combination with the use of dynamic optimization technologies results in increased asset utilization (thus delaying capital cost outlays). Dynamic optimization technology is a capability that uses telemetry, algorithms, service and resource analytics, and policies to drive
When refactoring these applications, it is critical that they be done with the new architectural standards so they too receive the benefits of increased speed (of change, composability, and so on) and lower cost of operation as well. Refactoring legacy applies to networking as well. Enterprises that use a significant amount of public cloud computing will need to rethink their network architectures to drive the speed and agility they seek, but this cannot be delivered with point-to-point networks to all providers.

From a customer perspective, the most aggressive stance we’ve seen is a plan to refactor all existing legacy applications over a five-year period for an optimized cloud style of computing. This decision was driven by the need for innovation (for example, legacy was holding the enterprise back from the speed needed to drive digital business initiatives), as well as the desire for a serious reduction in cost of application operations. In this particular example, monolithic legacy architectures were holding back innovation because of their difficulty and elapsed time to change them due to the considerable risk management required. This company’s digital business initiatives depended not only on new development (in an optimized cloud style of computing), but also on the ability to integrate with systems of record applications and to enhance application functionality (see the A section below). Look Into the Future of Technology

• Don’t forget to apply refactoring to infrastructure initiatives — particularly networking — to enable you to achieve your hybrid cloud architectures speed/latency requirements in a cost-efficient way.

Recommendations:

• For packaged applications, rely on your vendors to migrate to a cloud style of computing or move to a SaaS offering, replacing your on-premises implementation.

• Determine and prioritize which existing applications get moved to SaaS or an on-premises optimized cloud style over a specified time period.

• Determine and prioritize which existing applications are funding for refactoring over a specified time period.

• Prioritize legacy rearchitecture for the cloud based on the need for increased change frequency, the need to integrate with systems of innovation/differentiation, and costly variability in demand, which could be lessened through elasticity.

• For legacy applications that need integration to systems of innovation/differentiation but will not require frequent changes, enable their functionality and data via APIs.

• Choose IaaS and make use of API abstraction layers that allow you to manage and operate many public clouds as if they are one.

• Engage cloud service brokers/managed service providers that have the potential to minimize the impact of lock-in through their partnerships with multiple cloud service providers.

• Increased use of container models and microservices has the potential to provide greater choice in how, where and when to deploy application functionality (see the A section below).

• Some providers of technology components such as networks, security and PaaS software offer cloud-agnostic capabilities, meaning they can operate either in the public cloud or the private cloud in the same way. When operating in the public cloud, they replace the public cloud provider’s functionality with their own. This has the effect of reducing lock-in with the public cloud provider but moves the lock-in to the technology provider and limits the use of public cloud services that are being frequently enhanced.

CIOs: Beware of Lock-In to Cloud Service Providers/Services

CIOs and CTOs/architects must determine strategically what degree of vendor/technology lock-in is acceptable to public cloud service providers, especially since there are no public cloud standards. Cloud services can come with a significant degree of lock-in due to the lack of standardized IaaS APIs, data structures for SaaS data, and tools/languages for PaaS. This can become a problem if the selected provider exits the market or when a relationship must end for other reasons — like lack of innovation, price increases, or inability to deliver on SLAs. However, while fear of lock-in is often mentioned as a concern, we find that migration across different cloud provider services for the same capabilities is rare. The focus should be on value derived from the services. This will either validate or eliminate a provider from contention for a given solution. Further, since cloud computing is not a “stack” of service (for example, SaaS is not always built on PaaS, which is not always built on IaaS), one must consider the value of a service at each level.

Considerations when lock-in is a concern:

• Determine and prioritize which existing applications are funding for refactoring over a specified time period.

Real-time automated actions that reduce waste, cost and risk exposure, while simultaneously improving service levels. These technologies help reduce cloud service and virtual infrastructure sprawl and cost, while improving governance and compliance.
The right strategy is the one that is right for your enterprise based on the value you seek to derive from cloud services.

A Look Into the Future of Technology

One promising technology development is the emergence of containers and container orchestration as the foundation of new application architectures and software development life cycles. Containers and container orchestration allow for packaging of application logic and data to make it easy to develop, deploy, scale and change functions. From a cloud computing perspective, this technology offers the promise to be able to move applications between cloud providers, assuming the cloud providers implement the container strategy in the same way. CIOs should keep apprised of this technology through CTO/architecture groups, and determine whether and when it can and should be exploited by their enterprise.

Recommendations:

• Lock-in is inevitable in your software and service architecture, and your strategy must articulate when the value of lock-in is greater than the drawbacks.

• For all lock-in, assess your vendor exit strategy upfront so that you are aware of costs, risks and options if needed.

• Embrace higher-productivity PaaS development options that will allow multicloud deployment through multiple platforms. This will provide an exit strategy and choice for developers.

• Choose IaaS as lowest common denominator if your strategy is to enable switching between multiple public cloud IaaS providers.

• When evaluating options that offer similar capabilities both on public cloud and private cloud, make sure to evaluate whether there is equal strategic investment and mind share in each solution, or whether there are hidden agendas. Remember that lock-in would then move to that provider, but it would enable multicloud functionality. As such, the longevity of the solution is an equally important evaluation criterion.

• Keep apprised of container and container orchestration developments as a new means of application development and packaging, with the potential to enable fluidity between providers and reduce lock-in.

CIOs: Develop a Cloud Strategy

As a result of these benefits (speed, agility, composability, likely reduced cost if well-designed and executed), cloud computing is the new optimized design strategy for new applications, just like the internet replaced many client/server-based applications and client/server replaced mainframe-based applications. Cloud computing will become the dominant design style for new applications and for refactoring a large number of existing applications over the next 10-plus years. Therefore, cloud as an optimized style of computing is strategic to IT and is the underpinning of delivering on new digital business innovations. The bottom line is that cloud computing as a style of computing is strategic for your enterprise, and CIOs need to focus on it from top-down (business benefits and exploitation) and bottom-up (how to achieve it) perspectives.

A cloud strategy clearly defines the business outcomes you seek, and how you are going to get there. It specifies:

• The scope of the cloud initiative

• Expected business outcomes

• Where and why you will exploit SaaS

• A decision framework for using public cloud versus private cloud services for new applications

• A decision framework for existing legacy applications and which ones will be migrated to an optimized cloud style of service, and guidance on public versus private cloud

• Management, security and governance aspects of exploiting cloud services

• External provider evaluation strategy

• Investments required and time frames/milestones for execution of strategy

• Architectural standards and considerations to drive reuse and agility, and, if desired, cross-cloud provider migration

Having a cloud strategy will enable you to apply its tenets quickly with fewer delays, thus speeding the arrival of your ultimate business outcomes. For example, it will allow you to establish a decision framework that can be used to automatically define whether new applications will be developed and/or operated in the public cloud or private cloud rather than requiring a separate intake process with every new project or product initiative. This will enable IT to deliver services faster without interruptions or delays. Where there are gray areas (for example in terms of regulatory issues), the intake workflow process could always include meetings to make the final decision, but you certainly don’t want to do that for everything. (For more information on developing a cloud strategy, see Note 3.)
**Recommendations:**

- As part of your cloud strategy, identify the key benefits you seek in using cloud computing. This should include proximity to customers and enabling employees to focus on a higher level of value.

- As input to your cloud strategy, make sure you experiment thoroughly with public, private and hybrid cloud computing to understand where you can achieve value for different types of workloads.

- Develop a cloud strategy that identifies where and how you will exploit cloud computing for new applications and for existing legacy applications (which may migrate to SaaS or need to be refactored or replaced).

- Use your cloud strategy to develop policies on public, private and hybrid cloud services that can then be automated and abstracted away from the consumer of cloud services. This will reduce or eliminate the intake process for every new application development initiative.

**Note 1**

**About the Gartner Cloud Survey**

The Gartner cloud adoption survey was conducted in 3Q15 using 6,723 responses from organizations with more than 100 employees in 10 countries: Australia, Brazil, Canada, China, France, Germany, India, Mexico, the U.K. and the U.S. Fifty-eight percent of the respondents indicated they were using or planning to use cloud services by YE15.

For more detailed analysis of the survey, see:

- “Survey Analysis: How Cloud Adoption Trends Differ by Geography”

- “Survey Analysis: How Cloud Adoption Trends Differ by Organization Size”

**Note 2**

**Optimizing Application Design for Cloud Computing**

Traditional applications were built with rock-solid infrastructure to support the applications and keep them running 24/7. Application developers didn’t worry about the infrastructure failing because I&O engineers built an always-on platform. Optimizing application design for the cloud style of computing assumes there will be infrastructure failure, so solution architects and developers must design around it — meaning they either have many replicated components such that any single loss is negligible, they simply restart the component elsewhere, or both. Enabling this type of restartability generally requires the application components to be stateless — meaning that any work that was being done is lost and must be started over and the infrastructure is immutable. Once provisioned, they stay the same; that is, they are unchangeable. If they fail, you can replace them with identical features. If required to change, they are replaced rather than directly changed. This is counter to stateful designs of traditional applications that are intended to maintain state and never lose a session, transaction, and so on.

The statelessness of the application offers the benefits of scalability and elasticity — meaning application components can scale dynamically to match increasing or decreasing demand. This typically offers the benefit of reduced cost of operation when you pay by use in the public cloud, or through increased asset utilization in the private cloud (thereby avoiding new capital expenditures for increased demand) when combined with dynamic optimization technologies. It also means achieving SLAs in a more dynamic and effective way. This contrasts with traditionally built applications that could not be dynamically changed and had to be overprovisioned to handle increased demand, thereby increasing the cost of operation.

One of the other key attributes of cloud computing is that services are delivered “as a service.” This means there are no middlemen (or service tickets) between the requester of the services and the supply of them. The requester chooses services either through a request portal or via APIs, and they are delivered dynamically. The complexities behind service delivery are managed on behalf of the service recipient, who just sees fast, frictionless delivery. We liken this to democratizing IT, in that it arms everyone with the IT capabilities, thus increasing productivity (and potentially innovation) and shortening elapsed cycle times.

**Note 3**

**There Is No One Universal Cloud Strategy**

No one single cloud strategy dominates as a style of computing for existing or new applications; nor is there a single rule of thumb as to whether the public or private cloud should be favored. This will depend on many factors such as:

- Is data center and infrastructure engineering a critical differentiator? For example, you may decide that your intellectual property should be developed with the cloud style of computing and operated in the private cloud on-premises versus other nondifferentiated areas where it makes more sense to develop and/or operate in the public cloud.

- Is application engineering such as for Mode 2 innovation a critical differentiator (or do you primarily leverage packaged applications)? If you invest in application development focused on exploratory innovation, you will likely leverage public cloud computing either directly or
through application outsourcing (this is due to both speed and lack of desire to invest in capital for areas where you don’t know the result or whether they will succeed). If you mostly leverage packaged applications, you most likely will leverage cloud as a style of computing either as private cloud or as SaaS.

- Are there regulatory requirements that may favor private cloud computing such as the requirement for the data to be kept in particular geographical or country boundaries?

- Are there application classes that may favor public or private cloud computing other than greenfield or legacy applications? For example, there may be a desire to migrate customer-facing web applications to the public cloud to operate more closely to customers (for example, at more locations) with less latency and better customer experience.

- Are there cost or maturity factors that may influence whether to operate in the public or private cloud? Often, bursty or seasonal workloads where there is significant variability in demand are more cost-effective in the public cloud because you don’t have to own the infrastructure for occasional use. However, at the other end of the spectrum, often 24/7 production workloads are less expensive to operate internally (if you are fairly mature in your operations).

Documenting your types of workload and benchmarking your costs of service delivery as well as by type of application service will help in developing the cloud strategy.

- Does your company favor capital expenditure (capex) or operating expenditure (opex) spending? Generally those that favor capex prefer on-premises-owned infrastructure, while those that favor opex will favor nonowned assets such as public cloud computing or managed private cloud computing.

Source: Gartner Research Note G00310075, Refreshed: 27 June 2017, Published: 07 July 2016
About Telefonica Business Solutions

*Telefonica Business Solutions*, a leading provider of a wide range of integrated communication solutions for the B2B market, manages globally the Enterprise (Large Enterprise and SME), MNC (Multinational Corporations), Wholesale (fixed and mobile carriers, ISPs and content providers) and Roaming businesses within the Telefonica Group. Business Solutions develops an integrated, innovative and competitive portfolio for the B2B segment including digital solutions (IoT, Cloud, Security) and telecommunication services (voice, data, mobile, satellite, unified and global solutions). Telefonica Business Solutions is a multicultural organization, working in over 40 countries and with service reach in over 170 countries.

[Website Link]
[Twitter Handle]
[YouTube Channel]
[LinkedIn Page]