

# Developing a cloud sourcing strategy

## Six tips to select the right cloud partner

**NL** +31 20 316 2880  
**US** +1 571 814 3777  
**DE** +49 69 2475 2860  
**SG** +65 3158 7350

[www.leaseweb.com](http://www.leaseweb.com)  
[sales@leaseweb.com](mailto:sales@leaseweb.com)

# CONTENTS

<b>Executive Summary</b>	<b>3</b>
<b>Introduction</b>	<b>4</b>
<b>Six areas to consider before signing</b>	<b>5</b>
1. Support and services	5
2. Architectural alignment	6
3. Degree of security and compliance	6
4. Support for data sovereignty and residency requirements	7
5. Financial management	8
6. Cultural/Strategic alignment	9
<b>Conclusion</b>	<b>10</b>

## EXECUTIVE SUMMARY

Driven by industry and market hype, many companies feel compelled to move to the cloud as quickly as possible. However, few truly understand the difference between delivery models such as the degree of services they offer, the security they provide or their expected costs. Rushing into a contract for cloud services without defining your expected outcome typically leads to cultural and organizational misalignment and, worse still, significant overspending.

To find the right cloud partner as part of an effective cloud sourcing strategy, you must balance both business needs and technical requirements. These holistic criteria, six of which are outlined in this whitepaper, must highlight what that is important to your specific organizational needs.

# INTRODUCTION

Common practice presumes that the best strategies are rarely all or nothing propositions, and cloud strategy is no different. This line of thinking dictates that specific workloads require hosting in virtualized, single tenant environments. In fact, enterprises do have a choice in deciding where to put their workloads as most will benefit from highly dynamic, scalable, multi-tenant environments.

In the world of cloud services, the hyper-scale providers dominate both in market share and news headlines. When anyone – blogger, journalist, or end user – refers to cloud or infrastructure as a service (IAAS), they typically distill the entire market (\$30+ billion market by 2018 according to Gartner, Inc) to three providers: Amazon Web services, Microsoft Azure and Google Compute Engine. It is true that these providers account for more than 60% of the IaaS market share, but thinking that they represent 100% of the market players is dangerous and flawed reasoning.

Most businesses who have a need for cloud infrastructure services will have slightly different buying criteria and pain points; some will have more stringent compliance and privacy requirements, some will need to lean on a service providers' expertise, some will require massive compute capability while some require only temporary capacity. Expecting a single cloud provider to handle all of your cloud needs will feel like an octagonal peg fitting into a square hole – try as you might, it will never be a perfect fit.

Creating an effective cloud sourcing strategy requires a process where individual workloads and applications are classified by their requirements and dependencies. Once that heavy lifting is done, the sourcing strategy needs to take center stage. One must consider to what degree you need a provider who can co-develop solutions and effectively become an extension of your own IT staff. A word of warning: don't underestimate the value of a deep and valuable relationship with a provider. The secret to finding the right partner, a trusted advisor if you will, is to develop a set of criteria that address your organization's specific needs. Consider the following six areas, which have been compiled from conversations with hundreds of enterprises, before signing a contract with a cloud or hosting provider:

# SIX AREAS TO CONSIDER BEFORE SIGNING

Consider these six areas before signing a contract with a cloud or hosting provider:

## I. SUPPORT AND SERVICES

When most enterprises decide to engage a third party for services, a long laundry list of concerns is created. Concerns regarding cost, security, vendor management and technology are typically prioritized as the most pertinent. Surprisingly, the degree to which a provider can deliver customer support, SLAs and managed services is often minimized or overlooked. Reasons for this disconnect can be attributed to an enterprise's misconceptions about where a cloud and hosting provider's responsibilities end and the customer's responsibilities begin. Industry leading providers understand the division of responsibilities and will provide a matrix of responsibilities for the operational tasks. Traditional hosting providers, who have a pedigree for sharing best practices with their clients, have a spectrum of operational responsibilities from the hardware to the operating system and provide service level metrics to the components under their care.

This paradigm was the de facto market standard until the advent of the public, hyper-scale cloud provider. Public cloud providers have built platforms and tools intended for technical and operational users and labeled it as a service. Very few managed services are typically available and service level agreements tend to be tied to performance and the availability of their platforms. As part of their basic offerings, public cloud providers tend to provide only email and self-service portals, and charge a 10%–15% premium for named customer support resources.

Consequently, enterprises must decide what degree of support is required for all of their cloud environments and identify an internal resource to manage all support and service issues.

The value of leveraging a third party is only truly achieved when both sides understand their responsibilities and expectations.

## 2. ARCHITECTURAL ALIGNMENT

As enterprises start to develop their cloud sourcing strategy and investigate both traditional hosting and hyper-scale providers, they should take note of points where both delivery models run parallel, intersect and deviate. All providers use similar enterprise or open source technologies and solutions for the fundamental cloud and hosting services elements – like data centers and server infrastructure. VMware, Microsoft, Docker, Cisco and other mainstream IT products continue to be widely adopted by both hyper-scale and hosting providers. The deviation between service delivery models occurs in the way providers operate and deliver the web infrastructure.

For example, hyper-scale providers use “web scale IT” principles including industrial data centers, web oriented and programmable systems. This operational philosophy allows for rapid deployment of thousands of homogeneous systems. In contrast, hosting providers operate using elements of web scale IT but balance their platforms with the ability to customize configurations and support a wide array of technologies. The distinction may seem superfluous and unnecessary, as enterprises may mistakenly only focus on the service they’re purchasing. Practically speaking, enterprises need to understand that using a hyper-scale provider requires users/enterprises to be responsible for operational, day to day tasks. Hosting providers oversee the day to day management of the infrastructure elements. For those enterprises planning on a hybrid cloud strategy, understanding where service provider and internal IT responsibilities reside will be absolutely critical when deciding between a traditional hosting and a hyper-scale provider.

## 3. DEGREE OF SECURITY AND COMPLIANCE

The most challenging hurdle to clear when considering using a hosting or cloud provider is having to relinquish a degree of control. The value of leveraging a third party is only truly achieved when both sides understand their responsibilities and expectations. Both sides must articulate a common understanding of roles and responsibilities to help mitigate the occurrence of threats and expansion of attack vectors. Hyper-scale and hosting data centers are both high value targets for malicious attacks, making the evaluation of security policies and procedures critical. When considering either a cloud, hosting or hybrid cloud architecture evaluate these areas:

- **Physical.** Best practices are focused on restricting access to only those who require it. Closed Circuit Television both inside and outside the data center as well as biometrics to monitor access to critical customer areas should be standard offerings. 24x7 security presence is critical in managing any attempted breaches that might occur.
- **Perimeter.** Best practices focus on both detection and prevention of malicious acts before they impact client infrastructure. DDoS mitigation, next generation firewalls (web application centric) and IP reputation filtering are critical to blocking malicious activity and preventing malicious traffic from affecting customer deployment.
- **Network.** Best practices focus on blocking unauthorized access to customer VLANs through the following:
  - Intrusion detection and prevention
  - Isolated security zones
  - Private network segmentation

- Vulnerability monitoring and audits
  - **Server.** Best practices focus on:
    - Hardening OS and hypervisors
    - Virus and malware protection
    - Monitoring of network and event logging
    - Password and key management
    - Reporting of patches tested and applied
  - **Compliance.** Best practices will address both general and industry specific certifications and audits. Critical certifications should include:
    - SSAE 16
    - ISO27001
    - CSTAR
    - Privacy and compliance certifications are necessary for those organizations supporting compliant workloads and should include HIPAA, PCI and GLBA. Public sector customers should look for FedRAMP certification as well.

## 4. SUPPORT FOR DATA SOVEREIGNTY AND RESIDENCY REQUIREMENTS

In tandem with security and compliance issues, data protection is another hot button issue that frequently stalls cloud and hosting projects. The growth of bring your own device (BYOD), big data and cloud projects is dragging sensitive data to third party clouds and data centers. This makes many Chief Information Security Officers (CISOs) uncomfortable with how and where data resides and is secured. The issue becomes more complicated for both multinational enterprises that conduct business in multiple geographies and those that work in highly regulated environments. The CISO has two basic options: attempt to block any projects where data leaves their internal datacenter; or swim with the tide and apply best practices with their service provider to develop the effective strategies for data protection.

### COMPLIANCE CERTIFICATIONS YOU SHOULD LOOK OUT FOR

#### BASIC



#### PRIVACY AND COMPLIANCE

e.g. HEALTHCARE  
AND FINANCIAL SERVICES



#### PUBLIC SECTOR






The essential topics to address include:

- **Data encryption and tokenization.** A top strategy employed by most enterprises and service providers that still requires governance to be effective. Understanding how data is encrypted across its entire lifecycle will help users identify when data appears in clear text and when it's encrypted. Enterprises will have to decide where key and tokens are stored (on premise or cloud) and understand the tradeoff between security and performance in accessing those keys or tokens.
- **Geographic data export restrictions.** A critical and uncomfortable area for most CISOs, especially for those with data in multiple global locations. Many countries have created their own data privacy laws that vary in requirements to protect personal identifiable information. Certain jurisdictions such as the USA (Patriot Act) and UK (Regulation of Investigatory Powers Act) allow for access and interception of data while it passes through their boundaries. Enterprises must work with their service provider to identify at which locations data is stored and if those locations are subject to government restrictions around import and export of encryption technology.
- **Nature and location of stored data.** Data – even sensitive data such as medical records, financial information and tax records – has a lifespan. A critical and often overlooked part of enterprise data governance plans is the destruction of end-of-life sensitive data as well as associated tokens and encryption keys. Enterprises should work with their service provider to ensure that all backup copies of end-of-life data are deleted and associated keys and tokens are “digitally shredded”.

## 5. FINANCIAL MANAGEMENT

Ask most enterprises why they are considering a cloud and hosting provider for their applications and workloads and they will say that they expect to cut IT costs by 30–40%. The promise of shifting away from buying and amortizing hardware, software and license costs is usually enough to get initial buy-in from key stakeholders including the CFO. Soliciting bids and comparing external pricing against internal forecast moves the needle for most enterprises and paves the way towards success in the cloud... or does it?



Many enterprises struggle to track and report cloud usage and can't accurately predict if using cloud is more or less expensive than internal IT.



Both cloud and hosting services have distinct cost profiles that benefit specific use cases and workloads:

**Traditional hosting**

Hosting costs are typically more predictable and based upon initial configurations with monthly utilization. Hosting providers do typically require a one-time set-up fee when dedicated environments are provisioned. Virtualized environments can reduce the amount of one-time set-up costs. Variable costs are only triggered by planned capacity upgrades of servers and storage so shouldn't catch enterprises off guard with larger than expected monthly invoices. Hosting matches well with both virtualized and dedicated architectures for steady and predictable usage patterns. Regardless of the model, ensure you include capital expenditures in a hosting total cost of ownership analysis to truly reflect costs.

**Cloud providers**

Hyper-scale cloud services, on the other hand, were built around granular per minute or hourly costs from their inception. Provisioning is primarily self-service and allows users to turn up server, storage and network services. This feature appeals to users who need to spin up environments in near real time and then turn them down when not needed. However, many enterprises struggle to track and report cloud usage and can't accurately predict if using cloud is more or less expensive than internal IT. The end result? Users over-provision cloud resources and then receive a hefty bill for compute and storage, which shatters the notion that cloud is less expensive than hosting.

The financial issues in cloud and hosting procurement are much more nuanced than most realize until a total cost of ownership analysis is performed after three to four months post-deployment.

## 6. CULTURAL/STRATEGIC ALIGNMENT

Occupying a close second to customer support in importance is the cultural fit with the service provider. For nearly all enterprises, using a cloud or hosting provider is truly a new venture, one that requires extensive internal buy-in. For first-time cloud buyers, the ongoing degree of partnership is an unknown factor. Each provider engages and on-boards clients differently. Most hosting and some cloud providers assign a team that shares knowledge and best practices to design the best customer solution. Some providers – mostly hyper-scale and bare metal service providers – only offer on demand tools such as extensive wikis and help desk forums to enable users to self-provision. Neither solution fits all types of cloud buyer's needs. The goal is to choose a provider whose process is best suited for your enterprises operational expertise.

## CONCLUSION

No one becomes a cloud infrastructure expert overnight. It requires enterprises to open up and think about new service, support and delivery models that support both business and technical requirements. But the first step is to embrace the ideas of new service, support and delivery models for your business. And you need to realize that you will only achieve the higher performing and lower cost environments you are aiming for by choosing the correct type of provider. Next, consider the following recommendations:

- The best cloud strategies are a “custom fit” for each enterprise and are built around individual business drivers and IT goals. Choose managed hosting for enterprise critical applications, where you require day to day outsourced management; choose public cloud services for test/dev or for applications that require rapid scale. Be aware that most public cloud services offer only self-service management.
- Expand your thinking beyond behemoth hyper-scale cloud providers and consider those who offer multiple platforms including cloud, hosting and managed services. Hosting providers will offer better solution flexibility and customized support; public clouds support frictionless, standardized solutions. Consider architecting a hybrid solution that employs both public and hosted cloud infrastructure.
- Develop a set of balanced evaluation criteria including both technical and service elements; don't underestimate strategic alignment and cultural fit with your service provider. Ensure these providers offer the requisite security, compliance and data privacy support required for your enterprise.