Predicts 2019: Increasing Reliance on Cloud Computing Transforms IT and Business Practices

Published: 13 December 2018 **ID:** G00374367

Analyst(s): Yefim Natis, David Smith, Ed Anderson, Sid Nag, Neville Cannon, Rene Buest

Most technology innovation today is cloud-native or cloud-inspired. “Cloud computing” is morphing into just “computing,” and so application leaders must seek cloud-style quality of service across their hybrid information and technology environments.

Key Findings

- “Cloud computing” is shifting from an isolated delivery option to an all-encompassing computing strategy, including public and private cloud, on-premises enterprise systems, Internet of Things (IoT) edge and a variety of user experience outlets.
- Organizations are moving beyond, now common, “cloud-first” strategies. Even typically slower-changing government agencies are accelerating their cloud-only initiatives.
- Business innovation increasingly depends, in part or in whole, on the capabilities and performance delivered by public cloud’s advanced quality of service (QoS), including elastic scalability, agility, productivity and continuous global reach.
- Organizations are making strategic plans for consuming cloud services and are pursuing long-term relationships with cloud megavendors. They are looking for continuous access to cloud and hybrid innovation, and maximized efficiency, but, at the same time, wish to control vendor lock-in by adopting open standards and integration technologies.

Recommendations

Application leaders guiding their organizations’ cloud computing strategies should:

- Embrace cloud-native computing to stay abreast with information, technology and business innovation by investing in modern technologies and practices.
- Avoid exclusive commitments to any one provider; instead, embrace multiplatform operations and a hybrid integration strategy to retain greater flexibility of choice and innovation.

- Advance close relationships with business leaders to assist them in recognizing strategic cloud-centric business opportunities by creating IT-business liaison teams and practices.
- Promote organizational and cultural changes in support of cloud-native operations to ensure consistent transition outcomes by investing in continuous cross-organization education and process innovation.

Table of Contents

List of Figures

Strategic Planning Assumptions

By 2021, over 75% of midsize and large organizations will have adopted a multicloud and/or hybrid IT strategy.

By 2022, public cloud services will be essential for 90% of business innovation.

By 2021, less than 10% of multicloud deployments will take advantage of the anticipated portability.

Analysis

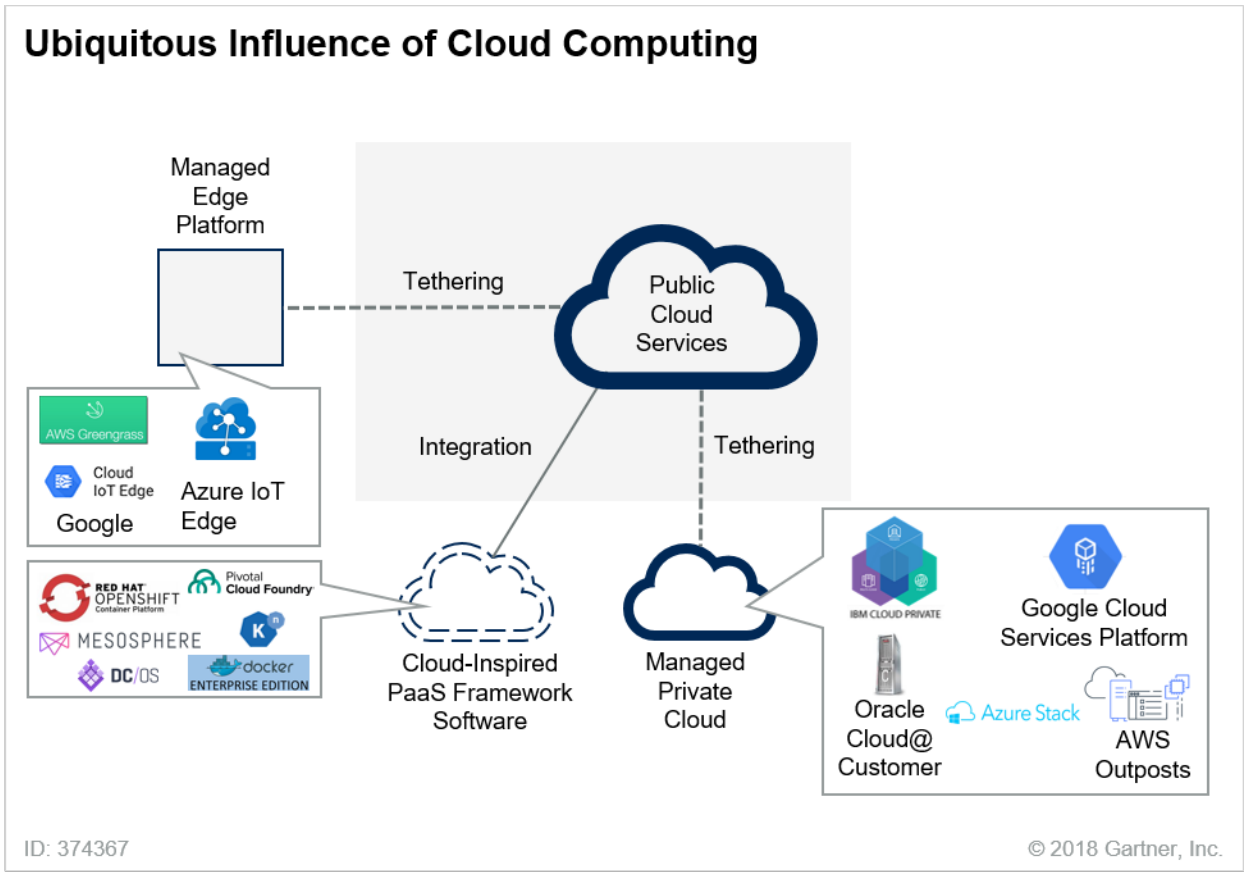
What You Need to Know

Cloud quality of service (CQoS) is now viewed as state of the art for enterprise computing and replaces enterprise quality of service (EQoS), which dominated computing for decades. Cloud quality of service is where business organizations demand access to information and technology services with self-service features, agility, effortless scaling, resilience, productivity, efficiency and data integrity, paired with continuous innovation. Meanwhile, most organizations discover that adopting cloud using a simple lift-and-shift migration does not deliver any of the cloud benefits, but

does incur costs and risks. In this context, computing is becoming a hybrid effort of cloud innovation, on-premises application modernization and strategic integration — all of which are increasingly cloud-based or cloud-inspired.

> The ubiquitous presence of cloud-inspired, cloud-based and cloud-native design in most cloud, on-premises and on-edge technology initiatives amounts to morphing "cloud computing" into just "computing."

Figure 1. Ubiquitous Influence of Cloud Computing



Source: Gartner (December 2018)

Gartner's 2018 CIO Survey indicates that IT leaders perceive improvement to core systems and adoption of cloud services as equally high priorities (see "The 2018 CIO Agenda: Mastering the New Job of the CIO"). Early hype centered on cloud fully replacing all on-premises computing, but this has given way to the reality of multicloud being combined with the some on-premises and other off-cloud computing (also referred to as "hybrid computing"). Most organizations have realized by now

that not only will the current situation be hybrid, but so will their long-term information and technology environments:

- Cloud providers compete through innovation. Organizations that wish to lead through business innovation want to have access to new technology as it emerges from various cloud service providers. Thus, organizations plan to consume the services of multiple cloud providers.
- Customers discover that most cloud services are at least partially proprietary. The prospect of lock-in in the cloud has become one of the widespread concerns among customer organizations. Most are determined to adopt a multicloud strategy to minimize lock-in.
- Few midsize and large organizations plan to fully eliminate their on-premises systems in the foreseeable future. And while traditional on-premises computing is gradually declining, other off-cloud deployments, such as IoT edge, emerge. Thus, hybrid IT is recognized by most organizations as a long-term strategic prospect.
- Most organization are planning, or are already engaged in, a digital transformation. One of the fundamentals of digital business is the interdependence of organizations and ecosystems of partners and providers. Cooperation and coordination between independent business organizations within an ecosystem inevitably creates a heterogeneous multicloud, multiplatform computing environment.

Issues of reconciling the dependence on multiple cloud service providers and continuing reliance on the on-premises core applications, has created new challenges. They lead organizations to redesign their cloud adoption strategies, shifting the focus from specific capabilities in isolation to integration and coordination of multiplatform business operations. While the challenges of hybrid computing may seem complex, expensive and even dangerous early in the process, as the new integration-centric strategy begins to martialize, organizations discover the liberation that it provides for their technology and business decision making. Once ready for heterogeneity, the organization is ready to embrace a vastly broader sources of innovation and permit more of their systems to be redesigned for cloud-native and cloud-only deployment.

This year, Gartner's SPAs highlight the increasing reliance of organizations on nearly ubiquitous cloud services, and the increasing maturity of cloud adoption in mainstream organizations.

Strategic Planning Assumptions

Strategic Planning Assumption: By 2021, over 75% of midsize and large organizations will have adopted a multicloud and/or hybrid IT strategy.

Analysis by*:* Sid Nag, Rene Buest

Key Findings:

- Cloud is the foundation for digital business, and hybrid cloud and multicloud models are increasingly being adopted by organizations. The market size for public cloud is growing exponentially and is projected to reach $360.3 billion by 2022 (see "Forecast: Public Cloud Services, Worldwide, 2016-2022, 3Q18 Update" and Note 1).

- The number of cloud managed service providers (MSPs) addressing this space will likely triple to peak in 2020, then face massive consolidation by 2023. While many service providers are racing to enter this space, fast movers will commence acquisition sprees as the rush turns into more of a flow.
- Multicloud or hybrid cloud models require add-on capabilities around aggregation, integration, customization and governance to manage these disparate cloud assets and properties. This presents a follow-on opportunity for providers.

Market Implications:

Cloud computing has become the epitome of modern IT environments, and cloud-first strategies are the common approach for new IT investment. Gartner expects cloud adoption rates among organizations to jump from 68% in 2017 to 85% in 2019. Through 2020, cloud will be used for use cases that impact most organizations' core business operations.

While cloud computing has become the new normal for modern IT environments, hybrid and multicloud are the reality when driving business transformation initiatives. Gartner research shows that, by 2020, about half of infrastructure as a service (IaaS) is expected to be deployed via public cloud and one-third will be deployed on-premises. Colocation, however, will be scarcely used.

Digital business requires organizations to leverage cloud solutions from more than one cloud provider. In doing so, they are able to take advantage of a variety of best-in-class services from every provider. Hybrid cloud and multicloud usage also lets them reutilize their systems of records and combine them with systems of innovation.

Leveraging hybrid cloud and multicloud environments, however, promotes complexity for the necessary cloud integration, as well as operation and management. That's why we expect that, by 2021, 75% of enterprise customers seeking cloud-managed IaaS and PaaS solutions will require multicloud capabilities from a cloud MSP, up from 30% in 2018.

Recommendations:

To fully leverage multicloud and hybrid cloud models, application leaders must:

- Adopt multicloud and hybrid offerings with the desired digital business outcomes and broader IT initiatives in mind by leveraging metrics-based service offerings, such as operating productivity, cost savings and business efficiency.
- Take advantage of the agility, innovation, scalability and synchronization capabilities of services and solutions for hybrid and multicloud environments.
- Engage and contract with strong ecosystem partners that focus on industry verticals, specific geographies, adjacent markets and customer size. Leverage intellectual property (IP) and advanced techniques from service providers for relevance to, and focus on, your desired business results.

- Adopt cloud integration capabilities that bring together multiple cloud services and make them work together to deliver seamless distributed business process execution. These capabilities are typically delivered via an enterprise integration PaaS (eiPaaS) or cloud service brokerage functions, which include integration of cloud endpoints at scale, and community management and migration skills.

Related Research:

"Market Guide for Cloud Service Brokerage"

"Market Insight: What Tech CEOs Need to Do About the Factors Influencing the Rapidly Growing Cloud Market"

"Market Insight: How Tech CEOs Can Capture the Growing Hybrid and Multicloud Service Market"

"What It Takes to Be a Multicloud Managed Service Provider"

"How Cloud Managed Service Providers Should Approach Their Hybrid Cloud Management Platform Strategy"

Strategic Planning Assumption: By 2022, public cloud services will be essential for 90% of business innovation.

Analysis by: Ed Anderson and Yefim Natis

Key Findings:

> Modern business depends on technology for its competitive operations and customer experiences; and most technology innovation has firmly shifted to the cloud. Few, if any, organizations will be able to implement new business models or ecosystem relationships without relying on cloud services.

- Integration technologies are ubiquitous, and have developed to the levels of maturity that enable organizations to safely combine the slowly modernizing traditional business systems with the fast-changing systems of innovation. This reduces the risk of the innovative use of cloud services and its agile operational models.
- Organizations that have achieved cloud adoption maturity use cloud to create a dynamic, agile and innovative platform for their new operating processes. Innovations flow from public cloud services into the organization, spawning new ways of thinking about the role of technology in driving business outcomes.
- The ease of consumption and proportional pricing models of many cloud services make innovation technologies accessible to every organization. These democratized IT capabilities

include AI, API marketplaces, event-driven continuous intelligence, next-generation user interfaces, real-time situation awareness, decision automation, digital twins and a large market of modern application systems (SaaS).

Market Implications:

- Innovation consumed from public cloud services democratizes IT innovation. It delivers new business outcomes that were previously out of reach for all but the most advanced IT organizations, to a broad spectrum of business users.
- Cloud-inspired business innovation is shifting organizations to new ways of thinking and operating. The new self-service access and productivity, delivered to lines of business by cloud services, forces IT organizations to redefine their mission and build a new relationship with business leaders.
- The requirement for cohesive business operations is challenged by the conflict between the entrenched dependence on traditional business systems and the emerging need to compete through cloud-based innovation. In this context, competence in hybrid multicloud integration becomes a strategic imperative for most organizations.

Recommendations:

Application leaders must plan for the use of public cloud services for future business innovations. To do so, they must:

- Establish cloud competencies for consuming public cloud services and operating in a cloud-like fashion dynamically, adaptively and innovatively.
- Use public cloud services for both tactical (short-term) and strategic (long-term) outcomes.
- Tie cloud initiatives to business outcomes, in addition to any technology outcomes you seek.
- Build strategic integration competency to facilitate business innovation across the new cloud investments, and the established enterprise processes and information systems.
- Manage the transformation of the IT organization in terms of how it adapts to the new modes of business operation and innovation, including self-service, agility and productivity of lines of business, and the fast-growing catalog of available SaaS solutions.
- To help enable rapid business innovation, begin consuming new technology capabilities delivered through public cloud services as they emerge, such as artificial intelligence, analytics, edge computing, event-driven design and IoT.

Related Research:

“4 Starting Points for Digital Business Transformation”

“Four Definitions Make a Digital Business Strategy Process More Effective: A Marketing Perspective”

“2018 Hype Cycles: Riding the Innovation Wave, A Gartner Trend Insight Report”

“Digital Disruption and Innovation Primer for 2018”

“Build the Right Justification for Moving to the Cloud”

“Innovation Insight for Hybrid Integration Platforms”

Strategic Planning Assumption: By 2021, less than 10% of multicloud deployments will take advantage of the anticipated portability.

Analysis by: David Smith and Yefim Natis

Key Findings:

- Multicloud can refer to many different scenarios. For vendors, it primarily refers to the availability of their offerings on multiple major cloud platforms and ecosystems. For users, it typically refers to the use of multiple major cloud data center networks (like AWS, Microsoft Azure or Salesforce, and their ecosystems) to meet all of the business’s cloud computing requirements.
- Customers’ cloud strategies often turn to multicloud to control costs and complexity, and to avoid excessive lock-in. To manage the lock-in, portability and dynamism are often prioritized in the decision framework for multicloud strategies.
- In practice, the ability to relocate applications (and their data) between the major cloud platforms (the dynamism enabled by portability) is rarely engaged because of business, technology and cost reasons:
  - Migration, even if with maximum portability, is bound to affect and inconvenience business users, which IT leadership would rather avoid in straight migration cases, when business does not get new capabilities.
  - Portability can never be complete, and technology changes during and after the crossing of the environments represent an unwanted unknown.
  - The cost of migration is usually hard to justify, given that it is hard to estimate and also represents potential challenges and minimal benefit for business users.
- Cloud computing strategies today increasingly include multicloud as a primary objective. Although multicloud computing is seen as offering the potential to increase customer resilience and to lower the risk of cloud provider lock-in, most organizations will not solve the problem of lock-in through multicloud, nor will they achieve greater resiliency.

Market Implications:

As with many cloud-related concepts, there are many variations in multicloud's real-world use and scope. While multicloud (much like cloud itself 10 years ago) is a hyped term that remains somewhat unclear to many, we have outlined three categories of multicloud computing competencies:

- **Multicloud strategy.** Most organizations will have a multicloud strategy focused on sourcing issues. This typically requires little to no technical or architectural decisions. It requires a strategy for vendor management, a framework for workload placement, and a strategy for developing and maintaining employees' skills.
- **Multicloud management.** This refers to a coordinated approach toward managing and governing environments making use of multiple cloud providers. This includes enabling standardization of some policies, procedures and processes, and tools, especially tools that allow cost governance and optimization across multiple cloud providers. This includes, but goes beyond "single pane of glass" approaches to monitoring,
- **Multicloud architecture.** The focus here is on architectures that enable applications to span multiple cloud providers. Indeed, some applications may be a composite of multiple different types of services and providers. Portability and migratability are usual goals. Some applications may also be deployed on different cloud providers' platforms at different times and decided at runtime. For example, a batch-job application might be deployed to the least expensive cloud provider at a given time.

Most multicloud situations today are centered around the strategy or procurement approach. This is followed by multicloud management, and then multicloud architectures. Even within the focus on multicloud, we expect that multicloud architectures enabling true portability (not just ease of migration), and dynamism will account for, at most, 10% of multicloud situations through 2021.

Recommendations:

Application leaders should:

- Avoid hype-driven multicloud strategies.
- When establishing multicloud strategies, do it to achieve provable benefits to the organization and respond to the reality of public cloud adoption practices.
- Examine the multitude of multicloud business and technology scenarios — it is not just one thing.

Related Research:

"Technology Insight for Multicloud Computing"

"Hype Cycle for Cloud Computing, 2018"

"Cloud Computing Primer for 2018"

Replay Prediction

The replay prediction is a prediction from a previously published report that is so significant that it is being republished here.

Strategic Planning Assumption: By 2020, more than 30% of government agencies with "cloud-first" strategies will adopt "public-cloud-only" strategies for all new initiatives.

Analysis by: Neville Cannon

Key Findings:

The first country to adopt a "cloud-first" policy was the U.S. back in 2011. Since then, many countries have followed suit, although it is fair to say that adoption and migration remained low for many years. The usual constraints of security and sovereignty played out for government IT departments. The focus of "cloud-first" policies during these early days was on revenue saving, with many white papers being produced extolling significant budget savings (75% to 85% was a commonly quoted figures). However the experience has been somewhat more limited and Gartner now reports cloud-based savings of around 16%.

In the intervening seven years since 2011, the hyperscalers have not stood still waiting for the bonanza. They have significantly developed their offerings, both in terms of the security and range of services offered, and the regions served by in-country data centers. This development has taken place as the understanding of cloud potential has matured. While savings are still paramount, governments and individual agencies are prioritizing different cloud capabilities and benefits to suit their requirements for flexibility and agility when it comes to policy introduction. Introducing more innovation is vital to many departments or ministries, and we now have examples at local, regional and national levels of agencies that are 100% operating in the cloud for just that purpose.

The U.K. government continues to recognize the wider value of cloud adoption in supporting agility. It encourages departments to break away from monolithic, complex contracts to consumption-based models that are flexible and agile. The U.K. now operates a "cloud-native" policy and Gartner has seen increased pressure being placed on governments in other countries, such as the U.S. and Australia. Data classified as "official" or "protected" is now routinely being placed in public cloud environments and, in the U.S., dedicated cloud facilities are able to host data that is classified as "secret" and "top secret." Such facilities share their infrastructure with public sector and approved clients, such as defense contractors.

The drive to use a public-cloud-first strategy is not solely being driven by policy, however. With the advent of SaaS, Gartner has seen consistent growth in the adoption of shadow IT — mission departments, hungry for innovation, are increasingly embracing their own directly sourced solutions. Across government departments, it is not uncommon to see 30% to 36% of organizational technology expenditure taking place outside of the view of the central IT department. Continued adoption of SaaS solutions is expected to contribute to making this prediction accurate, as departments take control of their own transformational initiatives.

Government agencies believe that supporting an on-premises policy is likely to create a number of challenges going forward:

- Improved security will mainly be developed for cloud architectures and solutions, given that cloud is increasingly becoming the mainstream method for computing.
- Talent will gravitate toward more modern solutions and architectures to improve their employability and overall career prospects.
- Software providers will seek to migrate users onto consumption- or subscription-based models by effectively ceasing development for on-premises solutions.

The implication of these issues will effectively support and accelerate the adoption of public cloud across governments.

Market Implications:

CSPs are continuing to address the sovereignty issue by creating more IaaS regions, but the cost of implementing these local regions is too high for vendors to cover all countries where they have (or wish to have) customers. These limitations are already being identified, and price increases are being applied in smaller (in hyperscaler terms) regions. As SaaS continues to become the dominant model for government applications, vendors are likely to continue the migration of existing applications to subscription-based models. This will put pressure on those government CFOs who are reluctant to address the need to update their accounting practices to support the cloud-native subscription model.

As the move to public cloud continues, governments will increasingly seek further security assurances and tools to not only protect data sovereignty, but also privacy. Vendors operating in this space should expect the market to grow.

Justification:

Gartner has noticed a shift in client inquiries regarding cloud services for the government sector. The conversation has moved away from security- and strategy-based inquiries to a migration planning focus — essentially moving from a “should I” mindset to a “how do I” approach. Even those operating at the most secure end of the government sensitivity spectrum (defense, intelligence and health) are now asking how they can better take advantage of the capabilities and services offered by the public cloud.

Recommendations:

Government application leaders must:

- Continue to develop the relevant skills within their teams — leaving this too late will only exacerbate the pressures on recruitment and retention.

- If not already started, begin experimenting with public cloud to appreciate the operational practices that need to be considered and mastered.
- Gain visibility into how the government is already making use of SaaS applications. Utilize tools such as CMPs or services from cloud access security brokers (CASBs) to obtain an overview of the shadow IT activities currently being carried out in the organization in use in order to build a stronger case for a full cloud strategy.

Related Research:

"Forecast Analysis: Public Cloud Services, Worldwide, 2Q18 Update"

"A Guidance Framework for Selecting Cloud Management Platforms and Tools"

"Get Ready for the Inflection Point in U.S. Federal Government Cloud Adoption"

A Look Back

In response to your requests, we are taking a look back at some key predictions from previous years. We have intentionally selected predictions from opposite ends of the scale — one where we were wholly or largely on target, as well as one we missed.

On Target: 2015 Prediction — Through 2017, the value delivered by Docker will be centered on a new ecosystem for container-oriented management, rather than vendor-hyped portability benefits.

We have seen vendor hype around portability — including hybrid cloud and multicloud portability — continue. That hype remains as feverish as ever, although it is increasingly focused on Kubernetes (container orchestration software) rather than Docker or containers in general. These technologies offer a more agile and consistent application development and deployment process. However, they do not significantly increase portability between on-premises and cloud environments, or between cloud environments, including different IaaS providers and PaaS frameworks.

As we anticipated, a large ecosystem has emerged around container-oriented management. That ecosystem is still evolving rapidly. The benefits of containers have primarily accrued to developers, especially those that use continuous integration/continuous delivery (CI/CD), DevOps automation tools, and immutable infrastructure. Infrastructure and operations (I&O) teams often struggle to adapt their processes to manage and secure containers, and to orchestrate containers at scale. Public cloud providers have responded to these operational challenges by offering container services, such as Amazon Elastic Container Service, Azure Kubernetes Service and Google Kubernetes Engine.

Missed: 2015 Prediction — By 2020, over 50% of all new applications developed on PaaS will be IoT-centric, disrupting conventional architecture practices.

The base expectation in this prediction was that adoption of IoT solutions would accelerate at a much faster rate than it in fact occurred. Part of the reason for the slower pace of growth is the complexity of multistaged IoT solutions, which deterred many organizations from developing custom IoT solutions. And, meanwhile, cloud service providers' IoT platform offerings are maturing

slower than expected, making it more difficult for organizations to rely on IoT platform service providers either. Another important change of direction that affected the prediction has to do with the shifting focus of IoT innovation to IoT edge computing. A larger than expected share of IoT solutions and investment is implemented directly at the edge, leaving the cloud IoT platforms with a smaller role in the overall design of IoT solutions.

It is important to note the second part of the prediction, however ("… disrupting conventional architecture practices …"). In those scenarios where IoT PaaS is engaged in the design of IoT solutions, that approach does indeed alter many conventional architecture practices:

- The pipelined assembly of platform capabilities
- The cascading application of analytics with increasing scope of context
- The adoption of a digital twin architecture
- The reliance on event processing and event stream analytics

For most organizations, these practices and patterns represent new design and architectural models.

As IoT solutions overall, and IoT platform services in particular, reach greater maturity and organizations develop best practices for adopting IoT-required architectural principles, the essential finding of this prediction will be justified. IoT architecture and use cases will become a common experience of mainstream organizations.

Additional research by Lydia Leong

Gartner Recommended Reading

Some documents may not be available as part of your current Gartner subscription.

"The Key Trends in PaaS, 2018"

"Hype Cycle for Cloud Computing, 2018"

"Get Ready for the Inflection Point in U.S. Federal Government Cloud Adoption"

"Technology Insight for Multicloud Computing"

"Market Insight: Making Lots of Money in the New World of Hybrid Cloud and Multicloud"

"Market Guide for Cloud Service Brokerage"

"2018 Hype Cycles: Riding the Innovation Wave, A Gartner Trend Insight Report"

"Build the Right Justification for Moving to the Cloud"

Note 1 Multicloud and Hybrid Cloud Defined

According to Gartner's Hype Cycle for Cloud Computing, the definitions for multicloud and hybrid cloud are as follows:

- Multicloud computing refers to the use of cloud services from multiple public cloud providers for the same purpose. It is a special case of "hybrid cloud computing," which is a broader term.
- Hybrid cloud refers to multiple cloud services from multiple providers. It does not specify the origin of those services, but in most cases a public source and a private source are involved. "Hybrid cloud," as a broad term, is subject to more hype and confusion, and is more common.

More on This Topic

This is part of an in-depth collection of research. See the collection:

- Predicts 2019: Leadership Means Expanding Options, Not Limiting Them — A Gartner Trend Insight Report

GARTNER HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
USA
+1 203 964 0096

Regional Headquarters
AUSTRALIA
BRAZIL
JAPAN
UNITED KINGDOM

For a complete list of worldwide locations,
visit http://www.gartner.com/technology/about.jsp

Inform Your Cloud Service Choice With Provider Maturity

Published: 15 November 2018 **ID:** G00350438

Analyst(s): Jay Heiser

Cloud service providers vary in reliability and trustability. Gartner's three-tier model provides sourcing, procurement and vendor management leaders with a practical, risk-based approach to the selection and continuous monitoring of public cloud services.

Key Findings

- The sheer number of cloud service providers (CSPs) is forcing significant changes in vendor security and risk assessment processes.
- Cloud seekers within the enterprise have no patience and will circumvent risk management processes if they perceive the approval process to be too long or unwieldy.
- Cloud service acquisition is often a "take it or leave it" proposition. CSP maturity level impacts its ability to negotiate contract terms or service features.
- The cloud service business model exacerbates market dynamics and provider behavior, resulting in extreme differences between CSP characteristics and reliability.

Recommendations

Sourcing, procurement and vendor management leaders responsible for managing security and risk related to cloud computing programs:

- Ensure efficient and effective selection and management of cloud providers in a complex risk scenario by incorporating a tiering model into your CSP vendor evaluation process.
- Concentrate your CSP vendor assessment and monitoring resources on the growing Tier 2 of midsize CSPs, some of which will be strategically important to specific departments or even your entire organization.
- Avoid putting significant levels of effort into assessing and monitoring the very largest and the very smallest CSPs.

Table of Contents

List of Tables

List of Figures

Strategic Planning Assumptions

By 2021, 90% of public cloud activity will be within CSPs that have undergone a third-party security evaluation.

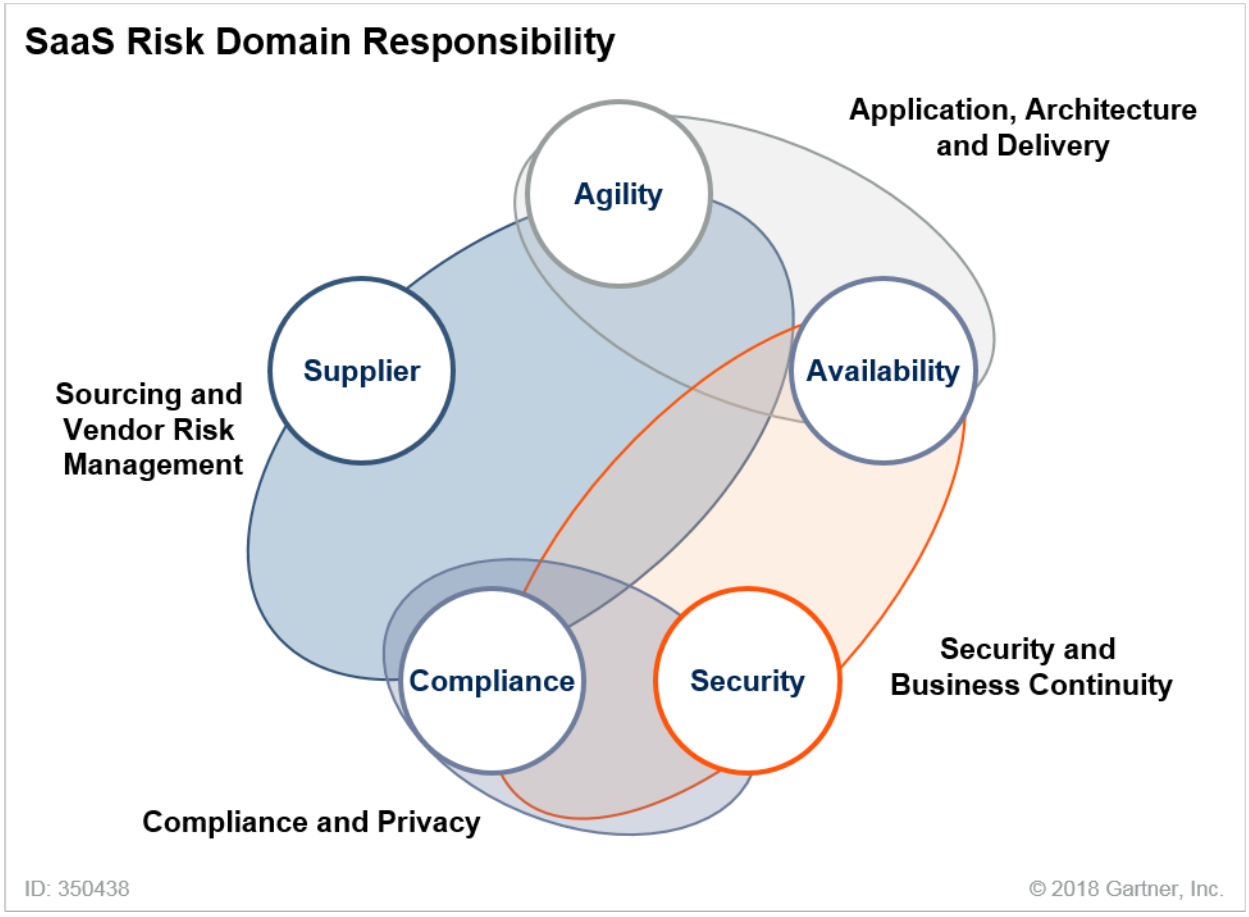
By 2023, over 10% of today's Tier 3 CSPs will be out of business.

Analysis

The scale, speed and novelty of the public cloud are stressing the ability of traditional IT risk management practices to address concerns about CSP performance, compliance, security,

reliability and viability. The large number of CSPs,[1] the rapid rate of cloud change, and the lack of best practices for CSP assessment and management are combining to overwhelm several IT functions that are struggling to reorganize themselves for these new challenges. Figure 1 shows some of the new teaming arrangements that are evolving within the enterprise to address cloud risk.

Figure 1. Managing the Complexity of Public Cloud Risks



Source: Gartner (November 2018)

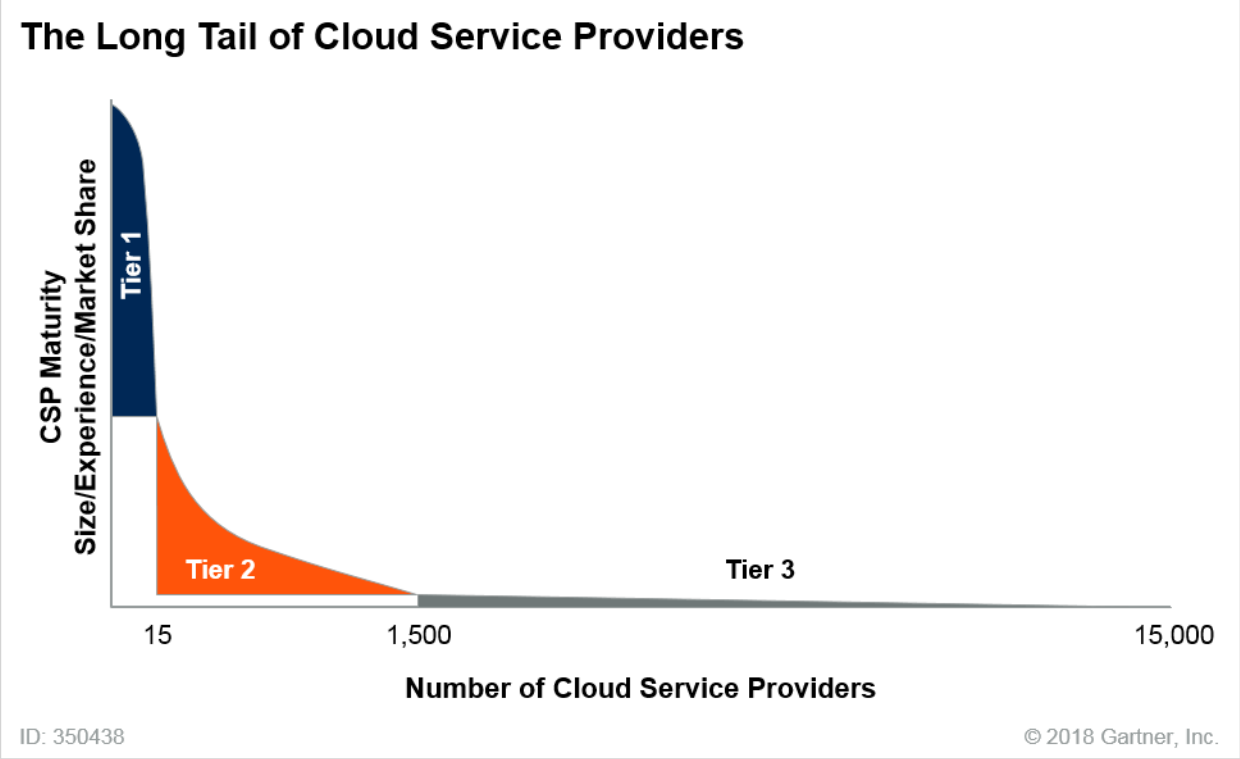
The management of public cloud utilization is further complicated by a cloud service market with unusually exaggerated dynamics, which invalidates assumptions based on precloud vendor assessment and management experience. In a relatively short number of years, cloud service providers have sorted themselves into relatively distinct maturity categories, which are described in Gartner's three-tier CSP maturity model. IT procurement, vendor, security, risk and compliance leaders can apply this model to better understand the relative maturity of prospective and current CSPs. They can then use this insight to inform their CSP acquisition decisions and governance practices, thereby reducing the potential for cloud failures, while increasing the speed of cloud adoption. The purpose of this model is not to precisely place each cloud service provider within an

abstract category, but to provide a conceptual tool that facilitates CSP use decisions and prioritizes the levels of ongoing service provider oversight.

Using the Three-Tier Model to Better Understand CSPs

High tech isn't the only domain in which vendors are routinely conceptualized as fitting within a three-tiered hierarchy. A small number of significant vendors occupy the prestigious first tier, and a greater number of vendors fall into the second and third tiers. It's a conceptual model that is easy to understand, and it provides useful insight into the nature of a market. By recognizing what tier a CSP likely fits into, IT professionals can better inform their cloud purchasing decisions and better plan their ongoing vendor risk management. Figure 2 illustrates the dramatically skewed nature of the cloud service realm. It shows a relatively small and stable population of market-dominating Tier 1 CSPs, a slowly growing set of approximately 1,500 to 2,000 Tier 2 CSPs, and a very long tail consisting of a changing set of thousands of small Tier 3 CSPs.

Figure 2. The Long Tail of Cloud Service Providers



Source: Gartner (November 2018)

A set of closely correlated characteristics — including revenue, market share, number of customers, amount of stored data, level of customer activity, brand-name recognition, media coverage and prestige — differs exponentially between CSP tiers. (A smaller set of characteristics, most significantly the number of years in operation, varies arithmetically between tiers.) As illustrated by the vertical scale in Figure 2, the major differentiator between tiers could be described as maturity, a composite of a service provider's market presence and ability to execute. In comparison to

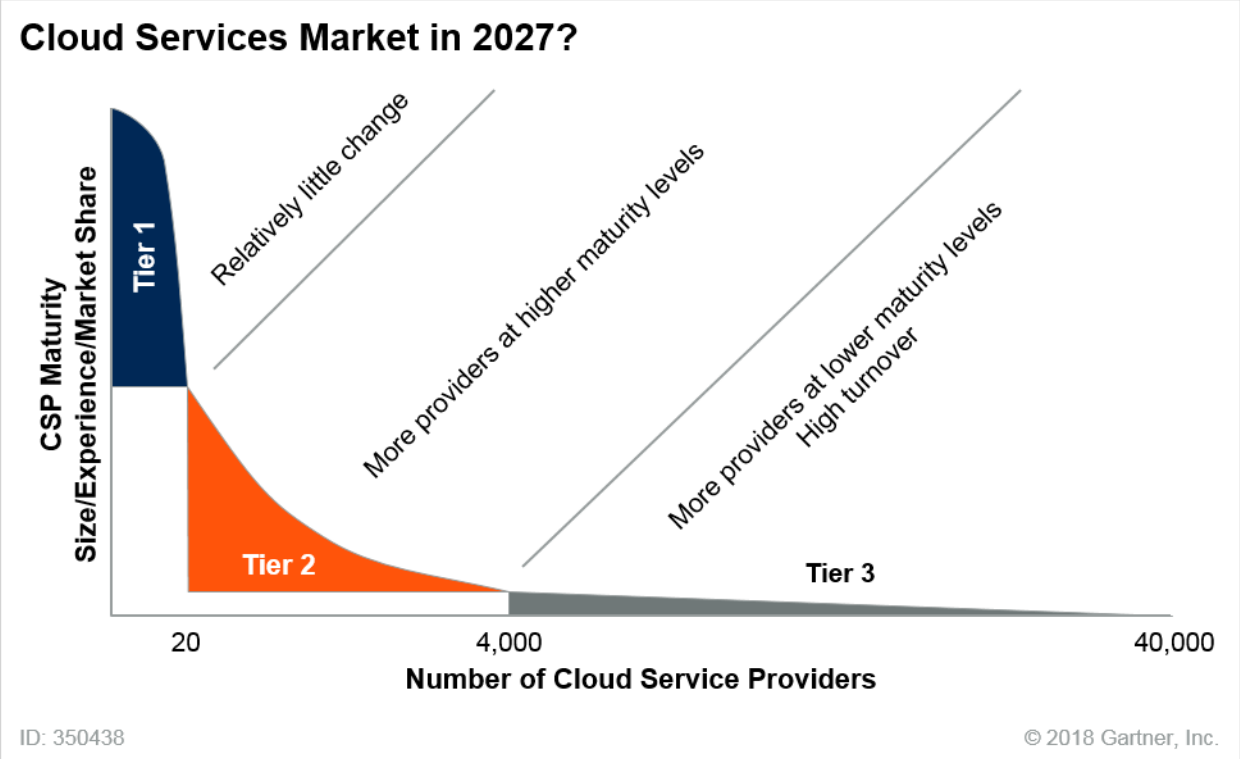
traditional outsourcing, cloud services represent a significant shift of responsibility to the service provider and, consequently, provider maturity is often a strong indicator of vendor utility and reliability.[2] Some of the significant qualitative risk-related differences that explain the variance between CSPs in the different tiers include:

- Transparency and ease of assessment and evaluation
- Security and reliability
- Business stability
- Merger and acquisition potential
- Acceptability to managers, executives, auditors, regulators and other stakeholders
- Size of the ecosystem of compatible and integrated components and services

The dynamics of cloud service markets favor early entrants, giving them an almost insurmountable market advantage. This usually results in a skewed market, with a small number of market leaders and a much larger number of smaller providers (see “Magic Quadrant for Cloud Infrastructure as a Service, Worldwide” and “Magic Quadrant for Sales Force Automation”).

It’s likely that these same market dynamics will continue indefinitely, with only a relatively small increase in the number of top-tier providers.

Figure 3. Cloud Service Tiers Extrapolated to 2027



Source: Gartner (November 2018)

Categorizing CSPs

The relative barriers to market entry and the competitive environment drive the unique dynamics of each tier.

Tier 1

A small and stable number of Tier 1 CSPs are global megavendors, leading virtually every national market. Their dominance is maintained through extremely high barriers to market entry, including not only capital and market mind share, but also significant levels of expertise and intellectual property gained through years of experience. (Amazon Web Services [AWS] did not report that it was profitable until nine years after launching commercial operation, at which point it was claiming $5 billion in annual revenue.[3]) All Tier 1 CSPs provide services in at least two of the three cloud layers (infrastructure as a service [IaaS], platform as a service [PaaS] or SaaS), with the very largest and most mature providers operating in all three layers. They provide a relatively generic set of services to customers in every vertical, of every size and, increasingly, in every part of the globe. Their target market is essentially everybody.

Tier 2

The growing set of middle-tier CSPs is engaged in a struggle for sustainability, with only the very largest hoping to break into the top tier. A growing number do provide services in multiple cloud layers, but most concentrate on one layer, and they only rarely extend across more than two layers. Tier 2 CSPs come in two types, with comparable market strength, but different financial and product status:

- **Category A** is composed of established high-tech vendors that are establishing relatively new public cloud offerings. But, cash doesn't equate to vision, and several very prominent multibillion-dollar high-tech companies have revised their cloud offerings multiple times, or have sold or even discontinued their service.[4] Several companies in this category should be treated as having offerings of mixed maturity levels, with some clearly in the first tier, but others much less mature.
- **Category B** consists of cloud-only (or cloud-primary) providers that have grown large enough to be considered significant. They usually do not have the financial resources of a Category A company; however, after multiple years of focus on a consistent cloud service offering, their product line is, by necessity, relatively stable.

Some middle-tier providers echo the nonspecific market-targeting approach of the Tier 1 providers, while others are carefully focused on specific verticals, limited geographies, or specific corporate roles. Tier 2 providers that are in direct competition with Tier 1 CSPs are under pressure to differentiate themselves, usually by choosing to provide higher levels of customer support or unique features. Competing on price against Tier 1 economies of scale is difficult or impossible.

A large number of small providers — primarily, but not exclusively, SaaS providers — populate the dynamic and growing lowest tier. In complete contrast to Tier 1, Tier 3 has virtually no barriers to entry. The low cost and high convenience of Tier 1 IaaS and PaaS mean that an individual with some code can initiate a SaaS offering on a part-time basis. This low market barrier makes the SaaS market highly dynamic, with many new entrants and many failures. The upside is that it is a rich experimental environment, allowing the exploration of interesting new application types. The downside is that vendors have a relatively high business failure rate. The majority of tiny SaaS providers are not supporting applications that are of strategic significance to most enterprises. But some relatively immature CSPs with fragile business models are offering applications that might be considered mission-critical by a corporate department or a small to midsize organization. IaaS and PaaS startups should be considered as Tier 3 providers, although when started by an existing high-tech provider, they normally have Tier 2 levels of maturity within a few years.

Table 1 summarizes the characteristics of each tier. This is a nominal model, a type of cloud maturity spectrum. Some vendors may be difficult to categorize, which usually means they have some characteristics of two adjacent tiers.

Table 1. Cloud Service Tier Characteristics

Tier 1	Tier 2	Tier 3
■ Over $2 billion in annual cloud service revenue for an IaaS provider, over 1 billion in annual cloud service revenue for an IaaS provider ■ Tens of thousands of paying customers ■ More than 10 years of consistent experience, primarily in cloud ■ Global dominance and brand recognition ■ Universal: Targeting all verticals and regions ■ Service offerings in at least two cloud layers (IaaS/PaaS/SaaS) ■ Multiple third-party security evaluations ■ Clear statement that all stored data belongs to customers and will not be used by the CSP for its own benefit ■ Magic Quadrant Leader	■ Over $40 million in annual cloud service revenue ■ More than 1,000 paying customers ■ More than five years of cloud experience ■ May target a specific vertical ■ May differentiate itself on customer intimacy or product features ■ May be active only in a single country or region ■ Service offerings in one or two cloud layers ■ Challenger or Visionary, if the market is covered by a Magic Quadrant **Category A:** Established high-tech firms still building their cloud business **Category B:** Midsize cloud-only providers	■ No brand-name recognition ■ Primarily SaaS, some PaaS and a few IaaS startups ■ No third-party security evaluation ■ Not a candidate for a Magic Quadrant, but could be a Cool Vendor

Source: Gartner (November 2018)

Purchase Implications

No single form of cloud service provider can ever meet all of the needs of the digital business, and every organization will end up using CSPs from each of the three tiers. To a surprising degree, the service offerings within each provider tier have similar advantages, disadvantages and purchasing complications.

Tier 1

The top tier represents the most stable set of cloud service providers. These CSPs can be relied on to offer the majority of their current product offerings and feature sets for an indefinite amount of time, with upgrade or migration paths offered for any products or features that they significantly change. Tier 1 CSPs not only have the largest set of products and features, but they also sit in the largest ecosystem of compatible product and service providers. This combination of a growing feature set, along with a healthy and vibrant set of third-party add-ons and services, means that Tier 1 providers are most likely to be able to meet future unanticipated needs. (Gartner uses the term “agility risk” to refer to the degree to which a service provider will not be able to meet future needs, a probability that can be especially acute in cloud services [see “A Public Cloud Risk Model: Accepting Cloud Risk Is OK, Ignoring Cloud Risk Is Tragic”]).

Somewhat ironically, given their rich set of feature offerings, Tier 1 providers are constrained by their own success. They rigidly follow a one-size-fits-all approach that refuses to entertain custom functionality or contractual changes. In other words, with a Tier 1 CSP, you get what they offer and nothing more. Tier 1 providers usually adhere strictly to their contracting models, with limited flexibility for contracting changes.

Tier 2

The middle-tier cloud service providers can be the most willing and able to accommodate customer requests. Their need to build a customer base motivates them to at least consider contract concessions, or even unique service levels. Their relative size and sophistication mean that they have the ability to follow through on their commitments. Likewise, Tier 2 CSPs can be the most customer-intimate of cloud service providers, offering higher levels of personal support than are typical of bigger or smaller CSPs. Seeking to differentiate themselves from “generic” Tier 1 providers, they may position themselves as having unique technology, security or regulatory compliance advantages.

Thoroughly evaluate the market and financial viability of a Tier 2 provider before becoming dependent on it. Category A CSPs — existing high-tech firms that are trying to build up a cloud service — usually have enough financial strength from their heritage business to enable them to sell their cloud service below cost., This is especially important as they are exploring potential new offerings and markets. The highly competitive nature of cloud markets encourages them to do so in order to grow their cloud customer base and gain Tier 1 economies of scale. This pricing approach may represent a short-term cost-benefit for their customers, but it also represents a medium- to long-term risk that an unprofitable product line may change significantly, or even be discontinued. Depending on the size of their target market and the number of competitors, Category B CSPs may or may not be under pressure to sell their service below cost. But, if they are, it means they are in a market race to sustainability that will reduce their flexibility and may impact their viability.

Tier 3

The bottom tier of the cloud service market — which is mostly, but not entirely, populated by SaaS services — offers a wide variety of service offerings. This is where much of the application innovation occurs, with startups taking advantage of the low cost and high convenience of PaaS and IaaS providers to host their SaaS or PaaS offerings. With the exception of a few well-financed startups (which normally move to Tier 2 maturity relatively quickly), Tier 3 providers usually lack financial, technical and personnel resources. Many Tier 3 providers, especially those targeting individual customers, are credit card only, with no sales or customer relations staff. Relatively larger Tier 3 providers targeting organizational customers may agree to make contractual and even product feature concessions. But, with such a fragile business model, they may lack the expertise or resources to meet their special commitments, and, of course, if they go bankrupt, all promises and contractual provisions are moot (see Table 2).

Table 2. Tier Implications for Purchase Decision

Tier 1: Stable	Tier 2: Accommodating	Tier 3: Diverse
■ Largest product and feature set ■ Access to an ecosystem of compatible and integrated components and services ■ Little or no flexibility on contract language	■ May have unique features or service levels not available from a Tier 1 ■ May be willing to negotiate and can live up to commitments **Category A:** ■ Can afford to sell below cost ■ Will eventually discontinue unsuccessful offerings **Category B:** ■ Cannot afford to sell below cost, but may be under market pressure to do so	■ Point products — each representing a new vendor relationship ■ Little or no capability to accommodate contract changes or other customization requests

Source: Gartner (November 2018)

Security Risk Assessment

CSP maturity has a huge impact on security level of effort, transparency and, hence, risk implications. Taking maturity into account can help inform the relative level of effort needed to evaluate the security posture and regulatory acceptability of cloud service providers, enabling security leaders to focus their risk assessment resources where they are most beneficial.

Tier 1

The major cloud service providers have all undergone multiple formal third-party security evaluations. Tier 1 CSPs have become increasingly willing to share detailed information about their security technology and internal processes, sometimes allowing access to hundreds of pages of material prepared by external security assessors. While it is never safe to assume "perfect" security, no evidence suggests that significant amounts of time spent evaluating Tier 1 cloud service provider security posture are beneficial. In other words, at any particular moment, a Tier 1 CSP may have a security problem, but there is nothing that its customers could do about it before the CSP finds and remediates the vulnerability.

Tier 1 providers have demonstrated their ability to exploit DevOps processes to minimize vulnerabilities, transparently delivering updates in a staged process that limits the impact of code mistakes. When the Spectre/Meltdown vulnerabilities hit the news in early 2018, it quickly became apparent that the Tier 1 IaaS providers had been aware of the vulnerability type, and had already implemented patches for hardware, the hypervisor and machine images (see "Security Leaders Need to Do Seven Things to Deal With Spectre/Meltdown"). Of course, if specific security features or compatibility are required, then those aspects of the CSP's offering must be evaluated. It always remains the case that much of the responsibility for overall security lies with the customer. So, time spent doing an in-depth analysis of a Tier 1 CSP's SOC 2 report would be better applied toward

working out procedures for how to use the service securely (see “How to Develop Infrastructure-as-a-Service Security Skills”).

Tier 2

For most organizations, concentrating on Tier 2 CSPs will be the most effective use of their CSP security and risk assessment efforts. Many Tier 2 services are strategically important to their customers, providing a mission-critical service either to a business unit or to the entire enterprise; yet many midsize CSPs remain undesirably immature. This uneasy balance between strategic significance and provider fragility suggests a need for higher levels of risk assessment attention.

Most Tier 2 CSPs are doing a more than adequate job of maintaining their security posture. But if the use case is a strategic one, then a Tier 2 CSP’s security level of effort and financial status should never be taken for granted. Tier 2 providers are not necessarily less secure than their larger competitors — indeed, some midtier providers position their offerings as having a security or compliance advantage — but their security status should be thoroughly evaluated (see “How to Evaluate Cloud Service Provider Security”). Approximately half of Tier 2 CSPs have completed a third-party security evaluation, and the number is growing. Those providers that have not completed an evaluation are not necessarily less secure than those that have. They are failing to provide the form of evidence that within the next few years will be considered a mandatory requirement for strategically important cloud services.

Tier 3

It isn’t necessarily the case that Tier 3 CSPs should automatically be considered as unsecure. No evidence indicates that security failure is a significant problem, but it is effectively impossible to make a definitive security risk assessment of a tiny SaaS provider. Risk transparency comes with business maturity, and no Tier 3 provider has the wherewithal to complete an ISO 27001 or SOC 2 assessment. Additionally, their ability to reliably complete a detailed security questionnaire is questionable. Market pressure means that, whatever their status is today, it may change radically tomorrow. Significant levels of effort spent evaluating the security of a Tier 3 CSP are usually not worth the effort (see Table 3).

Table 3. Tier Implications for Security Risk Assessment

Tier 1	Tier 2	Tier 3
▪ Security and reliability can be taken for granted ▪ Multiple third-party evaluations ▪ No potential for unanticipated business failure ▪ Acceptable choice for regulators and other stakeholders	▪ Security and reliability are likely acceptable, but must be carefully evaluated ▪ May have undergone a third-party evaluation ▪ May allow customer audits	▪ Security and reliability can never be expected ▪ No third-party evaluation ▪ Financial fragility means status may change quickly

Source: Gartner (November 2018)

Mitigating Risk/Sourcing

Keeping pace with the demands of today's enterprises for cloud service providers challenges sourcing leaders and requires different contracting approaches based on tiering. The flexibility and focus change with each tier level. Traditional Mode 1 sourcing has given way to the Mode 2 agile approach to contracting to reduce the risk of impatient cloud seekers circumventing sourcing and directly contracting with providers.

Tier 1

Large established CSPs offer homogeneous products and little room for customization. They succeed in having the ability to service thousands of customers, providing scalability, security and redundancy. They traditionally have approached contract negotiations with a "take it or leave it" attitude based on the premise that they are only one of a few large players in the market. The ability to negotiate with these providers is largely dependent on the size, strategic imperative and length of the deal. Focus should be on automation, innovation and business outcomes.

Tier 2

Middle tier CSPs may provide an opportunity to customize contracts and will negotiate more readily because they are eager for business, offering customers tailored product offerings. Leveraging these providers for strategic initiatives, while managing the potential for them to be less reliable and more acquisition-prone, is a balancing act. It requires a different focus on contracting to reduce risk and allow for flexibility to change providers if the service offering changes. Ideally, strong SLAs should be in place to drive the desired behaviors.

Tier 3

The instability and risk of smaller CSPs require a different approach in contracting. While sourcing managers may be able to negotiate stronger terms based on the provider's desire to gain business, the strategy should be to reduce risk and provide flexibility. Proper vetting early on and continuous monitoring of important vendors can help reduce the potential for future disruptions. Strong SLAs are desired, but may not be an effective mitigator of risk if the CSP is prone to bankruptcy or closure (see Table 4).

Table 4. Tier Implications for Sourcing Risk

Tier 1: Are Non-negotiable	Tier 2: Negotiate and Deliver	Tier 3: Present Bankruptcy Risk

■ Expect less flexibility in negotiation
■ Review efficiencies in automation and ask for reductions in price
■ Request automation and innovation clauses
■ Seek outcome-based SLAs
■ Include clauses that prevent the service provider from forcing a change in your subscription by upgrading its technology
■ Negotiate out of the contract the ability to unilaterally change terms
■ Ask about uncapped or unlimited liability in areas that the provider can control
	■ Negotiate for specific business needs
	■ Include change-of-control provisions (advance notice and termination options)
	■ Push for stronger discounts and SLAs
	■ Create flexibility in termination clauses
	■ Ask for code escrow on products, if worth the price and feasibility
	■ Ask for certificates and audit rights
		■ Aim for flexibility in terminations:
		  ■ Convenience
		  ■ Bankruptcy
		  ■ Change of control
		  ■ Poor performance
		■ Negotiate exit clauses
		■ Assess which applications and data are appropriate for this type of environment
		■ Create a stable of alternates
		■ Negotiate access to equipment and data if a closure occurs

Source: Gartner (November 2018)

Ongoing Monitoring/Vendor Management

Today's enterprise is finding itself dependent on hundreds of cloud service providers, most of which are engaged in a multiyear struggle for market sustainability. The number of vendors in use and the uniquely dynamic characteristics of cloud service markets suggest a strong benefit in continuous monitoring of provider status, typically within some sort of vendor risk management program. The disappointing ambiguity of CSP security evaluation processes also indicates a need for continuous monitoring. However, do not put significant effort into a flawed evaluation of a provider's status at a single point in time. Instead, redeploy those vendor risk management resources into an ongoing effort to detect changes in provider financial, security or regulatory compliance status. Each tier has significantly different implications for contingency planning, and the time periods allowed for customer transition away from obsolete services correspond to vendor size.

Tier 1

The top CSPs are highly stable. While they continuously offer new capabilities, including some gained through acquisition, they are financially motivated to avoid doing anything that would encourage existing customers to reduce their level of utilization. Therefore, Tier 1 CSPs avoid product obsolescence. When they do make incompatible upgrades or product discontinuations, they normally allow at least 12 months for the migration, and provide backward compatibility. When a Tier 1 provider acquires another service, it typically does whatever is necessary to maintain the

associated customer base. Planning for the contingency of a Tier 1 vendor failure or bankruptcy is probably not worth the effort.

Tier 2

Tier 2 CSPs normally account for the majority of organizational continuous monitoring attention, given the likelihood that multiple strategically significant applications or use cases will be located within relatively immature services that may be struggling to gain market stability. The very largest and most established high-tech firms have been surprisingly inconsistent in their attempts to build new businesses in the public cloud. Unsuccessful product lines are sometimes canceled, and acquisitions may be awkwardly forced onto existing customers. The financial stability of Category A vendors means that customers of service lines that turned out to be experimental failures can be given a lengthy transition period, making customer contingency planning less critical.

Having grown into their Tier 2 status over a period of years, Category B vendors have stable product plans, but may have weaker financial status. Even financially healthy CSPs may be acquisition targets of Category A vendors attempting to break into Tier 1 status.[5] An acquirer may make no significant changes to the original service, and usually has the financial ability to allow existing customers a six- to 12-month transition period. Tier 2 providers teetering on the edge of insolvency are often able to sell themselves to a larger CSP. But a small number of them have been unable to do so, leaving their customers stranded with a relatively short time period to transition to some other service.[6] Organizations dependent on a Category B CSP should continuously monitor that vendor's financial and product status, and should develop contingency plans that could be invoked immediately in case of a CSP business failure.

Tier 3

While the overall track record has been relatively good, tiny CSPs should not be considered reliable. Always assume that a Tier 3 CSP may shut down operations with no advance warning, making all customer data permanently inaccessible. No Tier 3 CSP should ever be used as the sole form of storage for critical data. If data loss would be unacceptable, then copies of that data should be stored outside of the Tier 3 CSP. The contingency plan should further consider how that application would be redeployed in a new production environment, which can be extremely difficult for structured data. For the most part, the smallest providers are not used for critical scenarios, meaning that contingency planning is unnecessary. If a tiny CSP is considered critically important, then ongoing vendor monitoring would be desirable, but may be impractical (see Table 5).

Table 5. Tier Implications for Continuous Monitoring

Tier 1: Minimal Benefit	Tier 2: Most Benefit	Tier 3: Impractical
Minimal need for continuous monitoring: ■ Stability of existing product offerings can be relied on ■ May make acquisitions; unlikely to be acquired ■ Vendor contingency plans are unlikely to be invoked	Vendor status can change rapidly, making continuous monitoring necessary: ■ Vendor contingency plans are probably necessary **Category A:** ■ May cancel product line or significantly change product direction, including through acquisition ■ Product cancellation may allow customers one year to migrate data **Category B:** ■ May be an acquisition target ■ Vendor shutdown typically offers three to 12 weeks to obtain data	Continuous monitoring may be impractical, but enterprise use of the service is usually too insignificant to be worth the effort: ■ Vendor contingency plans may not be worth the bother ■ Likely too small to be considered for an acquisition ■ Vendor shutdown might occur immediately, without opportunity to obtain data

Source: Gartner (November 2018)

Additional analysis for the Mitigating Risk/Sourcing section was provided by Stephanie Stoudt-Hansen.

Gartner Recommended Reading

Some documents may not be available as part of your current Gartner subscription.

“Cloud Procurement Skills and Guidelines Optimize Results and Minimize Risk”

“Clouds Are Secure: Are You Using Them Securely?”

“Developing Your SaaS Governance Framework”

“Formalized Vendor Risk Management Lessens the Probability of Business Disruption”

“Reduce Security Risks by Mastering Cloud Contracts and Security Standards”

“Develop Contingency Plans for Your Critical Suppliers, or Risk Business Disruption”

Evidence

[1] According to the “Netskope Cloud Report — October 2018,” “Enterprises have an average of 1,246 cloud services in use, an increase from 1,181 last report.”

[2] As an example of the relationship between tiers and product capability, see “Critical Capabilities for Public Cloud Infrastructure as a Service, Worldwide,” which shows the top-tier CSPs as outscoring the lower tier CSPs in most categories.

[3] “Amazon Web Services ‘Growing Fast,’” BCC News.

[4] “NTT Data Closes Acquisition of Dell Services,” NTT Data.

“Barracuda Kills CudaDrive and Copy Cloud Storage Services,” The Register.

[5] “IBM Buys SoftLayer, a Cloud Computing Firm,” The New York Times.

[6] “Cloud Provider Nirvanix Gives Customers Two Weeks to Vacate Data,” Information Age.

GARTNER HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
USA
+1 203 964 0096

Regional Headquarters
AUSTRALIA
BRAZIL
JAPAN
UNITED KINGDOM

For a complete list of worldwide locations,
visit http://www.gartner.com/technology/about.jsp

Providers' Strengths and Weaknesses: Cloud Migration, Hybrid Infrastructure and Workplace Services

Published: 19 December 2018 **ID:** G00369166

Analyst(s): Claudio Da Rold, Mark Ray, DD Mishra, Daniel Barros, David Groombridge

More than 600 customer references (the voice of the customer) clearly show undeniable strengths and weaknesses for 34 global infrastructure service providers. Sourcing, procurement and vendor management leaders can leverage our 2018 findings to identify the provider to best meet their needs.

Key Challenges

- Due diligence often follows the selection phase as customers evaluate proposals without an objective evaluation of reality. This leads to the selection of the wrong provider.
- All major providers claim automated cloud discovery and migration tools and low cost, highly automated cloud migration farms. The reality is that a gulf in performance exists in this area.
- Many major providers claim customer centricity and support for digital workplace transformation. However, some providers get scores on specific items as low as 1.0 (e.g., chatbots).
- Providers claim investments in end-to-end integration and management of hybrid infrastructures (tools, IA and IP), yet some get scores as low as 2.0 on specific items (e.g., intelligent automation).

Recommendations

Sourcing, procurement and vendor management leaders in the strategy and selection phase for sourcing infrastructure services must take these steps:

- Identify three to five major critical success factors from the 12 metrics we provide and align them to your objectives. Evaluate the gap between current status and targeted objective as a measure of the required change management.
- Select the providers with the best fit to your prioritized critical success factors, and use the shortlist you obtain to kick off an exploratory engagement model for transformational deals.

- Add regional or niche providers to your shortlist by engaging early in the process with their references, while gathering information through Gartner Peer Insights. Compare niche providers and the global ones against the same data-driven metrics.

Table of Contents

List of Tables

List of Figures

Introduction

This document was revised on 27 December 2018. The document you are viewing is the corrected version. For more information, see the Corrections page on gartner.com.

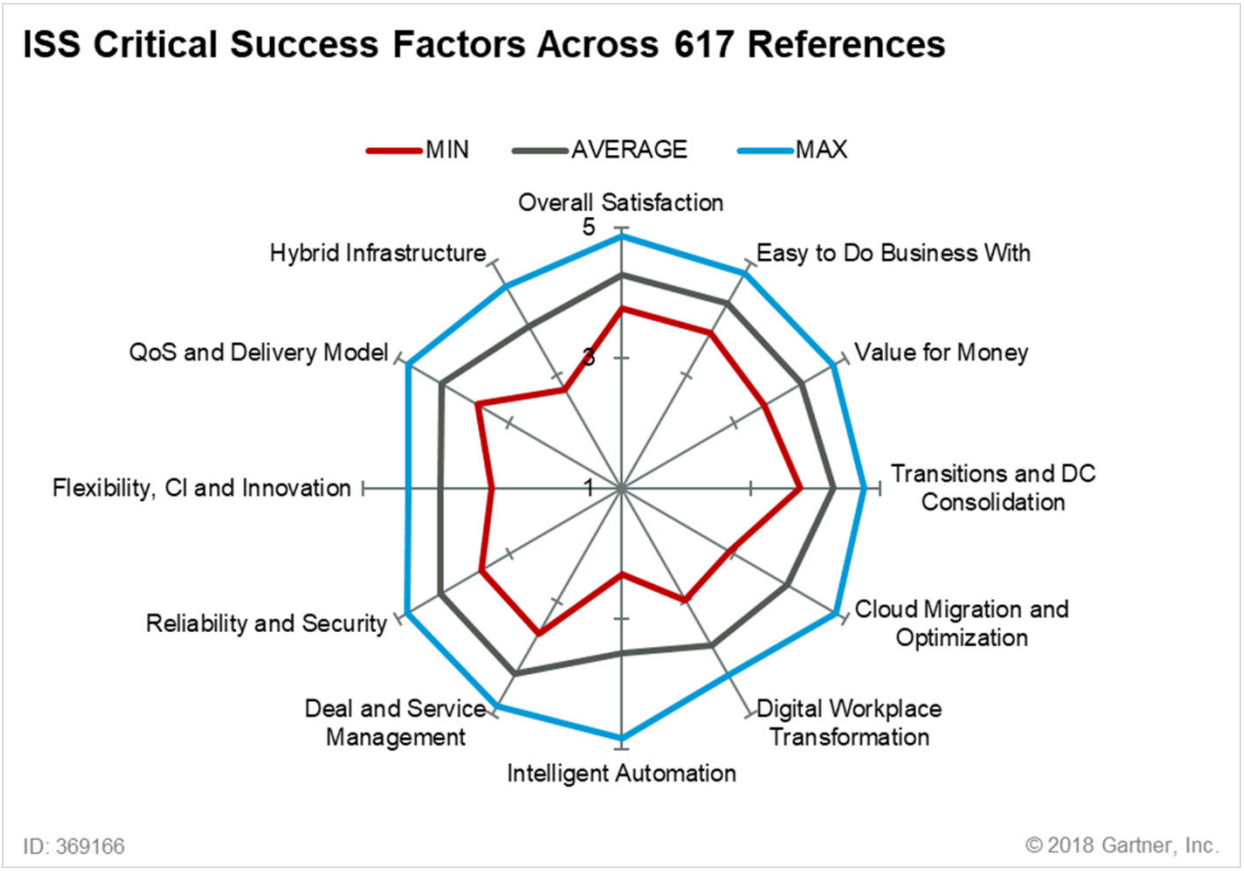
The implementation and management of business innovation-driven technologies, such as hybrid infrastructures extending to cloud, mobile, IoT, edge computing and artificial intelligence, are rapidly becoming games of industrial scale based on API platforms. In such a rapidly moving environment, there are two powerful fact-based ways to identify the best-fit providers: customer references and industrial performances.

The voice of the customer clearly shows that even the most satisfied customer identifies the global providers' weaknesses, not only their undeniable strengths.[1] Gartner has measured the voice of the customer in the infrastructure service market through 617 global references. Respondents were surveyed during the 2018 infrastructure services Magic Quadrant research for Data Center

Outsourcing, Hybrid Infrastructure Management and Managed Workplace Services across North America, Europe and Asia/Pacific.[2]

Figure 1 shows — on a scale from 1 (poor) to 5 (delighted) — that major infrastructure service providers have been successful with their references on several key aspects including "value for money" and "easy to do business with." However, there is significant variability; the differences between minimums and maximums range between 1 and 2 points on a 5-point scale (which is 20% to 40% lower than best scores). Also, references (e.g., marquee customers) have 20% higher-than-general satisfaction levels,[3] which means that the gap between high satisfaction and average delivery is about 50% and more.

Figure 1. 12 Infrastructure Services Sourcing Critical Success Factors Across 617 References



Note: Data derived from Gartner Infrastructure Managed Services References Surveys.
Ratings are based on a scale 1 to 5, where 1 = Completely Dissatisfied, 5 = Completely Satisfied

Source: Gartner (December 2018)

The data clearly indicates that, even for marquee customers and best industry brands, many aspects of digital services are still a work in progress. Look at the minimum scores in Figure 1 for cloud migration and optimization, intelligent automation, hybrid management, digital workplace transformation, with flexibility, continuous improvement and innovation. This research provides

sourcing, procurement and vendor management leaders with the data required to benchmark their results and expectations for customer satisfaction, and implement agile sourcing strategies and selection processes for their next global infrastructure service contracts. See “How to Select Global Infrastructure Service Providers in 90 Minutes Instead of 90 Days Using Fit, References and Performance Metrics.”

Analysis

Identify the Major Critical Success Factors for Your Initiative and Mind the Gap

A clear identification of sourcing initiatives’ objectives is paramount to success of the entire sourcing life cycle. Today, all organizations in the world are looking to accelerate innovation, cut cost, get new skills and capabilities, and optimize performances. Working against generic objectives is a waste of time. Specific, measurable, agreed, realistic, time-bound (SMART) objectives provide a clear definition of success.

Table 1 reports the 12 critical success factors we have measured across the 2018 infrastructure services (IS) references across the globe (Note: customers can access regional or industry view of these measures through inquiries). The overall average customer satisfaction of the references (the providers’ happiest customers) is 4.22 for data center services and 4.25 for workplace services. The average customer satisfaction (all surveyed customers) ratings are 3.1 for data center and service desk, and 3.0 for workplace services.[3] This means that the marquee customers (references) satisfaction can be defined as the target of excellent outsourcing relationship, achieved when the sourcing, procurement and vendor management life cycle is managed without flaws. Each of the 12 factors presented in Table 1 is measured through an average of five subfactors that incorporate the multiple aspects associated with each factor (see Note 1). Some of the extreme scores mentioned in the introduction are averaged out; but those detailed scores are still available to customer through analyst inquiry.

Table 1. The 12 DCO/HIMS and Managed Workplace Service Sourcing Critical Success Factors vs. References Statistics

	Your Priority	Minimum	Average	Maximum
Overall Satisfaction		3.75	4.27	4.86
Easy to Do Business With		3.76	4.28	4.81
Value for Money		3.55	4.22	4.79
Transitions and DC Consolidation		3.75	4.28	4.75
Cloud Migration and Optimization		2.94	3.96	4.83
Digital Workplace Transformation		2.97	3.77	4.31
Intelligent Automation		2.31	3.53	4.83
Deal and Service Management		3.57	4.29	4.86
Reliability and Security		3.50	4.23	4.83
Flexibility, CI and Innovation		3.01	3.80	4.29
QoS and Delivery Model		3.57	4.21	4.81
Hybrid Infrastructure		2.75	3.87	4.58

Source: Gartner (December 2018)

To effectively source infrastructure services:

- Ban generic objectives from your sourcing initiatives. Replace them with SMART objectives for each initiative by engaging and collaborating with key business and IT stakeholders.[4]
- Select the three to five most important criteria for the achievement of your SMART objectives across those identified in Table 1.
- Assess your current levels of customer satisfaction on to the three to five identified critical success factors, and use the difference between today and the future required levels to judge the level of change needed.

Select the Providers With the Best Fit for Your Prioritized Critical Success Factors

Table 2 compares the scores of the 34 service providers positioned in Gartner DCO/HIMS and managed workplace services (MWS) Magic Quadrants against the 12 infrastructure services sourcing (ISS) critical success factors.[2] This data can be used to shortlist service providers based on

a coherent and trusted fact base, derived from providers' elected customers, surveyed by an independent party and published by Gartner. Additional ratings and reviews of enterprise technology solutions by end-user professionals are available online in Gartner Peer Insights communities, and in the User Review section for each Magic Quadrant.

Figure 2. 34 Major Providers' Results Against the 12 ISS Critical Success Factors

34 Major Providers' Results for 12 ISS Critical Success

Critical Success Factors	Overall Satisfaction	Easy to do business with	Value for money	Transitions and DC Consolidation	Cloud Migration and Optimization	Digital Workplace transformation	Intelligent Automation	Deal and Service Management	Reliability and Security	Flexibility, CI and innovation	QoS and Delivery Model	Hybrid Infrastructure
YOUR PRIORITY												
Accenture*	4.27	4.35	4.06	4.33	4.14		3.16	4.36	4.27	4.12	4.22	4.04
Atos	4.11	4.17	4.21	4.17	3.95	3.98	3.55	4.36	4.14	4.01	4.10	4.27
Bell Techlogix**	4.00	4.21	4.07	4.29	4.67	4.01	4.38	4.21	4.33	3.86	4.14	
C3i Solutions**	4.60	4.56	4.79	4.56	4.83	4.02	3.89	4.56	4.60	4.07	4.66	
Capgemini1	4.11	4.08	3.99	4.02	3.59	3.61	3.19	4.13	4.20	3.72	3.98	3.17
Centurylink*1	3.85	3.72	3.80	3.89	2.94		2.71	3.57	3.65	3.34	3.57	3.44
CGI*1x	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Claranet*3	4.63	4.63	4.50	3.75	4.08		4.83	4.39	4.25	3.85	4.29	4.38
Cognizant1	4.28	4.34	4.24	4.31	3.94	2.97	3.66	4.27	4.29	3.80	4.26	4.23
Compucom**	4.46	4.63	4.54	4.75	4.17	4.11	4.41	4.46	4.57	4.15	4.65	
Computacenter**3	4.29	4.36	4.24	3.86	4.50	4.31	3.67	4.23	4.67	3.55	4.15	
DXC Technology	3.73	3.70	3.68	3.77	3.10	3.22	3.03	3.77	3.79	3.01	3.64	2.75
Ensono*2	4.38	4.49	4.39	4.15	3.92		2.50	4.53	4.17	3.82	4.17	3.75
Fujitsu	4.10	4.05	4.00	4.10	3.60	3.59	3.18	4.04	4.11	3.59	4.06	3.95
Genpact**	4.86	4.86	4.79	4.71	4.00	4.22	4.56	4.86	4.67	4.29	4.81	
Getronics**	4.11	4.28	4.11	4.56	3.67	3.80	4.00	4.28	3.50	3.52	4.15	
HCL Technologies	4.13	4.31	4.29	4.23	4.08	3.72	3.45	4.26	4.34	3.94	4.26	4.38
IBM	4.11	3.87	3.96	4.00	3.80	3.72	3.63	4.16	4.37	3.62	4.10	3.82
Infosys*1	4.18	4.39	4.30	4.02	3.85		3.15	4.49	4.29	3.96	4.01	4.04
Insight**2	4.57	4.43	4.57	4.57	4.25	3.59	4.33	4.36	3.50	3.95	4.43	
Long View Systems**2	4.33	4.56	4.39	4.56	4.00	3.73	4.50	4.50	4.75	3.70	4.37	
NTT Data**	3.96	4.09	4.05	4.24	3.92	3.28	2.49	4.01	3.63	3.48	4.04	3.22
Orange Business Services*3	3.75	3.75	3.55	3.87	3.67		2.96	4.07	3.70	3.64	3.90	3.54
Pomeroy*2	4.63	4.66	4.44	4.38	3.50	3.65	3.98	4.54	4.20	3.58	4.50	
Sopra Steria*3	4.75	4.58	4.50	4.58	3.33		3.20	4.50	4.83	3.83	4.20	3.13
Stefanini**1	4.45	4.57	4.23	4.58	4.29	3.64	3.50	4.34	4.00	3.69	4.36	
Sungard AS*1	4.33	4.04	4.04	4.53	3.78		2.31	4.27	4.29	4.14	4.27	4.52
Tata Consultancy Services	4.28	4.38	4.28	4.32	4.01	3.86	3.57	4.32	4.36	4.06	4.22	4.03
Tech Mahindra*x	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Tieto*3	4.13	4.29	3.88	4.58	4.25		3.04	4.38	4.38	3.70	3.91	3.43
T-Systems1	4.44	4.31	4.32	4.54	4.33	3.90	3.74	4.42	4.58	3.98	4.37	4.29
Unisys1	4.47	4.24	4.27	4.35	4.36	3.75	3.12	4.30	4.06	3.96	4.37	3.92
Wipro	4.16	4.23	4.31	4.26	4.19	4.13	3.72	4.31	4.21	3.90	4.28	4.18
Zensar Technologies2	4.08	4.33	4.22	4.11	4.03	3.81	3.57	4.21	4.52	3.81	4.14	4.58

*DCO/HIMS only; **) MWS Only; 1 NA and EU; 2 NA Only; 3 EU Only; 4 Asia/Pacific Only; x No references provided
ID: 369166

Note: Results derived from vendors' customer references for data center outsourcing (DCO) and MWS Magic Quadrants. This analysis is not intended as a strict statistical evaluation of the listed vendors. Rather, the data presented supports directional findings from vendor-provided customer references. For providers with less than 15 references that are marked with an

asterisk (*), the information provided should be considered anecdotal evidence and confirmed with additional direct checks of the providers' references during the selection or due diligence phase.

Source: Gartner (December 2018)

To successfully source infrastructure services:

- Use the three to five critical success factors selected in the previous step to identify the providers that are delivering the best results to their references.
- Put this analysis in the context of a broader set of factors. Evaluate the geographical and functional fit and the industrial performances identified in "How to Select Global Infrastructure Service Providers in 90 Minutes Instead of 90 Days Using Fit, References and Performance Metrics."
- Add niche or regional providers to your shortlist, as explained in the next recommendation.
- Start an agile, exploratory approach by meeting with shortlist providers to understand how they would afford the deal and perform against the selected critical factors while achieving the SMART objectives. Evaluate the provider's approach and ability to manage the gap between existing and expected performances using proof of concepts and pilots.

Complete the selection and negotiation process based on your compliance requirements, engaging the shortlisted service providers through a focused RFP, a competitive dialogue and/or a parallel negotiation process. See "Toolkit: Outsourcing Contract — Attachment N — SOW, SLA, OLA, Price, Behavior Drivers" and "Toolkit: Statement of Work for Managed End-User Computing and Print Services."

Add Vertical, Regional or Niche Providers to Your Shortlist

Table 2 provides the macro geographical and functional coverage through inclusion in the regional Magic Quadrants. It also provides the number of references for each provider for you to judge the quality of the data reported.

The 34 providers that reported clearly represent a formidable set of technology and services capabilities delivered across most areas of the world. These providers have service revenue ranging from well below US$500 million to more than US$45 billion. Unique deal factors may nevertheless require the leverage of additional providers. These factors may include unique vertical requirements, regional capabilities, need for cultural alignment, specific IP or skills in fast-moving technologies (AI, blockchain, IoT) or a very high speed and agility.

Table 2. List of Magic Quadrant Geography Coverage and Number of References, 2018

Participant and Global Reference	DCO/HIMS North America	DCO/HIMS Europe	DCO/HIMS Asia/Pacific	MWS North America	MWS Europe	DCO/HIMS References	MWS References	Total References
Accenture	x	X	x			26		26
Atos	x	X	x	x	x	20	18	38
Bell Techlogix				x			7	7
C3i Solutions				x			10	10
Capgemini	x	X		x	x	19	17	36
Centurylink	x	X				10		10
CGI	x	X				0	0	0
Claranet		X				4		4
Cognizant	x	X		x	x	18	17	35
CompuCom				x			13	13
Computacenter					x		6	6
DXC Technology	x	X	x	x	x	13	16	29
Ensono	x					12		12
Fujitsu	x	X	x	x	x	27	17	44
Genpact				x			7	7

Participant and Global Reference	DCO/HIMS North America	DCO/HIMS Europe	DCO/ HIMS Asia/ Pacific	MWS North America	MWS Europe	DCO/HIMS References	MWS References	Total References
Getronics					x		7	7
HCL Technologies	x	X	x	x	x	22	19	41
IBM	x	X	x	x	x	25	13	38
Infosys	x	X				14		14
Insight				x			7	7
Long View Systems				x			9	9
NTT Data	x			x	x	7	6	13
Orange Business Services		X				10		10
Pomeroy				x			8	8
Sopra Steria		X				4		4
Stefanini				x	x		20	20
Sungard AS	x	X				12		12
Tata Consultancy Services	x	X	x	x	x	27	20	47
Tech Mahindra	x	X	x					0
Tieto		X				8		8
T-Systems	x	X			x	13	4	17

Participant and Global Reference	DCO/HIMS North America	DCO/HIMS Europe	DCO/HIMS Asia/Pacific	MWS North America	MWS Europe	DCO/HIMS References	MWS References	Total References
Unisys	x			x	x	6	13	19
Wipro	x	X	x	x	x	31	17	48
Zensar	x			x		10	8	18
Total	**20**	**20**	**9**	**20**	**15**	**338**	**279**	**617**

Source: Gartner (December 2018)

When adding vendors to your shortlist, consider the following actions:

- Adopt a collaborative and iterative approach working with business units and product/process owner and enterprise architects to ensure business strategy alignment, and I&O delivery managers and solution architects to understand detailed capabilities. If required, add external market or technology expertise to identify vertical, regional or niche providers that have specific capabilities that could be leveraged to achieve the SMART objectives.
- Leverage multiple approaches to this evaluation. Gartner sources include:
  - IT services market share reports (providing a list of providers, revenue and growth per geography and service area).[5]
  - Hype Cycles, especially for technologies and solutions in the early stages, report a list of relevant market players, as do our Cool Vendors reports.
  - Market Guides, for emerging markets especially, provide definitions, market trends and a list of representative providers.
  - Peer Insights is Gartner's platform for ratings and reviews of enterprise technology solutions by end-user professionals for end-user professionals. As such, it reports customers ratings aligned with our market definitions. Also, our Magic Quadrants provide further references covering additional customers and providers.
  - "Toolkit: Identify the Right Company From 80+ Agile/DevOps Service Providers," addresses agile and DevOps providers with geographical and functional information
  - "Toolkit: Global Market Scan for Selecting Service Providers in Business and Application Services" provides a list of 400 service providers with specific information on geographical fit and service competencies.
  - Inquiry with Gartner analysts covering a specific technology, vertical or service area can be a source of additional insight into emerging market players.
- Conduct active reference checks. Leverage the questions associated to the 12 critical factors listed in Note 1.
- Make the niche providers and the global ones compete against the same data-driven approach to maximize competitiveness and success rate.

Gartner Recommended Reading

Some documents may not be available as part of your current Gartner subscription.

"Infrastructure Services Sourcing Strategy: Key Reasons to Outsource"

"Infrastructure Services Sourcing Strategy: Practical Principles for Dynamic Insourcing Versus Outsourcing"

“Infrastructure Services Sourcing Strategy: Practical Principles for Sourcing IOT and Digital Platforms”

“How to Select Global Infrastructure Service Providers in 90 Minutes Instead of 90 Days Using Fit, References and Performance Metrics”

Evidence

[1] During the research process for Gartner Magic Quadrants, service providers included in the research are asked to provide a minimum number of their customer references. The process after the identification of the references is completely carried out by Gartner research and providers never know what answers each customer provide to us. The references are surveyed online and the data is used to confirm or compare with providers’ capabilities, results and strategic directions, as well as used for this publication. Providers are interested in getting high score from their references, so it’s fair to assume that the references represented in this research are across the most satisfied customers of each provider (e.g., marquee clients). Additionally high scores associated to a low number of references must be seen with caution and should be confirmed with additional direct checks of the providers’ references during the selection or due diligence phase.

[2] The reference reported in this research has been surveyed as part of the following Magic Quadrant and critical capability analysis:

- “Magic Quadrant for Data Center Outsourcing and Hybrid Infrastructure Managed Services, Europe”
- “Magic Quadrant for Data Center Outsourcing and Hybrid Infrastructure Managed Services, North America”
- “Magic Quadrant for Data Center Outsourcing and Hybrid Infrastructure Managed Services, Asia/Pacific”
- “Magic Quadrant for Managed Workplace Services, North America”
- “Magic Quadrant for Managed Workplace Services, Europe”
- By January 2019, a new Magic Quadrant covering MWS in Asia/Pacific will add to this roster of major IS Magic Quadrants

[3] Average satisfaction for major outsourced functions is in the 3 to 3.5 range on a scale of 5. See Table 1. The What: Typical Managed Services Sourcing Functions (Service Towers) in “Infrastructure Services Sourcing Strategy: Practical Principles for Dynamic Insourcing Versus Outsourcing” and “IT Key Metrics Data 2018: Key Outsourcing Measures: Outsourcing Profiles: Current Year.” More specifically, the average customer satisfaction are 3.1 for data center and service desk, and 3.0 for workplace services. At the same time the reference (marquee customers) average satisfaction is in the 4.2 to 4.3 range for data center and workplace managed services and in general.

[4] Identify key drivers and objectives in the very early phases of each IS sourcing initiative. Identify “nice to have” versus “must have” priorities. Put stakeholder expectations in context. Guide IS

leaders and other stakeholders to spell out their definition of success for the initiative in a quantitative form.

[5]"Market Share: IT Services, 2017" and "Market Share Analysis: IT Services, Worldwide, 2017"

Note 1 Detailed Question Items Associated With the 12 ISS Critical Success Factors

Overall Satisfaction

- DCO: Please rate your overall experience with this vendor
- DCO: Overall rating of delivery and execution with the vendor
- MWS: Overall rating of delivery and execution with the vendor
- MWS: Please rate your overall experience with this vendor

Easy to Do Business With

- DCO: Provider was flexible in negotiating (especially unlimited liability, security, confidentiality and data privacy, exit terms)
- DCO: Overall rating of evaluation and contract negotiation with the vendor
- DCO: Overall rating of planning, implementation and transition
- MWS: Overall rating of evaluation and contract negotiation with the vendor
- MWS: Overall rating of planning, implementation and transition
- MWS: Flexibility and adaptability in negotiating final contracts

Value for Money

- DCO: Your vendor provided good value for money
- DCO: Delivers the expected business outcomes that were promised
- MWS: How satisfied is your organization with the value the product or service provides for the money spent?
- MWS: Delivers the expected business outcomes that were promised

Transitions and DC Consolidation

- DCO: Centralization and consolidation of data center operations
- DCO: Overall rating of planning, implementation and transition
- DCO: DC consolidation and transformation

- MWS: Overall rating of planning and transition

Cloud Migration and Optimization

- DCO: Cloud migration and workload optimization
- DCO: Cloud migrations and transition
- MWS: Support of cloud applications

Digital Workplace Transformation

- MWS: Has your vendor offered any services to support a digital workplace strategy that takes a user-centric approach to end-user services for your corporate workplace environment?
- MWS: Creative and innovative approach to building the solution and proposal
- MWS: Desktop virtualization services (desktop as a service or virtual desktop infrastructure)
- MWS: Self-service
- MWS: Support through social media collaboration
- MWS: Walk-up support services
- MWS: IT kiosks
- MWS: Virtual assistance (chatbots)
- MWS: Virtual assistance (avatar)
- MWS: Persona-based support
- MWS: Mobility services

Intelligent Automation

- DCO: Have you seen relevant automation initiatives taken by your vendor that have resulted in visible benefits for your organization?
- DCO: What are the different benefits, in terms of percent increase, that you have achieved by implementing these automation initiatives within your organization?
- DCO: Intelligent service automation (AI, machine learning or smart machine-based managed services)
- MWS: Workplace analytics
- MWS: Intelligent automation
- MWS: Contextualization of knowledge

Deal and Service Management

- DCO: Your vendor's management of the services provided
- DCO: Your vendor's account manager and senior leadership are actively engaged and treat us more like a partner than a client
- DCO: Contract structure was flexible and the agreement contains a well-defined statement of work where roles and responsibilities are very clear
- MWS: Overall rating of evaluation and contract negotiation with the vendor
- MWS: Overall rating of delivery and execution

Reliability and Security

- DCO: Promptness of outage resolution
- DCO: Effective and defined procedures for handling any escalation
- MWS: Workplace services security

Flexibility, CI and Innovation

- DCO: Staff and resources to meet widespread geographic coverage, includes appropriate staffing numbers and strong skill set
- DCO: Vendor provided continuous improvement and innovation that resulted in excellent service
- DCO: Your vendor's alliances and partnerships are excellent and deliver great value
- DCO: Your vendor is an industry thought leader and we benefit greatly from their experiences with the many companies in our industry
- DCO: IoT enablement/managed platform
- MWS: Continuous improvement and efficiency achieved
- MWS: Effective resource management that provides high quality skills when needed
- MWS: Does the vendor have the ability to provide a differential level of service to an organization of your size?

QoS and Delivery Model

- DCO: Depth and breadth of services capabilities
- DCO: Robust and standardized methodologies and quality assurance processes (i.e., — ISO 20000, ITIL management practices)
- DCO: Private cloud, utility and industrialized services

- DCO: Quality of services and remote delivery methods from your vendor's low cost geographies/labor
- DCO: Your vendor's operational and tool expertise
- DCO: Please indicate your level of satisfaction with SLA performance (including penalties and rewards) for those SLAs defined by your vendor.
- DCO: Overall rating of service capabilities.
- MWS: Overall rating of delivery and execution
- MWS: Reliability of deliverables, SLAs, budget and timelines
- MWS: Overall rating of services capabilities

Hybrid Infrastructure

- DCO: Private cloud services (infrastructure as a service/platform as a service)
- DCO: Hybrid IT Infrastructure management
- DCO: Public cloud brokerage
- DCO: Intelligent service automation (AI, machine learning or smart machine-based managed services)

GARTNER HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
USA
+1 203 964 0096

Regional Headquarters
AUSTRALIA
BRAZIL
JAPAN
UNITED KINGDOM

For a complete list of worldwide locations,
visit http://www.gartner.com/technology/about.jsp