

# Devise an Effective Cloud Computing Strategy by Answering Five Key Questions

**FOUNDATIONAL****Refreshed:** 23 June 2017 | **Published:** 20 November 2015 | **ID:** G00270415

**Analyst(s):** David Cearley

Cloud computing affects every aspect of IT and the business, so organizations need a high-level bimodal strategy and decision process to manage its impacts. The EA team is in a prime position to lead and coordinate the effort to develop an overarching cloud strategy for the enterprise.



## FOUNDATIONAL DOCUMENT

This research is reviewed periodically for accuracy. Last reviewed on **23 June 2017**.

## Key Findings

- Cloud computing affects many aspects of organizations' IT and business environment, requiring coordination across multiple domains to ensure successful and safe cloud exploitation.
- Organizations that do not have a high-level cloud computing strategy driven by their business strategy will significantly increase their risk of failure and wasted investment.
- Organizations must answer five key questions when formulating their cloud strategy.

## Recommendations

EA teams:

- Use a bimodal approach to create a cloud strategy that delivers flexibility for current business needs, while also supporting rapid application and business innovation for future needs.
- Develop a structured decision framework that identifies potential use cases for cloud computing, analyzing the benefits and challenges for specific application workloads.
- Evaluate if and how the enterprise should build its own private cloud infrastructure as a service (IaaS) or platform as a service (PaaS) capabilities.

- Assume that the enterprise will use cloud services from internal and external sources, and create security, management and governance processes for this hybrid cloud environment.
- Create a multifaceted application strategy to determine when rehosting, refactoring, rebuilding or replacing applications delivers value, and how new applications can be built using cloud-optimized and cloud-native design principles.
- Recognize that cloud computing represents the best-practice model for building scalable, Web-class services for delivery of applications, content or business process functions to partners and customers.

## Table of Contents

---

Analysis.....	2
The Bimodal Business Baseline.....	4
Where and How Will the Enterprise Consume Cloud Services?.....	6
Where and How Should the Enterprise Implement Private Cloud Environments?.....	9
How Will We Secure, Manage and Govern a Hybrid IT Environment?.....	12
How Will the Enterprise's Application Strategy and Architecture Be Impacted by Cloud Computing?.....	13
Consider Opportunities for Your Organization to Become a Cloud Service Provider.....	15

## List of Tables

---

Table 1. Typical Traits of Bimodal IT.....	5
--	---

## List of Figures

---

Figure 1. Categorizing Cloud Service Options Based on Benefits and Challenges.....	8
Figure 2. A Private Cloud Goes Beyond Virtualization.....	10
Figure 3. A Spectrum of Cloud Options in Application Development.....	14
Figure 4. The Enterprise as a Cloud Service Provider.....	16

## Analysis

Cloud computing — a style of computing where elastically scalable capabilities are delivered as a service, using Internet technologies (see Note 1) — is becoming a mainstream component of enterprise IT with impact across the business. Fifty-six percent of CIOs in Gartner's CIO survey indicate they are adopting cloud as either an option or as part of a "cloud first" approach, while 71% look to SaaS either first or as an option. In reality, however, there are many nuances to the

decisions involved, and most enterprises should take a nuanced approach that applies cloud design principles and uses cloud services along with traditional approaches to create a hybrid approach. Organizations that do not have a high-level bimodal strategy to address how the organization will coordinate and manage these disparate impacts will significantly increase their risks and potentially waste their investments. Given this reality, it is critical to focus on a decision framework for how the organization will adopt and coordinate cloud computing decisions and issues across the organization.

Enterprise architecture (EA) teams that have adopted a business-outcome-focused EA approach are uniquely positioned to develop a high-level cloud strategy for the enterprise across multiple groups. Cloud computing will impact every aspect of IT and the business, and EA practitioners typically already work across many of the same IT and business teams that should be involved in key decisions about the enterprise's cloud strategy and approach. Hence, EA is well-positioned to bring others into the process who have the mandate and authority to plan details in specific areas, including technology implementation, sourcing, application portfolio management, finance and legal. The key is to follow a decision framework, which the CIO and EA team can use to work with various parts of the organization to answer key questions on how the enterprise will approach its most important cloud-related decisions.

The decision framework must take into account a bimodal approach. Mode 1 is focused on addressing traditional/existing processes and workloads, and systems of record where the focus is on safety, accuracy and stability. Mode 2 is focused on systems of innovation and differentiation, especially emphasizing new/exploratory workloads where agility, speed and flexibility are important. Multiple parallel initiatives addressing both modes should be pursued using a framework that addresses the following five areas:

- The organization's consumption of cloud services
- Development of private cloud services
- Hybrid cloud and hybrid IT issues
- The impact of cloud computing on applications and business processes
- The enterprise as a cloud service provider

Using a framework that addresses these five areas, the EA team can work across several constituencies to:

- Help implement a business-outcome-driven application and cloud service provider evaluation process
- Work with business to identify key areas where cloud can provide significant benefits
- Help evaluate where cloud models do and don't fit in the current business model
- Codify key risks involved

Here, we offer practical guidance on how best to approach this effort. The analysis in this report is framed by the following best practices, which correspond with the five key cloud strategy areas cited above:

- Where and how should the organization consume cloud computing services?
- Where and how should the organization implement private cloud environments?
- How will we secure, manage and govern across hybrid environments?
- How does cloud computing factor into our application strategy and architecture?
- Are there opportunities for the business to become a cloud computing service provider to others?

## The Bimodal Business Baseline

---

IT organizations have been placed under tremendous pressure by the demands of digital business. Gartner has recommended that CIOs create a bimodal IT organization. In a bimodal IT approach, one part of the organization is responsible for Mode 1 — "reliable IT," which emphasizes safety and efficiency. Another part of the organization is responsible for Mode 2 — "agile IT," which emphasizes speed and flexibility. The needs of these two modes of IT are distinct, although both sides of the IT portfolio need to integrate and interoperate. Over time, Mode 2 may be transformative for all of IT. The employees who support each mode have distinct personality types and skills, and they need processes and tools that are optimized to support that style of IT. The differences in the two approaches are outlined in Table 1.

Table 1. Typical Traits of Bimodal IT

Trait	Mode 1 – Reliable	Mode 2 – Agile
Value	Price for performance	Revenue, brand, customer experience
Objectives	<ul style="list-style-type: none"> <li>■ Cost reduction</li> <li>■ Cost predictability</li> <li>■ Build to a specification</li> <li>■ Reliable, secure, well-managed risks</li> </ul>	<ul style="list-style-type: none"> <li>■ Flexibility and speed</li> <li>■ Manage uncertainty</li> <li>■ Validate, learn, pilot</li> <li>■ Fail fast, fail frequently, fail small</li> </ul>
Governance	Plan-driven, approval-based	Empirical, continuous, process-based
Culture	IT-centric, removed from customer	Business-centric, close to customer
Requirements	<ul style="list-style-type: none"> <li>■ Predictable and known functionality</li> <li>■ Performance requirements are known</li> <li>■ Capacity needs can be predicted</li> </ul>	<ul style="list-style-type: none"> <li>■ Requirements change frequently</li> <li>■ Requirements are uncertain</li> <li>■ Unpredictable capacity needs, scale to demand</li> </ul>
Rate of Change	Stable, low-change, incremental change	Rapid and frequent
Sourcing	<ul style="list-style-type: none"> <li>■ Mature technology</li> <li>■ Mature suppliers</li> <li>■ Long-term deals</li> </ul>	<ul style="list-style-type: none"> <li>■ Technology may be immature</li> <li>■ Suppliers may be small or immature</li> <li>■ Short-term deals</li> </ul>
Personality	Linear, step-by-step, slow but steady	Inquisitive, thrives on change
Cycle Times	Long (months)	Short (days, weeks)

Source: Gartner (November 2015)

A viable cloud strategy must address both modes, but the emphasis on Mode 1 and Mode 2 is determined by the business strategy. Therefore, the cloud strategy must start with an understanding of the overall business strategy and the degree to which the business is focused on driving innovation and aggressively pursuing digital business. Each of the five elements of the overall cloud strategy must address this business-driven balance of Mode 1 and Mode 2 needs.

For more information, see:

- "Bimodal IT: How to Be Digitally Agile Without Making a Mess"
- "Bimodal IT and Adaptive Sourcing Are Critical to Digital Business Success"

## Where and How Will the Enterprise Consume Cloud Services?

---

The first question deals with the enterprise in the role of a consumer of services. At this level, evaluations consider when and how the enterprise will consume cloud services, whether from an external cloud service provider, or from internal groups acting in the role of a cloud provider (that is, offering "private cloud" services). The key goal here is to provide a consistent framework to help determine where the organization will or won't consume cloud services, using consistent considerations of factors such as security, risks, costs and benefits.

Our recommended approach is to systematically examine particular applications and related use-case scenarios in the organization for which cloud services might be used. It is important to note that this question assumes that one has a clear understanding of the desired business outcomes and key challenges and risk factors associated with a use-case scenario. Four critical elements need to be understood for each cloud scenario:

- **The nature of the application.** The baseline for this examination is a solid understanding of the business and technical requirements associated with the application and the business processes it supports. On the business side, a clear understanding of the business outcome and associated business capabilities supported by the application is needed. Further segmentation of the application as a system of record, differentiation or innovation is also needed to guide the decision process (see "Application Deployment Options Through the Pace Layer Lens"). Other considerations include the anticipated need for agility in terms of enhancements or the user population, the degree of customization desired and the expected life of the application need. The technical nature of the application must be examined as well, including the level of resource volatility anticipated, the current architecture of the application, and the need to support geographically distributed, mobile or disconnected users.
- **The data associated with the application.** The sensitivity of the data and the associated legal, compliance and security issues must be identified to understand especially where cloud computing creates potential challenges. However, this is only the starting point. One must consider the size of the dataset, and the size and volume of data updates.
- **The points of integration between the application and other systems.** Most enterprise systems are linked in some way to other systems. You must understand which systems must be linked, the nature and frequency of the interaction (for example, data movement, notifications and action invocation) and the acceptable latency of the interactions in order to assess the use of a cloud service.
- **Bimodal considerations.** How does the business approach impact the benefit/risk profile? If the core business needs for the application are stability, reliability and efficiency, then factor Mode 1 needs into the evaluation. If the business is more concerned with flexibility, agility and innovation, then Mode 2 factors are used to influence the benefit/risk weighting.

Building on the baseline understanding of the application requirements, the following three factors are examined for each cloud scenario:

- **Cloud readiness:** This is an examination of the basic suitability of the workload being handled by a cloud service (in terms of specific attributes not directly tied to the "benefit" or "risk"

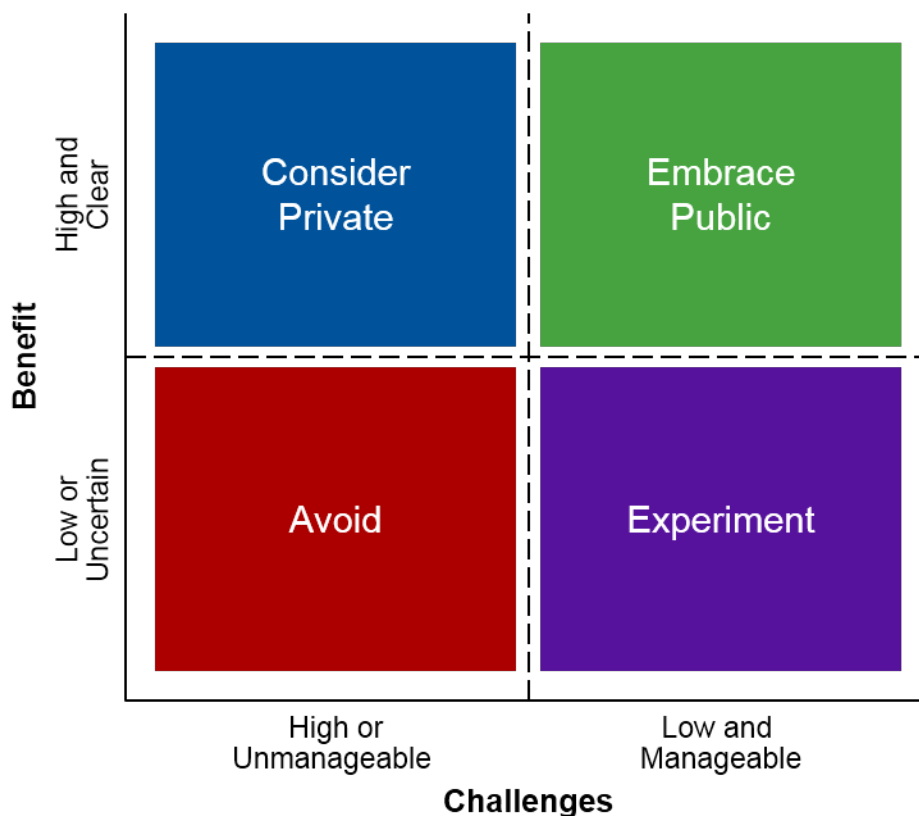
categories below). In the case of an existing application that will be hosted on a cloud infrastructure and/or cloud platform service, a key consideration is whether the architecture of the application makes it feasible to be migrated or enhanced within a cloud model. In the case of a new application, the application can be architected as a cloud-native solution, but other factors, such as integration and connectivity needs (for example, the need for low latency of offline execution, or to connect or interact with other systems in the organization), must be considered. If any of these factors rule out the cloud service option for a specific workload, the evaluation of that option ends here. Otherwise, analysis moves on to the benefit and risk challenges below.

- **Potential benefits:** For each application or use-case scenario, consider, "How high-priority are the benefits or rewards that cloud provision could offer?" Such benefits may include improved agility, cost savings, simplification, access to innovation, solutions to capacity problems, better handling of workload imbalances or volatility, lowered risk through reduced upfront commitment, or more rapid time to solution.
- **Potential risks and challenges:** What are the potential downsides or dangers to using cloud services? For each use case under consideration, factors to consider here include security issues, lack of transparency, market immaturity, potential lock-in or integration difficulties, or financial-reporting or regulatory challenges. Key attributes here include security- and regulatory-related factors related to the dataset handled by the workload or application.

Based on these case-by-case evaluations of the benefit and risks that a cloud model poses, the various options under consideration can be plotted in a matrix (see Figure 1), which sorts options into four categories defined by where each option falls on the benefit and risk axes, as follows:

- The vertical axis ranks the level of cloud benefits, ranging from low or uncertain at the bottom to high and clear at the top.
- The horizontal axis plots the risks and challenges, ranging from high or unmanageable on the left to low and manageable on the right.

Figure 1. Categorizing Cloud Service Options Based on Benefits and Challenges



Source: Gartner (November 2015)

The upper-right quadrant in Figure 1 is the public cloud "sweet spot," where externally provided cloud services make most sense. Conversely, any options that land in the lower left are currently unsuitable for provisioning via the cloud computing model. Applications that land in the upper left, where cloud service benefits are high and clear but the risks or challenges are also high, may be good candidates for a private cloud service approach. For example, if an application would benefit from cloud computing agility but has highly sensitive data subject to regulatory compliance issues that cannot be guaranteed by public cloud offerings, a private cloud option may eliminate that challenge, since the enterprise has control of the underlying enabling technologies in a private cloud. Such an option would land in the "consider private" category in Figure 1.

This risk/benefit analysis is just a first step. Further analysis should follow from here, which may shift some of the parameters and "move the dots" on the matrix. For example:

- *Risk mitigation options:* Further analysis may reveal that previously insurmountable-seeming risks can be ameliorated. For example, some security downsides may be mitigated through a use of encryption or tokenization that protects the data residing in the cloud service.
- *Cloud maturity:* As enterprises become familiar with cloud computing and implement best practices to secure, manage, and govern access and use of public and hybrid cloud services,



perceived risk tends to go down, and paths to concrete value go up. In our interaction with Gartner clients, we often see solutions that originally were in the lower-left quadrant move up and/or right to be considered for private, public or hybrid approaches.

- *Service provider market options:* The initial review is looking at the cloud computing model overall. When the evaluation of specific cloud service providers gets underway, the information uncovered may change the picture for certain applications or workloads. For example, if the need to keep data associated with an application within the U.S. was a risk factor that weighed against the use of cloud email service, then the discovery that a certain provider allows the service consumer to specify that data is only stored on U.S. servers could shift that dot from the "consider private" category to the "embrace public" one.

Several other factors should be examined as well. The key, however, for all required analyses is to apply a consistent framework for evaluating these aspects — rather than letting individual teams and planning groups decide cloud service questions on an ad hoc basis, using their own criteria, whenever a new project comes up. The key is to ensure that a common decision framework consistently drives the enterprise's strategy on where it should and shouldn't consume cloud services. For more information, see:

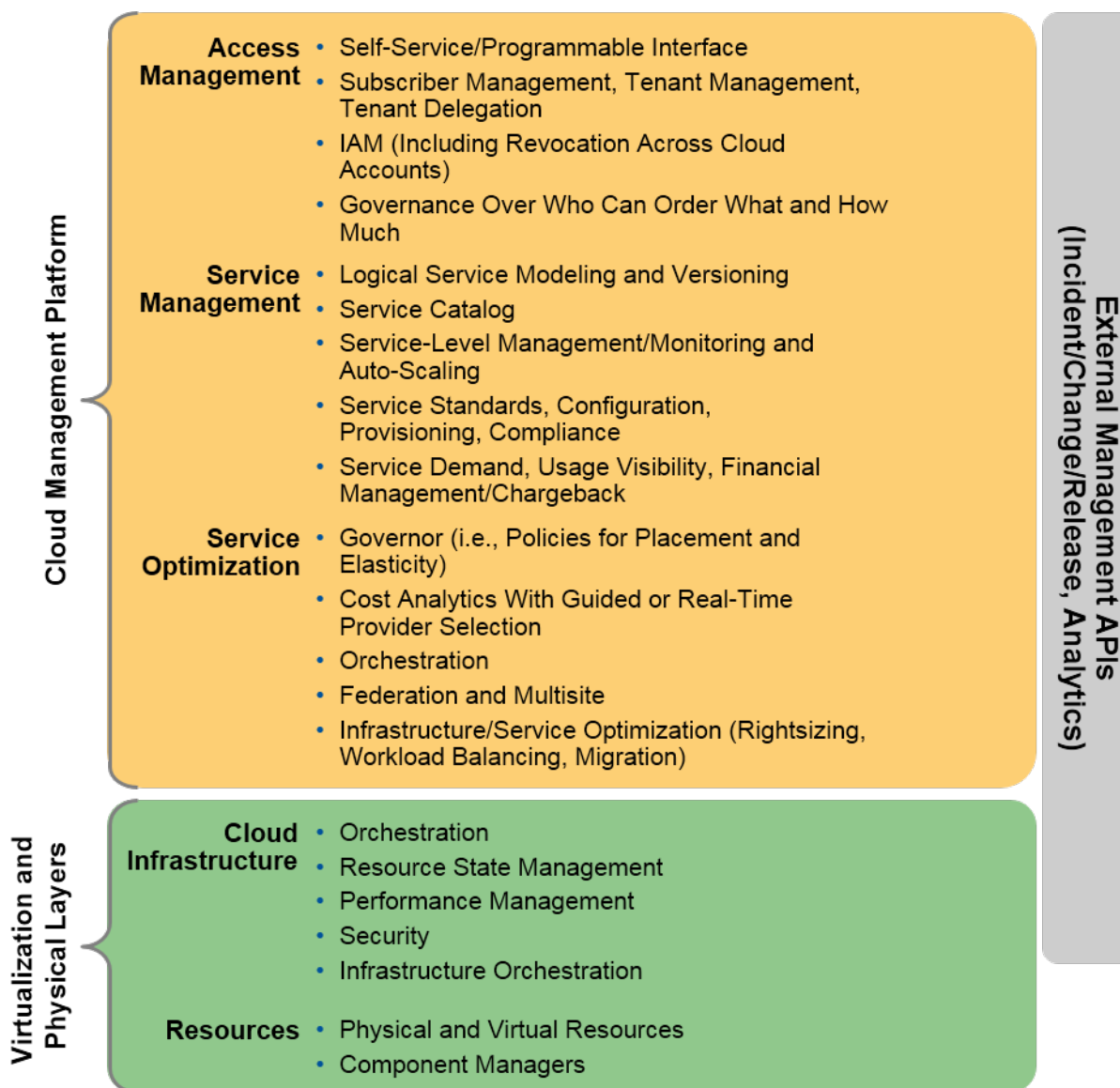
- "Look Before You Leap Into Cloud Computing"
- "How to Ease the Planning, Sourcing and Implementation of SaaS Projects"
- "Cloud Services Will Establish the Foundation for Next-Generation Solutions"
- "Best Practices for Planning a Cloud Infrastructure-as-a-Service Strategy — Bimodal IT, Not Hybrid Infrastructure"

## Where and How Should the Enterprise Implement Private Cloud Environments?

---

The second question shifts attention away from consuming cloud services to the enterprise building its own private cloud services. While the previous consideration focused on the consumer side of the cloud interface — with the implementation details hidden behind an abstraction layer — this next level of the framework deals with concerns on the provider side of the interface. It is primarily concerned with the implementation details needed to stand up the service and present the abstraction layer to the consumer (see Figure 2).

Figure 2. A Private Cloud Goes Beyond Virtualization



Source: Gartner (November 2015)

For most organizations, private cloud services will reside primarily at the IaaS level, with some PaaS elements. Most organizations will not need, or desire, to create their own multitenant, shared cloud application services. Assuming the enterprise builds a private cloud IaaS/PaaS foundation, it then becomes a consideration as one option in the cloud service consumption decision framework shown above.

The main motivation for an organization to consider embracing private cloud service development should be a simple one: to gain some key benefits of cloud service provision — such as improved adaptability, flexibility and elasticity — within their own controlled infrastructure environment. The key driving force behind considering private cloud is that having the enterprise in control of the

underlying implementation details provides a higher degree of control and transparency than is available from public models. The downside to building private cloud is the cost of implementing and then maintaining the full set of public cloud service characteristics. Unfortunately, a too common motivation for private cloud is a belief in the myth that external cloud services are always less secure and cannot be used for any mission-critical applications (see "The Top 10 Cloud Myths").

Working with members of the infrastructure and operations team, EA practitioners should facilitate a structured analysis of when and how the organization will go the route of the private cloud IaaS and, potentially, PaaS. Private cloud services could be delivered from internal data centers or via outsourced/hosted models. Note that achieving these benefits may entail building a complete "pure" cloud environment internally. Another approach is to merely consider what lessons from the leading cloud computing service providers can be applied within the organization's own infrastructure to make it much more adaptive, flexible or elastic — that is, to be inspired by and apply select best practices such as a high degree of automated management or self-service provisioning interfaces without going the full-blown private cloud route. Some organizations may build fully aligned private cloud service that delivers all of the characteristics of the cloud style of computing, while others may choose to build cloud-inspired capabilities that deliver some of the characteristics and value of cloud computing, but fall short of delivering a full cloud service (for example, employ a high degree of automation but do not deliver a full self-service API interface layer). The degree to which the infrastructure embraces the cloud style is driven by a balance between the cost and complexities of building and maintaining a full cloud service model versus the benefits of having full control of the infrastructure service. It is critical to understand the full implications of building a private cloud service to avoid failures (see "Six Reasons Private Clouds Fail, and How to Succeed").

A common pitfall in cloud strategy discussions is to blur the distinctions between the consumer using cloud services and the provider building cloud services. Cloud computing mandates a strict separation of concerns between the consumer and the provider, with the two interfacing at the service interface layer, which hides implementation details from the consumer. Often, vendors that do business in both areas will contribute to this confusion by discussing cloud offerings of both types as part of a single discussion. This blurring often leads to a private IaaS cloud that does not have a complete abstraction layer that separates the concerns of the consumer from the implementation details of the provider. Applications on the consumption side of the equation then become inappropriately tied to implementation details of the data center running these applications. This is why it's important to keep the private cloud service development portion of the strategy separate.

Other key private cloud considerations include:

- *Cloud management platform (CMP) deployment:* If a private cloud environment is adopted, a CMP will need to be deployed (see Figure 2). The CMP can be levered to provide capabilities to manage access to external cloud services as well.
- *The need to track and develop skills in emerging and rapidly evolving cloud technology areas:* Examples include software-defined networking (see "Enterprises Planning Private Clouds

Should Include Software-Defined Networking With Major Network Changes") and Web-scale IT (see "Web-Scale IT Influences the Market and Enterprises for Cloud Computing").

- *Internal cloud service brokerage:* Even when a private cloud service is created, most enterprises will need to coordinate use of these services with external public cloud services. The IT group needs to develop capabilities as a service broker across different service providers.
- *Bimodal approach:* The need to support Mode 1 versus Mode 2 requirements will impact how the organization will approach private cloud. Mode 1 will often lead to a cloud-inspired approach in which cloud best practices are selectively adopted to incrementally improve existing data center, infrastructure and application models with a primary emphasis on cost savings. Mode 2 will lead to a more complete embrace of the cloud model and development of full private cloud services — typically a more expensive and risky approach, but one that delivers significantly more cloud-related benefits (for example, agility).

For more information on key concepts related the private cloud portion of the cloud strategy, see:

- "When Building a Private Cloud, Start Small, Think Big"
- "Six Reasons Private Clouds Fail, and How to Succeed"
- "Emerging Technology Analysis: Cloud Management Platform Tools"

## How Will We Secure, Manage and Govern a Hybrid IT Environment?

As the organization begins to use multiple public and private cloud services alongside traditional infrastructure and applications, the result is a hybrid environment that raises unique security, management and governance issues. In an effort led by representatives of the organization's IT operations and IT security teams, EA practitioners should help provide a framework to answer the question: How will the organization secure and manage its hybrid IT/cloud environment? Given the reality of externally provided cloud services, internal cloud environments and cloud-enabled applications coexisting with traditional data center and application environments, a model will be needed to address security, management and governance across these boundaries. Issues to be addressed in this portion of the enterprise cloud strategy include:

- *Security:* Analysis here should focus on building out a model that enables the organization to secure information across a hybrid cloud landscape, including issues such as on-the-fly encryption and Active Directory (AD) federation.
- *IT management:* A hybrid IT environment may prompt a broader strategy to position IT as the broker for a mix of IT services delivered in different ways — as traditional and cloud services.
- *Governance challenges:* In a hybrid IT model, every group has the potential to act as its own broker of services. Without a plan to address this, the result can be organizational chaos caused by a loss of governance over technology procurement and consumption.
- *Supporting technologies:* What technologies (such as virtual LANs, LAN acceleration or storage replication) could be put in place to smooth out the movement of work and data across traditional and cloud boundaries?

- *Bimodal considerations:* Security, management and governance models must address both Mode 1 and Mode 2 needs.

It is important to note that the specific tools used to secure, manage and govern access and use of cloud services in a hybrid environment themselves may be delivered as external public or private cloud services or as traditional software, which can be implemented in-house, outsourced or run on an external cloud IaaS foundation. Evaluation of the right delivery model to use will leverage the decision framework outlined in the first part of the cloud strategy. Many issues addressed in this aspect of the cloud strategy will impact the other four aspects of the cloud strategy. For example, the security aspect of the hybrid cloud strategy may specify standard mechanisms to perform active directory federation between internal systems and external cloud providers. In this case, evaluations of cloud service providers addressed in the first, "service consumption" portion of the cloud strategy would be supplemented with criteria related to these security considerations. Specifically, does a particular cloud provider's offering have the capability to take the organization's group policies that have been defined in AD, and extend and integrate them within the external cloud service?

For more information on hybrid cloud strategies, see:

- "Become a Cloud Enabler by Following Our Eight Steps to Hybrid IT"
- "Hybrid Cloud Is Driving the Shift From Control to Coordination"

## How Will the Enterprise's Application Strategy and Architecture Be Impacted by Cloud Computing?

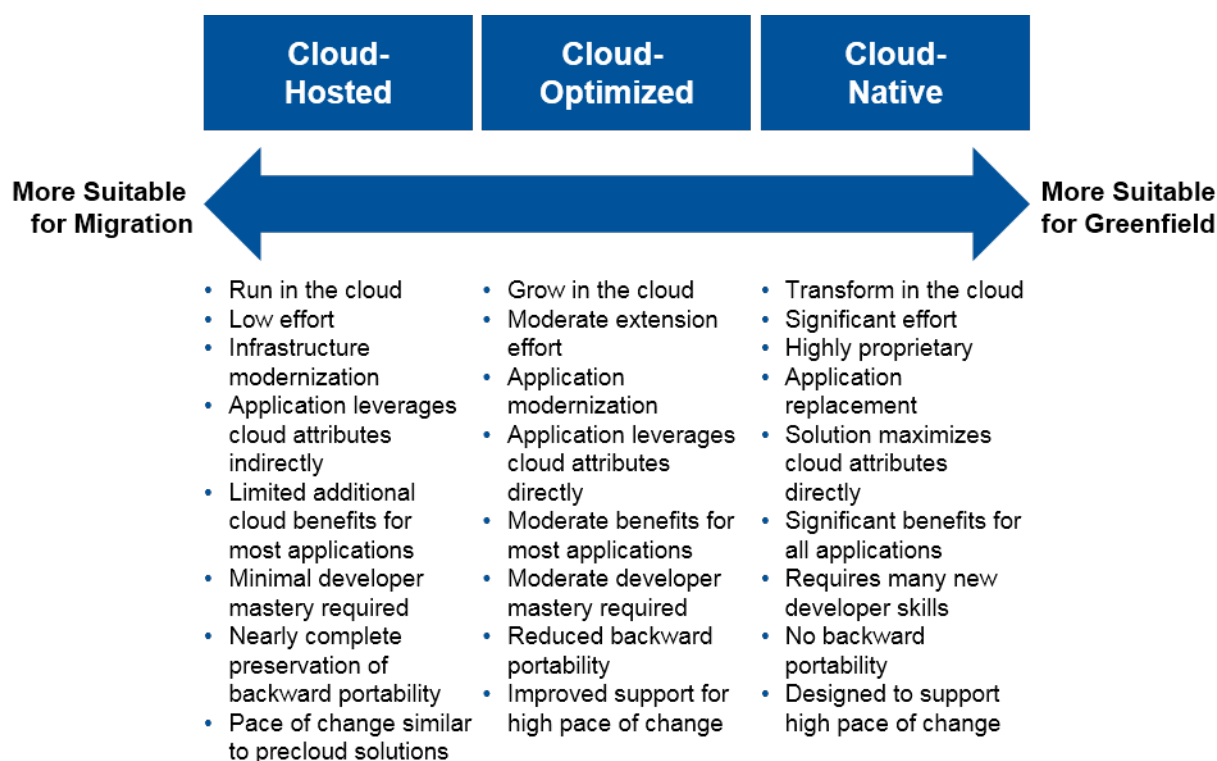
The next question focuses on applications: What is the overall strategy for acquiring, developing or adapting applications for deployment onto a cloud IaaS and/or PaaS foundation and for optimizing the application environment to achieve cloud benefits? This not a simple question to answer, given that the cloud can impact an enterprise's application picture along several dimensions. The starting point is the evaluation of SaaS as part of the cloud service decision model to replace software. However, enterprises must also consider scenarios where it will purchase or build software for deployment onto private, or public IaaS and/or PaaS services. The most simple approach is to simply rehost current enterprise software, but the enterprise will often find they get minimal value from this "lift and shift" approach — assuming the applications are architected such that it is even possible. Application development strategies need to evolve to understand where and how cloud-optimized and cloud-native applications can be created. When acquiring software applications, employ additional evaluation criteria to evaluate each application's ability to be deployed to the cloud and take advantage of cloud potential (for example, horizontal and dynamic scaling). Without a plan, these impacts will occur in a chaotic fashion, so a strategic, framework-based approach is key.

This portion of the strategy should be led by the organization's application team, with input and facilitation from the EA group. EA practitioners will work to help set appropriate standards, and can devise frameworks to lead considerations of the various options for different functions. One key consideration involves newly developed or acquired software applications. Will these new

applications have no cloud-related elements at all, or will they be cloud-hosted, cloud-optimized or cloud-native (see Figure 3)? For example:

- *Cloud-hosted solutions* transplant enterprise applications on IaaS to gain the benefits of simple shared-hardware multitenancy. This is a primary approach for Mode 1 needs where an application is cloud-ready and has highly volatile resource requirements, and where security issues can be addressed. Hosting these workloads on IaaS should provide cost savings, but users are cautioned to examine the details of the IaaS pricing model versus the resource needs over time of the workload.
- *Cloud-optimized solutions* are refactored or redesigned to take advantage of the global-class characteristics of cloud platforms, such as horizontal scalability, fault tolerance, high performance, efficiency and interoperability.
- *Cloud-native solutions* are designed to take full advantage of the defining characteristics of cloud computing platforms, and are built using the core principles, patterns and best practices that deliver and support these characteristics. This is a primary approach for Mode 2 needs, where speed, agility, flexibility and optimized performance across a globally distributed network are primary considerations.

Figure 3. A Spectrum of Cloud Options in Application Development



Source: Gartner (November 2015)

In addition to the options above, other key considerations include replacing software with an externally provisioned cloud service (which loops back to the first consideration in this framework),

or modifying existing applications to adapt them to a cloud environment. These options may reveal optimal ways to achieve cloud benefits with varying degrees of investment or effort. The five basic options to consider for each application in the existing portfolio include:

- *Rehost*: Redeploy an application to a cloud-based platform without modifying the application's code.
- *Refactor*: Make application code or configuration changes to connect the application to a PaaS provider's infrastructure.
- *Revise*: Modify or extend the application's code base to support legacy modernization requirements, and then use the rehost or refactor options to deploy it to the cloud.
- *Rebuild*: Redevelop the application from scratch on a provider's PaaS platform.
- *Replace*: Eliminate the former application altogether, and replace it with an external SaaS offering.

Each of these options entails unique considerations that should be evaluated as part of the cloud strategy. For example, will any of these options pose issues related to licensing rights, security, technical feasibility or data management? The key is to ensure that all of these cloud-application-related options and their implications are examined under consistent framework, rather than in a chaotic, ad hoc basis from application to application.

For more information on application-related aspects of the enterprise's cloud strategy, see:

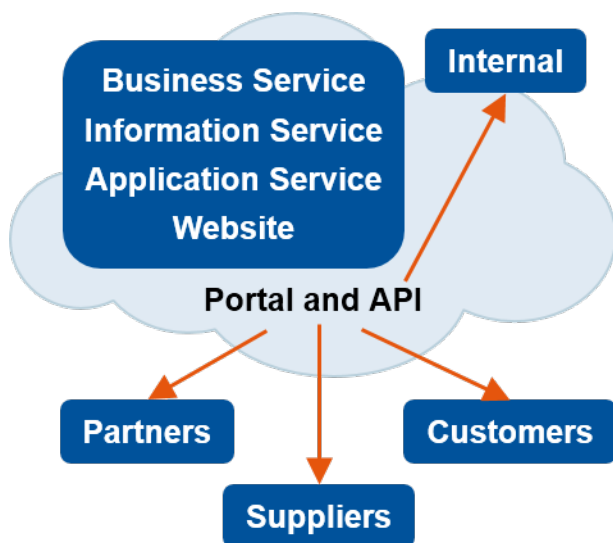
- "What You Need to Know About Cloud Application Development"
- "Moving Applications to the Cloud: A Survival Strategy for Data Management Professionals"
- "Define Your Customization Strategy for SaaS/Cloud Business Applications"

## Consider Opportunities for Your Organization to Become a Cloud Service Provider

---

The final important aspect of a comprehensive cloud strategy concerns the potential for the organization to gain important benefits by becoming a cloud service provider in its own right (see Figure 4). This is first and foremost a business issue, focusing on when and where the enterprise will deliver application functionality, information or business process capabilities to its customers or business partners. The best practice for delivering these digital business and e-commerce capabilities is to employ the cloud style, delivering elastic capabilities as a service via self-service interfaces based upon a shared and standard industrialized foundation using Internet technologies. That is the cloud style of computing. Some enterprises will find that groups outside of IT are already employing these principles and delivering what is essentially a cloud service today. Learning from these efforts and creating synergy with IT moves to cloud computing will accelerate efforts and maximize business value.

Figure 4. The Enterprise as a Cloud Service Provider



Source: Gartner (November 2015)

Systematically examining these opportunities from a strategic perspective is an important activity for CIOs and for EA practitioners who support them in facilitating enterprise future-state planning for the cloud. It is important to avoid limiting the cloud strategy to an inward-facing one, which would fail to recognize the likelihood that your organization will act as a cloud service provider to other entities at some point. For most businesses, opportunities to play a cloud provider role would not occur at the platform (PaaS) or infrastructure (IaaS) level, but are more likely to arise at a software or process level.

Any externally facing application, information or business process activity is a candidate for provisioning under a cloud model. The potential benefits of doing so would be to improve these activities by gaining the benefits that as-a-service provisioning can offer — for example, by making them more elastic, easily shared, metered and "self-service" in nature, and by exploiting the benefits of development using standard Internet technologies in a Web-oriented architecture (WOA) model. In general, the more an enterprise can find ways to "think like a cloud provider," the more opportunities to exploit such benefits may arise. In considering such opportunities, focus on target consumers for which cloud services would offer high value — not only customers or business partners, but also internal or external application developers. A key component of providing cloud services internally will be the Web API. Gartner expects the number of organizations offering cloud services through Web APIs to increase to 25% by 2015 — up from less than 10% in 2010.

Most large enterprises that Gartner encounters are already becoming cloud providers in one form or another. Any company using the Web to deliver applications, information services and business process services — including B2B or B2C e-commerce activities, as well as newer digital business offerings — is a cloud service provider, as long as these offerings are delivered as elastic services, in a shared environment, with the technical details hidden behind an abstraction layer with a self-service interface. In fact, these very cloud-related attributes (for example, elasticity, measurability and self-service) define the best-practice model for delivering technical or business capabilities to



any outside customer or partner. This is why the process of becoming a successful digital business will increasingly involve thinking like a cloud provider.

## 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>

---

© 2015 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates. This publication may not be reproduced or distributed in any form without Gartner's prior written permission. It consists of the opinions of Gartner's research organization, which should not be construed as statements of fact. While the information contained in this publication has been obtained from sources believed to be reliable, Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information. Although Gartner research may address legal and financial issues, Gartner does not provide legal or investment advice and its research should not be construed or used as such. Your access and use of this publication are governed by [Gartner Usage Policy](#). Gartner prides itself on its reputation for independence and objectivity. Its research is produced independently by its research organization without input or influence from any third party. For further information, see "[Guiding Principles on Independence and Objectivity](#)."