2017 Planning Guide for Cloud Computing

Published: 13 October 2016

Analyst(s): Mindy Cancila, Douglas Toombs, Alan D Waite, Elias Khnaser

In 2017, IT organizations must develop or advance their cloud strategies by adopting and maturing the use of cloud services across the enterprise. This Planning Guide outlines the key planning trends and design considerations for technical professionals focused on cloud.

Key Findings

- In 2017, as public cloud services mature, organizations will continue to aggressively build and invest in "cloud-first" strategies and architectures. All industries and verticals are adopting cloud services across all layers of cloud deployment models — software as a service (SaaS), infrastructure as a service (IaaS) and platform as a service (PaaS).

- Organizations will live in a hybrid IT world in 2017 and beyond. They will rapidly adopt cloud services, but will also maintain traditional, on-premises hosting environments. The key to success will be to manage all of the integrations, interdependencies and management tasks while brokering cloud services to the business.

- Public cloud services are essential for emerging digital business use cases, next-generation applications and initiatives like the Internet of Things (IoT). However, the public cloud is also a viable hosting alternative for traditional enterprise applications.

- Most IT organizations will continue to lose interest in building and maintaining their own on-premises private clouds, and will instead focus on improving their virtualization estate.

Recommendations

- Start building a cloud-first strategy now, if you haven’t done so already. The transition is difficult and takes time. Organizations must make public cloud services the primary, prioritized and promoted deployment model for all new business processes, workloads or applications.

- Continuously evolve your cloud application suitability model. Applications that were not a fit for the public cloud two years ago may be ideal candidates today due to the rapid innovation and improvement of public cloud services.
Plan for a multiprovider strategy, and begin transforming the organization into a broker of cloud services. Delivering IT as a service (ITaaS) will require training, integration and investments in hybrid architectures for networking, identity, data and other key services.

Choose the level of private cloud that is right for you. Focus on the most frequently provisioned workloads, where agility is required. Select virtualization automation (VA) and public cloud services rather than building a fully featured private cloud.

Table of Contents

Cloud Computing Trends ................................................................................................................................................3
Organizations Will Prioritize Building, Implementing and Maturing Their Cloud Strategies ......................5  
Planning Considerations.................................................................................................................................................6
Multiprovider Strategies Will Become the De Facto Standard for IaaS and PaaS ......................................12  
Planning Considerations.................................................................................................................................................12
Corporate IT Will Live in a Hybrid World for the Foreseeable Future .........................................................17  
Planning Considerations.................................................................................................................................................17
Most Organizations Will Forgo Trying to Build Full On-Premises Private Clouds ..................................20  
Planning Considerations.................................................................................................................................................21
Setting Priorities.........................................................................................................................................................26
Gartner Recommended Reading.................................................................................................................................27

List of Figures

Figure 1. Organizational Approaches to Adopting Public Cloud Services ......................................................4
Figure 2. Digital Disruption Through Technical and Business Innovation ....................................................5
Figure 3. Architectural Comparison of Ownership by Cloud Layer ................................................................8
Figure 4. Gartner’s Cloud Adoption Framework .............................................................................................9
Figure 5. Cloud Functional Roles and Disciplines .........................................................................................10
Figure 6. Application Migration Approaches .................................................................................................11
Figure 7. Gartner 2016 Scoring of Cloud IaaS Platforms ...........................................................................13
Figure 8. Hybrid IT — IT Brokers Cloud Services to the Business .............................................................16
Figure 9. Hybrid Architectures Defined .............................................................................................................18
Figure 10. Private Cloud Implementations .......................................................................................................25
Cloud Computing Trends

Digital business has unlocked a world where everything and everyone are connected, all the time. Organizations need a scalable architecture to support on-demand capacity and ever-increasing amounts of data. In 2017, organizations will increasingly look to the public cloud to address these scalability requirements. The cloud allows organizations to augment data center capacity and to take advantage of value-added services. Organizations that decide not to leverage the public cloud, or that take a "wait and see" approach, will run the risk of being disrupted by others in their industry.

In 2017, Gartner expects the public cloud to reach a level of maturity where organizations embrace cloud computing and build strategies to leverage cloud services.

By 2020, 24% of the total addressable IT market will be cloud.¹

Furthermore, nearly one in five virtual machines (VMs) worldwide are in the public cloud,² and we are really just starting to see the growth and adoption of public cloud for traditional enterprises. Cloud computing is not the sole technical innovation to focus upon. However, cloud services are the most pervasive and broadly impactful technical innovation underpinning so many other technical advancements, such as big data, analytics, the IoT and software development. Therefore, a business strategy without a cloud strategy in today’s environment is risky and analogous to deliberately ignoring the importance of a foundation to a building.

Many organizations have been using cloud services for some time for SaaS initiatives. Today, organizations are commonly engaging central IT to implement a better structure to accelerate the adoption of cloud services. This means many organizations are moving beyond initial deployments and making investments that will enable cloud computing to be deployed in a repeatable and governed fashion (see Figure 1).
Organizations that leverage technology to deliver business differentiation will succeed and may displace their competitors. Organizations that avoid technical innovation will run the risk of being disrupted in their core business, potentially resulting in catastrophic outcomes. Figure 2 plots companies along this digital disruption curve.
This Planning Guide assesses the major technology planning trends in 2017 for the cloud computing market. It discusses the planning considerations that organizations should account for in 2017 to unlock the competitive differentiation that cloud-based architectures deliver. The following trends are examined in this report:

- Organizations will prioritize building, implementing and maturing their cloud strategies.
- Multiprovider strategies will become the de facto standard for IaaS and PaaS.
- Corporate IT will live in a hybrid world for the foreseeable future.
- Most organizations will forgo trying to build full on-premises private clouds.

Organizations Will Prioritize Building, Implementing and Maturing Their Cloud Strategies

IT organizations have moved past asking whether applications can be deployed or migrated to the public cloud, and instead are asking why applications can’t live in the public cloud. This paradigm shift is key. A similar shift happened inside the data center at the end of the last decade when
organizations switched over to virtual-first strategies. Gartner recommends that organizations invest in cloud-first strategies — where the cloud is primary, promoted and preferred.

Cloud adoption continues to increase across all verticals and industries. As organizations increase their knowledge of the providers’ services, many are turning to the public cloud to host more complex and mission-critical applications.

By 2018, 50% of the applications hosted in the public cloud will be considered mission-critical by the organizations that use them.³

Many organizations that are embracing the cloud are implementing cloud adoption frameworks to enable efficient use of cloud services and consistent architectural designs. A framework provides a governing process for identifying applications, selecting cloud providers and managing the ongoing operational tasks associated with public cloud services.

Organizations are building centers of excellence that allow them to leverage more value-added cloud services. Over time, these organizations will gain a competitive advantage in their industries through the use of these highly scalable, on-demand resources.

Implementing a cloud strategy requires functional expertise across both technology and business teams. Many organizations have moved beyond asking someone to develop a cloud strategy as a "hobby," and instead are now investing in a dedicated cloud architect. Cloud architects work across a number of distributed teams and disciplines, and over time, many intend to broker cloud services to the business.

As organizations develop and execute their cloud strategies, they must define and implement governance procedures within each cloud platform, as well as across cloud platforms. Failure to define, implement and audit governance policies can lead to catastrophic failures, such as data losses, security breaches or overspending on cloud services. The cloud architect and center of excellence must collaborate to define governance policies and to ensure that those policies are consistently implemented across projects and throughout the organization.

Planning Considerations
Because building, implementing and maturing cloud strategies will continue to be a high priority in 2017, IT organizations must take the steps needed to:

- Implement a cloud-first strategy
- Hire and invest in a cloud architect and a cloud core team
- Move beyond the low-hanging fruit
Implement a Cloud-First Strategy

Historically, Gartner has seen many organizations evaluate public cloud services only when "everything aligned perfectly" to support a given workload demand. If any provider shortcomings arose, these organizations would disqualify the use of any cloud services. To maximize long-term success in the use of cloud services, organizations need to invert this way of thinking. They must adopt a cloud-first strategy, whereby public cloud services are the first choice for all new workload demands that come into the IT organization.

A cloud-first strategy should extend far beyond the purview of the IT organization. It must be understood and embraced by the overall organization, including business units and C-level management. Thus, IT organizations must focus on more than just the technical steps required to implement a cloud-first strategy. They must evangelize both the merits of moving to a cloud-first strategy and the future benefits that can be achieved as a result.

Reality must play a role in this approach, however. "Cloud first" should not be interpreted as "cloud always." There may be legitimate reasons why specific workloads should not be placed outside of an organization's "four walls" or direct control. However, Gartner advises that the requirements to meet such a bar — and, consequently, to burden on-premises infrastructure with workload demands — should be set relatively high, even to the point of refactoring internal IT or business processes if necessary.

Organizations evaluating public cloud services as the preferred deployment approach need to consider a number of factors. To determine the appropriate tier of cloud services to use, they should consider the value proposition of each:

- **SaaS** — Organizations evaluating moving an existing application to the cloud, or looking for a new application, should likely start here first, to determine whether a suitable offering exists in the market. However, adoption of cloud services at this tier is more similar to off-the-shelf software, in that little to no customization may be possible. In addition, unlike on-premises, off-the-shelf software providers, SaaS providers will typically update their software whenever they desire — which could potentially impact users' workflows. For many of these reasons, Gartner typically sees SaaS solutions being adopted primarily in non-mission-critical areas.

- **PaaS** — Still a somewhat emerging marketplace (and the smallest tier of the public cloud), PaaS is a viable choice for in-house-developed applications or for open-source solutions where the organization has access to the source code. However, many public PaaS solutions have shortcomings that may make broad enterprise use challenging, such as out-of-date runtimes or the inability to add third-party or custom libraries to the platform.

- **IaaS** — The most flexible of the three options, IaaS is suitable for most on-premises workloads that can be virtualized today. However, most IaaS providers are not in the business of managing systems anywhere above the hypervisor layer. This is especially true for the hyperscale-tier providers, such as Amazon Web Services (AWS) and Microsoft Azure, that are dominating market share. Therefore, IT organizations are still left with many of the tasks they already perform, such as patching operating systems and applications, and monitoring processes and file systems.
Each tier brings varying levels of management tasks that IT will need to perform, and each comes with trade-offs in the areas of control and choice (see Figure 3).

**Figure 3. Architectural Comparison of Ownership by Cloud Layer**

Source: Gartner (October 2016)

In "Solution Path for Developing a Public Cloud Strategy," Gartner provides a high-level cloud-first adoption framework (see Figure 4).
Hire and Invest in a Cloud Architect and a Cloud Core Team

Cloud computing is not a simple IT initiative, and it must have a dedicated architectural leader. Consider the impacts that cloud computing has on an organization, in areas such as application development, IT operations, legal, finance, procurement, security, compliance, privacy, identity management, data integration, mobility, customer experience and business development. These impacts are not trivial, and they do not take care of themselves.

In 2017, IT organizations should appoint a cloud architect, if they haven’t already done so. This individual should direct a cloud core team that will address organizational transformation in a variety of areas. The cloud architect’s primary responsibility is to instill a cultural reorientation toward the cloud across many aspects of the organization. Cloud architects should not be responsible for conducting all of the cloud transformation, but they should orchestrate the changes needed across many disparate areas. (See "An Emerging IT Role: The Cloud Architect.")
There are dependencies across teams, and various architects must collaborate as they work through cloud architectural design. Figure 5 identifies the functions of the key stakeholders who should be included in the cloud team.

**Figure 5. Cloud Functional Roles and Disciplines**

<table>
<thead>
<tr>
<th>Operations</th>
<th>Governance</th>
<th>I&amp;O Management</th>
<th>Data Protection and Recovery</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business</td>
<td>Legal</td>
<td>Procurement</td>
<td>Finance</td>
</tr>
<tr>
<td>Architects</td>
<td>Network</td>
<td>Identity</td>
<td>Security</td>
</tr>
<tr>
<td>Cloud Architect</td>
<td>Storage</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

I&O = infrastructure and operations

Source: Gartner (October 2016)

Having a cloud architect is crucial to the success of any cloud-first strategy. However, it is equally important to ensure that the technical team responsible for implementing, managing and supporting this new environment is well-versed in public cloud IaaS and PaaS technologies. Thus, in 2017, IT organizations must also focus on developing the skill sets of system administrators and engineers.

To achieve the required skill set upgrades, IT organizations must invest in training and certification. They should also encourage employees to use the free trial offers from cloud providers such as AWS, Microsoft Azure and Google Cloud Platform to gain hands-on experience.

**Move Beyond the Low-Hanging Fruit**

Public cloud IaaS and PaaS have been very successful at attracting new and innovative applications that are natively designed to take advantage of an elastic, scalable and highly available infrastructure. However, when we assess existing enterprise applications that have been migrated to the public cloud, the landscape is different.
Figure 6 is based on Gartner’s client inquiry data. It presents a general view of which applications have moved to the cloud, which cloud platforms they have migrated to, and why they were migrated. Of course, there are exceptions, but a significant majority of organizations have migrated applications based on the patterns shown in Figure 6.

Figure 6. Application Migration Approaches

As shown in Figure 6, many organizations have begun migrating some of the following workloads to the cloud: website, e-commerce, messaging/collaboration, development/testing and support applications. Although some enterprises have begun to move production and Tier 1 applications to the cloud, many hesitate to migrate these workloads for the following reasons:

- Lack of trust in the public cloud
- Lack of public cloud IaaS and PaaS maturity to support production workloads
- Lack of the expertise needed to successfully migrate
Lack of motivation or business drivers

In 2017, customers must move beyond migrating the "low-hanging fruit." Many of the shortcomings that prevented organizations from migrating production and Tier 1 applications to the public cloud have now been addressed. Therefore, customers that subscribe to a cloud-first strategy should begin to:

- Identify a suitable time frame to reassess where production and Tier 1 applications should be hosted
- Migrate those that are suitable to the right cloud layer

SAP recently certified its software for deployment on AWS and Microsoft Azure, providing a good testament to the hyperscale cloud providers' readiness and maturity to host production and Tier 1 workloads on IaaS and PaaS. (See "Migrating Production Applications into Public Cloud IaaS." )

Multiprovider Strategies Will Become the De Facto Standard for IaaS and PaaS

Many organizations have already invested in a single provider by learning its service offerings and building internal skills and expertise. However, cloud providers continue to innovate in their platform offerings, and the provider market is becoming more competitive on both technology and business fronts. The expanding market is causing a number of organizations to consider use cases where one provider may be better-suited for one application, while a second provider may be better-suited for a different application. These organizations are looking at the cloud for particular applications, rather than considering whole-scale migration of cloud applications from one provider to another.

In addition, many organizations recognize that a single strategic cloud provider introduces potential risks, such as unavailability, lock-in or less-than-ideal placement of applications. Therefore, many organizations are in the process of selecting a second strategic provider. In parallel, business demand is also driving the need for a second provider. Many organizations are evaluating additional providers to:

- Leverage discounts or realize other cost-saving opportunities
- Align to existing investments
- Enable portability and an exit strategy
- Provide tighter integration with their preferred ecosystem of vendors

Regardless of the scenario, Gartner expects multiprovider IaaS/PaaS strategies to become the de facto standard. Today, multiprovider deployments are predominantly in silos by application, but that is likely to change over time.

Planning Considerations

Organizations are already using multiple providers at the SaaS layer, and most have a single IaaS provider. In 2017, organizations should start the process of evaluating and selecting a second IaaS/PaaS cloud provider. To successfully navigate this transition, IT must:
Plan for a multiprovider strategy

Create a multiprovider design approach

Develop a management strategy, and broker cloud services to the business

Plan for a Multiprovider Strategy

A multiprovider strategy offers the opportunity to match each application with the most appropriate provider. It also offers risk disaggregation by reducing provider lock-in.

Organizations that are looking to select the ideal platform provider commonly ask how to compare and choose the platform that is best-suited for their applications. AWS, Microsoft Azure and Google Cloud Platform are the biggest providers in the IaaS market, and the majority of Gartner inquiries about IaaS providers relate to them. As such, Gartner has evaluated these platforms through In-Depth Assessments based on our "Evaluation Criteria for Cloud Infrastructure as a Service." These reports are published annually, and recent evaluation scores are shown in Figure 7.

Figure 7. Gartner 2016 Scoring of Cloud IaaS Platforms

<table>
<thead>
<tr>
<th></th>
<th>Required</th>
<th>Preferred</th>
<th>Optional</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon Web Services</td>
<td>92%</td>
<td>71%</td>
<td>61%</td>
</tr>
<tr>
<td>Microsoft Azure</td>
<td>88%</td>
<td>57%</td>
<td>47%</td>
</tr>
<tr>
<td>Google Cloud Platform</td>
<td>70%</td>
<td>41%</td>
<td>24%</td>
</tr>
</tbody>
</table>

Refer to the following Gartner reports for details:
- "Evaluation Criteria for Cloud Infrastructure as a Service"
- "In-Depth Assessment of Amazon Web Services"
- "In-Depth Assessment of Microsoft Azure IaaS"
- "In-Depth Assessment of Google Cloud Platform"

Source: Gartner (October 2016)

In 2017, organizations that have not already chosen a second strategic cloud provider should start evaluating, onboarding, integrating with and offering a secondary provider. During the process, IT organizations should focus on the manageability of multiple providers, and on how multiple providers will impact IT processes and tools. This effort will lead to procuring a third-party management framework or broker. It will also result in the centralization and standardization of processes such as network integration, data integration, asset management, deployment management and financial management. For more details, see "Selecting an Approach for Managing Public Cloud Services."
Create a Multiprovider Design Approach

When creating a multiprovider design approach, organizations must first decide on how they intend to use multiple cloud providers. Potential approaches include the following:

- **Use different workloads with different cloud providers.** This approach is fairly straightforward and is the use case Gartner sees predominantly today: Organizations deploy different workloads on different clouds. For example, they may decide to deploy their SAP high-performance computing workloads on AWS, and their e-commerce, messaging and collaboration workloads on Microsoft Azure (or vice versa).

- **Use the same workload across multiple cloud providers.** This approach is more complex, and Gartner sees it very rarely today. This approach is suitable for customers that are looking to reduce lock-in to a single cloud provider, and looking to mitigate risk from a potential outage at any single cloud provider. To design an application for consumption across multiple providers, customers have three options:
  1. **Develop the application to work with multiple providers' native features and services (for example, load balancers).** This approach is costly and requires expertise across multiple providers. It must have a true business driver that supports and justifies the expense.
  2. **Drive portability and automation.** Evaluate automation tools, such as Puppet and Chef. These tools enable organizations to reconstitute and/or redeploy applications across a second provider with relatively little effort. Also, consider leveraging containers to make the application as portable as possible across a multiprovider environment. Although containers are a great option, they have limitations. Portability decreases as customers employ more native and value-added capabilities from the cloud providers. This is an option only for custom-developed applications.
  3. **Deploy different components of an application across multiple providers, potentially leveraging a microservice approach.** This is the most common scenario today, and it requires no integration between the two cloud providers' platforms. However, organizations must govern and manage across cloud platforms.

- **Use one provider for production, and a second provider for disaster recovery.** This approach is more complex and seen less commonly today. This option is most viable for organizations leveraging a cross-connect solution, such as AWS Direct Connect or Microsoft Azure ExpressRoute. In this approach, customers deploy all workloads to one cloud provider, while developing a second deployment that can be initiated at any moment to fail over to a disaster recovery cloud provider. A highly automated deployment, through the use of templates or blueprints, will cover the provisioning of the compute nodes and the continuous replication of data, but will require prework for infrastructure components like networking and security. You cannot rely on the provider’s replication services because they will not function across other providers.

Regardless of the multiprovider design approach customers choose to pursue, one constant infrastructure component needs to be efficiently architected to enable one or all of these approaches. That component is networking — more specifically, connectivity. Gartner believes that
most organizations will have hybrid architectures for the foreseeable future. However, the network designs that customers employ today will not be efficient for a hybrid architecture that includes an on-premises data center and multiple clouds (including IaaS, PaaS and SaaS). For example, some organizations today are using Office 365, Microsoft Azure IaaS and PaaS, AWS, and Salesforce, in addition to their on-premises data centers, regional offices and branch offices. This is not an unusual customer environment, but it requires that IT rearchitect the network and connectivity to clouds.

In 2017, organizations must evaluate their networks and prepare to rearchitect their WANs to more efficiently enable a multiprovider approach. In doing so, these organizations must:

- Consider a regionalized connectivity approach instead of a traditional Multiprotocol Label Switching (MPLS) approach
- Investigate and adopt software-defined WAN (SD-WAN)
- Consider broadband usage
- Consider interconnection sites for their proximity to major cloud providers

For more in-depth insight on cloud networking, see "How to Optimize Your Enterprise Network for Hybrid Cloud."

**Develop a Management Strategy, and Broker Cloud Services to the Business**

Many organizations are now focused on enabling ITaaS — where IT brokers both traditional and cloud services to the business (see Figure 8).
Cloud management problems become more complex as multiple providers are deployed, and organizations need to manage across cloud providers. Forming partnerships with multiple strategic cloud providers offers choice in deployment options. Such choice allows the IT organization to be more responsive and adaptable to business needs. However, it requires IT to compare public cloud providers and make recommendations for application placement, whether on-premises or in a public cloud.

Another key priority is to develop a cloud management strategy. Cloud management is often overlooked until a problem occurs. A management strategy helps organizations avoid failures that are likely to result in new tools and in unwanted, added expenses. However, many organizations simply do not know what tasks they need to manage in the cloud. The maturity of public cloud providers, combined with the adoption of public cloud services, introduces a new set of management requirements. Organizations need integration between their on-premises traditional management tools and their public cloud deployments, yet the management tool market is still very immature. See "A Comprehensive List of Management Requirements for Organizations Using Public Cloud Services" for a detailed list of public cloud management tasks. This list can be prioritized and then used to generate an RFP to aid in tool selection.
Corporate IT Will Live in a Hybrid World for the Foreseeable Future

"Cloud first" does not mean "cloud always" or "cloud only." Data centers will live on in most companies for the foreseeable future, so these organizations must augment their processes and tooling in order to integrate their data centers with the public cloud. "Cloud first" also doesn't mean that organizations should take everything in their data centers and build an exit strategy. Some organizations are building data center exit or consolidation strategies, but many intend to augment data center capacity with the public cloud. That means the majority of organizations will live in a hybrid world for the foreseeable future.

While many organizations expect to end up in a hybrid state, few can clearly articulate what "hybrid" means in terms of architecture. Often, the term is used inconsistently. Hybrid architectures become the footprint that enables organizations to extend beyond their data centers and into cloud services across multiple platforms. To enable end users to consume cloud services at scale and in a repeatable fashion, organizations must pay careful attention to the architectures for foundational components like networking, identity and security.

Just as organizations are embracing cloud and maturing in their adoption of public cloud services, IT is being challenged to make the data center more agile and efficient. Some use cases within organizations will remain better-suited to on-premises deployment. For those uses cases, it is imperative that integrations exist at all layers — infrastructure, workloads, applications and cloud platforms.

Planning Considerations

The public cloud should be woven into the organization's IT modernization strategy. It should be treated as a tier of services that solve the modern business challenges of mobility, scalability, globalization and speed to market. In 2017, organizations must plan for a hybrid IT environment. This will require evaluating new architectural approaches and investments. IT organizations should:

- Identify the level of integration required between traditional data centers and public cloud platforms
- Invest in hybrid architectures to enable public cloud consumption
- Establish a data protection strategy that spans the data center and the public cloud

Identify the Level of Integration Required Between Traditional Data Centers and Public Cloud Platforms

Moving your organization into the hybrid IT world of interconnected technology silos should not be an ad hoc process. Careful planning of the journey will allow you to anticipate the critical inflection points and to implement hybrid IT successfully.

Organizations should plan for hybrid IT in terms of the integration of technology silos across four levels: multiprovider management, hybrid applications, hybrid orchestration and hybrid infrastructure (see Figure 9).
Integration is implemented through stages of maturity. At each stage, you will face major changes to organizational structures, toolsets, governance processes and required skills. The inflection points at which you face significant changes are the events you should plan for. For more information, see "Hybrid Architectures for Cloud Computing."

**Invest in Hybrid Architectures to Enable Public Cloud Consumption**

As cloud adoption rises, an IT organization’s supported applications inevitably begin to span multiple locations. When this happens, IT should focus on the integration between these systems, concentrating on the primary areas of identity management, networking, security and storage/data. To provide a seamless hybrid cloud experience to users, organizations should address all of these areas as early as possible, because retrofitting necessary controls into live production applications can be very disruptive.

- **Identity management** — To provide connectivity from on-premises environments, IT organizations should evaluate standards-based identity federation solutions, such as Security Assertion Markup Language (SAML) and OpenID Connect. They should also evaluate directory synchronization solutions to replicate users from an on-premises directory environment to third-party cloud services. For more in-depth insight on identity management and federation with public cloud services, see "Modern Identity and APIs: Mobile, OpenID Connect, OAuth, JSON and REST."

- **Networking** — Enterprises often deploy cloud services without revisiting their WAN architecture, but today’s enterprise WANs were not built with cloud computing in mind. Organizations will need to assess the network impacts of adopting cloud services. They should aim to make WAN infrastructure as carrier-, transport- and cloud-service-provider-agnostic as possible to minimize lock-in and maximize overall business agility. For more in-depth insight on cloud networking, see "How to Optimize Your Enterprise Network for Hybrid Cloud."
Security — Inadequate security practices can quickly turn an otherwise well-intentioned cloud initiative into a massive disaster for an organization. Working with application stakeholders, IT organizations must fairly and adequately assess business risks for applications that leave the organization’s "four walls" and reside in the hands of a third party. IT organizations must also re-evaluate security policies that were established for on-site execution to see whether they need to be modified when applications are hosted in a third-party cloud. They must then determine whether the provider has adequate security controls, such as firewalls, role-based access controls, encryption or tokenization, to meet those requirements. For more in-depth insight on assessing the security of public cloud services, see "Effective Security Assessment of Public Cloud Services."

Storage/data — Cloud providers don’t natively protect or replicate data placed in their clouds. Some architectural approaches within hybrid infrastructures allow you to keep your data in your environment while leveraging public cloud services for compute (see "Using Colocation-Based Hybrid Cloud Architecture to Ensure IaaS Mobility and Reduce Lock-In"). Organizations may also implement a hybrid architectural approach for cloud-based backup or disaster recovery.

Establish a Data Protection Strategy That Spans the Data Center and the Public Cloud

Corporate data is often the most important asset that an organization owns. Data unlocks the secrets to an organization’s success, intellectual property, know-how and operational excellence. It also contains the organization’s financials, client lists and contacts. Protecting this data is a fiduciary responsibility. While most organizations have developed a robust and effective on-premises data protection strategy, in 2017, organizations must re-evaluate this strategy to ensure that it can support all cloud layers (IaaS, PaaS and SaaS), data sovereignty, and compliance requirements. Refer to "2017 Planning Guide for Data Center Modernization and Infrastructure Agility" for more details on the trend "IT organizations will protect data and services regardless of their location."

The customer service agreements for the large hyperscale providers — AWS, Microsoft Azure and Google Cloud Platform — clearly indicate that customers are responsible for their own data. While these cloud providers will make every effort to preserve the data, cloud providers in general do not offer protection against data corruption, and they do not have granular data restore capabilities. Cloud providers continue to invest in their architectures to make them highly resilient and highly available, but resiliency and availability are not enough to protect against data loss or data corruption. Moreover, cloud providers do not typically offer a robust backup service (with the exception of Microsoft, which has Azure Backup for the protection of VMs). These providers do, however, offer point-in-time volume snapshots, versioning capabilities and transaction archive capabilities (for databases). For more information, see "Take Responsibility for Backing Up Cloud-Based Data."

In 2017, Gartner advises that organizations begin to re-evaluate their data protection strategies. Recommendations include:
Assess current on-premises data protection processes, recovery point objectives (RPOs) and recovery time objectives (RTOs). Determine whether any changes need to be made to enable and protect cloud usage.

Assess current data protection tools. Determine whether they can extend to the cloud, or whether retooling is necessary.

Look beyond traditional data protection vendors to complement the organization's new data protection strategy. Although many of these traditional vendors are evolving for the cloud (some more slowly than others), there are many third-party data protection vendors that focus specifically on cloud data protection.

Furthermore, as organizations rethink their data protection strategies, they must ensure that their tools enable the following:

- **Application consistency** — The snapshot capabilities offered by the cloud providers are mostly crash-consistent ones, meaning they are point-in-time snapshots that ignore any open files or cached data. Crash-consistent snapshots are usually not recommended for database systems or for messaging systems such as Microsoft Exchange. The tools you select must have application-consistent capabilities that can tie into Volume Shadow Copy Service (VSS) on Windows, for example, to account for any open files or cached data. Tools with these capabilities offer a more complete backup and a more consistent restore.

- **Restore granularity** — The tool must be able to support file- and object-level restore capabilities across different platforms, services and operating systems (Windows and Linux).

- **Backup data location** — If you choose to leverage the cloud as a backup destination, your selected backup tool must integrate with object-based cloud stores.

Given the sensitivity and importance of data protection, prioritizing it to the top of the "rethink and rearchitect" list is a must.

**Most Organizations Will Forgo Trying to Build Full On-Premises Private Clouds**

Gartner inquiries indicate that many enterprises are no longer trying to build private clouds, and instead have accepted the public cloud. The allure of building a fully functioning, on-premises private cloud is fading because many implementations are failing to deliver against the expectations of users or IT staff. The process of building and managing an internal, full-function IaaS private cloud is much more complex and costly than virtualizing a data center (internal) or adopting public cloud computing (external). Successful private cloud projects tend to be in web-scale companies that invest significantly to differentiate their infrastructure and application development.

Gartner sees high value in embracing cloud computing as a method to achieve the scale and agility that most IT organizations cannot realize with their data centers. Cloud providers also deliver innovation on this faster, more economical infrastructure through a highly sophisticated development community. It is impossible for most IT organizations to match this scale at a comparable price point, and certainly not within the time frame that the cloud providers can meet.
Cloud providers continue to purchase infrastructure at volume discounts, and often have access to faster hardware before traditional enterprise organizations.

Few organizations can justify the investments needed to stay competitive with major cloud providers. Cloud providers can purchase infrastructure at a much lower cost than enterprises can, due to volume discounts. They also employ numerous, sophisticated developers to build software differentiation on top of the already discounted infrastructure. The cloud providers can develop an extensive set of service offerings that traditional enterprise organizations cannot compete with on cost. Given the capabilities and the pace of innovation of the large public providers, private cloud implementations are often functionally obsolete before the projects are completed.

Moreover, organizations that attempt to progress directly from server virtualization to private IaaS often fail because of the skills required, the organizational issues and the unexpected complexity. Building private clouds requires a transformation in usage patterns, IT staff skills, organizational structure, processes, funding and technologies. The magnitude of change required is too much for most organizations to digest successfully in the time frames expected.

Planning Considerations

In light of this trend, IT organizations should plan to do the following in 2017:

■ Re-evaluate public cloud as the preferred deployment model.
■ Determine the level of automation and self-service required.
■ Evaluate hosted private cloud as an alternative to building a private cloud.

Re-evaluate Public Cloud as the Preferred Deployment Model

Some organizations still believe that the cloud is not secure, and therefore, they cannot move applications into the cloud. However, many organizations are moving past this mindset and focusing on building security and governance policies that enable the business to use cloud services in a governed manner.

Through 2020, 95% of cloud security issues will be the organization’s fault, not the cloud provider’s.4

Unlike the organizations that are still skeptical of public cloud security, many other organizations believe that the cloud providers have a better understanding of how to implement robust security policies (as shared through Gartner inquiries). They often go as far as to say that the cloud providers understand how to secure the cloud better than they can secure their own data centers. This is a
significant paradigm shift that Gartner has seen in the past two years, and warrants the cloud architect really challenging any security-related concerns. Security should always be a top concern, but organizations must push forward and define the security policies and procedures that allow the organization to leverage cloud services. Furthermore, the cloud architect must engage networking and identity architects to develop a strategy that allows users to securely connect and authenticate to cloud service providers in a governed manner.

If your organization is conservative and risk-averse, reference Gartner’s "Decision Point for Application Placement: Cloud, Managed, Colocation or Do It Yourself" to assess whether any of your enterprise’s applications are candidates for the public cloud. Then, engage technical leaders on the security, networking and identity teams to evaluate risk mitigation techniques, as detailed in "Effective Security Assessment of Public Cloud Services."

Some organizations may think they can host the applications more inexpensively in their own data center. Gartner is often asked if cloud will be more cost-effective than traditional hosting, and we have published a cost model that addresses this question (see "Calculating and Comparing Data Center and Public Cloud IaaS Costs").

"Don't assume you will save money unless you have done the hard work of honestly analyzing the situation."  

In reality, public cloud implementations may or may not be more cost-effective, depending on the circumstances. Gartner has seen some organizations deploy a number of applications at scale that have been well-architected and well-managed, but these deployments required additional investment. Other organizations may trip up on those key design decisions and lose control of their environment, resulting in costly remediation measures. These organizations will not be more cost-effective in the cloud. Be mindful that cost models can be manipulated. Organizations must really evaluate all the benefits of cloud computing (not just cost) and drive organizational alignment to those benefits.

In some cases, organizations may not find a suitable match after they’ve evaluated a workload need against the public cloud providers in the marketplace. A cloud solution may not be possible due to various roadblocks, such as:

- Compliance requirements that mandate that certain data cannot leave a country’s borders
- Software vendors that will not amend their licensing agreements to allow an organization to run their software outside of its own facilities

In these scenarios, on-premises solutions — either traditional architecture or a private cloud — are likely to be the only viable option.

**Determine the Level of Automation and Self-Service Required**

Gartner does not expect private workloads to disappear in the near future. Conservatively, 80% of active VMs still run on private infrastructure. What is needed is more nuanced thought about the
categories of workloads that need to remain "private" and the types of environments in which they should run. In their strategies for modernizing their virtualization environments, many organizations are considering simpler alternatives to building a private cloud IaaS. Gartner has seen many organizations decide to manage private workloads in a standardized, automated virtualization environment and to address their "as a service" requirements with public cloud functions.

The secret to a successful private cloud implementation is to do just enough and only as you need it. You can’t outpace public cloud providers in terms of cloud development. Pick only what you need for private infrastructure, and implement it well. Those applications that are best-hosted on public cloud infrastructure should be placed there, and the first option for hosting new workloads and Mode 2 applications should be the public cloud (see Note 1). However, certain workloads will have to be isolated and hosted on dedicated (private) infrastructure due to reasons such as security, performance, financial models, compatibility, life cycle control or skill sets.

Before developing a private cloud strategy, confirm you really need the attributes of cloud computing:

- Rapid provisioning
- Self-service
- On-demand services
- Pay-as-you-go services
- Services using internet technologies (in this case, within your data center firewall)

If all five cloud attributes are necessary, evaluate hosted private cloud deployment options. If all five cloud attributes are not necessary, you may achieve greater success by further automating your virtualization estate.

Consider simpler alternatives to a private cloud IaaS for extending your existing virtualization environment — either as a first step in a journey to full private cloud IaaS, or as a long-term hybrid solution that combines private and public cloud functions. Attempting to do too much in the private cloud at the beginning is a common cause of failure. Trying to accommodate all workloads inspires a least-common-denominator design. It also causes overruns in project cost and time, due to the exponential increase in complexity created by attempts to automate multiple components. You should focus initially on providing better management, automation and agility to only the private services that need them the most.

Virtualization automation solutions allow the IT organization to offer VMs, container hosts or associated infrastructure as an automated service for administrators or end users. VA solutions are simpler but less functional than IaaS. VA can be used as an extension to the virtualization management environment, or as the first step toward building an internal IaaS private cloud. (See "'Just Enough’ Private Cloud: Deliver Value Quickly With Virtualization Automation.")

A common use case for private cloud today is to speed up the provisioning of infrastructure for DevOps-style projects using continuous integration/continuous deployment methodologies. Many
organizations are addressing these requirements through VA or private PaaS options rather than building an IaaS private cloud.

PaaS frameworks, such as Apprenda, Cloud Foundry and Red Hat OpenShift, provide services that enable developers to create applications in an automated environment, while masking the underlying complexity of the infrastructure automation. Utilizing PaaS for DevOps use cases without building a full IaaS cloud for end users is also an option.

Thus, organizations looking to improve the agility of their virtualized data centers have several alternatives to building a fully functioning private cloud IaaS:

- **DevOps only** — Automate development/testing with VA, but avoid building a full IaaS private cloud.
- **DevOps and production** — Take the steps above, but also automate some production workloads using VA.
- **Hosted/outsourced private cloud** — Leverage an outsourcer or service provider to host and/or manage a private cloud on- or off-premises (see the Evaluate Hosted Private Clouds as an Alternative to Building a Private Cloud section).
- **PaaS** — Implement an internal PaaS environment without internal IaaS.
- **Hybrid virtualized** — Stay with a highly virtualized data center, and leverage the public cloud for appropriate workloads.

**Evaluate Hosted Private Clouds as an Alternative to Building a Private Cloud**

There are different definitions and interpretations of private cloud. Gartner commonly sees four different private cloud implementations, as shown in Figure 10.
Figure 10. Private Cloud Implementations

One solution to the private cloud complexity issue is to outsource the difficult cloud control functions, as well as the mundane chores of managing hardware, to a third-party provider. This option is called "hosted private cloud" (see "Hosted Private Clouds: The Alternative to Building It Yourself").

One of the easiest ways to reduce complexity is to access a capability that has already been industrialized by a large-scale provider. This is also called "externalizing the function." Accessing capabilities that have already been industrialized is usually more efficient than trying to build them yourself. The question to be answered here is, "What components does my organization need to build and operate, and what can we access from a third-party provider?"

Organizations should first define the workloads that truly need to remain private. For those workloads, they should evaluate third-party offerings for outsourced private cloud services or for hosted private clouds before deciding to build an on-premises private IaaS cloud.

Organizations should also determine:
- The level of control they need over management of the system infrastructure (data center, networking, storage and compute)
- The level to which they will build, own and maintain the cloud management platform (control plane)

The transformation to service-oriented IT is difficult in terms of processes, organization and culture. However, third-party private cloud services can speed this transformation.

**Setting Priorities**

Most organizations will not be able to tackle every planning consideration described in this document. Therefore, organizations should set priorities based on their specific needs and consider using the following priority-setting framework.

**For all organizations:**

- Advocate a cloud-first strategy, and build a multiyear cloud maturity plan.
- Empower the cloud architect to work across functional teams, and start building expertise across all functional areas.
- Establish a multiprovider strategy, and begin the process of onboarding a second strategic provider, if you have not done so already.
- Develop a management strategy and approach to ensure you retain governance of cloud deployments. Plan for multiprovider management, learn the providers’ native services and evaluate third-party tooling options.
- Plan for cloud service expense management (CSEM). Evaluate tooling alternatives to retain control of cloud spend.
- Push teams to evaluate the next "tier" of workloads for deployment or migration. Develop architectures to mitigate risk and to deliver the availability your end users demand.
- Begin the transformation necessary to broker cloud services to the business. This will require cloud expertise across public cloud platforms, and will require IT to augment current processes. In addition, new tooling will be required.
- Consider VA and hosted private clouds as alternatives to the difficult and expensive project of building your own internal private cloud.

**For organizations just starting out with cloud computing:**

- Document your cloud strategy. Identify the benefits and risks of cloud computing for your organization. Document what aspects of the cloud you will and will not use, and why.
- Encourage leadership to appoint a cloud architect to oversee the cloud strategy and to be responsible for tracking movements in the cloud industry.
- Create a cloud decision framework to help select the best location to host applications and data. If that location turns out to be the public cloud, the framework should also provide guidance concerning whether IaaS, PaaS or SaaS is the right deployment model.

- Prioritize a SaaS-based model for all applications that you can relinquish some control over. A SaaS solution should be considered first for all new software procurement decisions to start freeing IT from the burden of managing and maintaining a large portfolio of commercial off-the-shelf (COTS) and custom applications.

- Choose a strategic, blended IaaS and PaaS strategy, and select two strategic providers that you will maintain a relationship with for several years.

- Start designing for hybrid architecture, prioritizing hybrid infrastructure. Hybrid infrastructure becomes the foundation that enables your organization to consume cloud services at scale. This foundation includes a strategy for integrating networks, identity, data and services across multiple cloud providers.

Gartner Recommended Reading

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

- "Solution Path for Developing a Public Cloud Strategy"
- "Designing a Cloud Strategy Document"
- "Decision Point for Application Placement: Cloud, Managed, Colocation or Do It Yourself"
- "Decision Point for Selecting an Application’s Cloud Migration Strategy"
- "An Emerging IT Role: The Cloud Architect"
- "The Cloud Architect’s Guide to Implementing Public Cloud Services"
- "Key Services Differences Between AWS and Azure — Availability, Network, Compute and Storage"
- "Hybrid Architectures for Cloud Computing"
- "Building an IT Business Case for Public Cloud IaaS or PaaS"
- "A Comprehensive List of Management Requirements for Organizations Using Public Cloud Services"
- "Hosted Private Clouds: The Alternative to Building It Yourself"
- "Evaluation Criteria for Cloud Infrastructure as a Service"
- "In-Depth Assessment of Amazon Web Services"
Evidence
Gartner routinely fields inquiries from clients on the topics of cloud computing and data center modernization. This research is based on client inquiry data collected between January 2015 and September 2016. These clients were located in North America, Latin America and EMEA, and spanned a wide array of industries.

1 "Market Insight: Cloud Shift — The Transition of IT Spending From Traditional Systems to Cloud."


3 "Predicts 2016: Cloud Computing to Drive Digital Business."

4 "Clouds Are Secure: Are You Using Them Securely?"

5 "The Top 10 Cloud Myths."

Note 1 Bimodal IT, Mode 1 and Mode 2
Mode 2 refers to bimodal IT, which is the practice of having two modes of IT, each designed to develop and deliver information-intensive and technology-intensive services in its own way:

- Mode 1 is traditional, emphasizing safety and accuracy.
- Mode 2 is nonsequential, emphasizing agility and speed.

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