In 2019, hybrid IT will be the standard. Technical professionals focused on cloud must continue to advance cloud-first strategies, embrace multicloud and maintain on-premises environments, with a focus on integration and brokering. This Planning Guide outlines trends for successful cloud adoption.

Key Findings

- In 2019, the lines between IaaS and PaaS will continue to blur. Organizations will need to develop the right strategies for deciding how to place or build an application on the right services, and how to manage across all IaaS and PaaS on a multiprovider basis.

- Most organizations expect cloud to be cheaper. To realize cost savings, they must move the right applications, optimize them properly and continuously track spend.

- Hybrid IT has become the standard, as organizations rapidly adopt cloud services while also maintaining traditional on-premises hosting environments. The keys to success will be managing all integrations and implementing management tasks (like provisioning and monitoring) while brokering cloud services to the business.

- The most successful cloud-adopting organizations appoint or hire a cloud architect, and grant this role principal responsibility for the organization’s cloud initiatives. As cloud adoption matures, organizations also establish a cloud center of excellence and hire cloud engineers.

Recommendations

Technical professionals focused on cloud computing:

- Start developing and implementing a cloud-first strategy now, with an emphasis on multicloud architecture. Organizations must advance the use of public cloud services to become the primary, prioritized and promoted deployment model.

- Embrace public cloud while continuing to evolve your data center resources to be more efficient and more hybrid. Define integration strategies between data centers and public clouds.
- Strategically rethink and invest in your network architecture for multicloud. Implement robust network architecture that can enable hybrid IT and multicloud cost-effectively and redundantly.

- Act now to find or become your organization’s cloud architect. Promote internally from roles such as enterprise architects, I&O architects or application architects. Hire externally by clearly defining the position using the research in this report.

Table of Contents

Cloud Computing Trends........................................................................................................................3
Organizations Will Advance Cloud-First Strategies With Multicloud Adoption........................................7
Planning Considerations.......................................................................................................................8
Optimizing Workloads for IaaS, PaaS and SaaS Will Be an Increasingly Critical Priority....................20
Planning Considerations.......................................................................................................................21
Hybrid IT Strategies Will Continue to Mature Across Organizations.................................................32
Planning Considerations.......................................................................................................................33
Organizations Will Invest in Developing Cloud Skills Across Disciplines...........................................48
Planning Considerations.......................................................................................................................48
Setting Priorities...................................................................................................................................56
Gartner Recommended Reading...........................................................................................................57

List of Tables

Table 1. Contextual Independence Principles Aligned to the Cloud Computing Tiered-Service Model... 28
Table 2. Native Automation Tools for Public Cloud IaaS........................................................................31

List of Figures

Figure 1. Cloud’s Evolution to Become Mainstream................................................................................4
Figure 2. Solution Path for Implementing a Public Cloud Strategy...........................................................6
Figure 3. Long-Term Multistep Cloud Migration Strategy.........................................................................12
Figure 4. Solution Path for Implementing a Public Cloud Adoption Maturity Plan.................................14
Figure 5. Multicloud Governance...........................................................................................................16
Figure 6. Evaluation Criteria Categories and Attributes: The Cloud Management Wheel.......................19
Figure 7. Application Migration Options..................................................................................................23
Figure 8. LIFESPAN Defined.....................................................................................................................24
Figure 9. Integrated IaaS and PaaS..........................................................................................................26
Cloud Computing Trends

Cloud computing is the platform for innovation that the digital business demands. Cloud has become the foundation that enables businesses to transform, differentiate and gain a competitive advantage. In fact, cloud strategies are now quickly evolving into data and analytics, Internet of Things (IoT), and application architecture strategies as well. Many organizations are now focused on cloud-first strategies as they turn their attention to advancing the use of cloud services across the business. Given this context, organizations must continue to invest in and mature their cloud competency to ensure it becomes the mainstream computing platform in the organization (see Figure 1).
Organizations will struggle to move forward, and their maturity will vary across the different workstreams. Furthermore, cloud initiatives are often delayed by internal politics, with some in the business hesitant to relinquish their control. Other parts of the organization may think they can build and protect their applications better through the use of internal resources. However, most organizations just can’t compete with the pace of innovation and economies of scale of the cloud providers. Most cloud providers are developing value-added services on top of this faster, less expensive infrastructure with massive automation and standardization of commodity hardware. The pace of innovation is fastest in the public cloud, and competitors that can react faster tend to win in markets.

Cloud projects are complex for two main reasons:

- Organizations typically have multiple projects executing at different speeds. One team may be down the path of selecting providers and developing architectures, while another team may be just getting started. Depending on the size of the organization, these teams may not even be aware of each other’s initiatives.

- Many people need to be involved in cloud initiatives to ensure the proper architecture is implemented. Many legacy IT operations tools and processes can’t easily be extended to the cloud, so new tools are required for monitoring, provisioning, troubleshooting, backup and other
traditional processes. However, organizations often get started with these initiatives before their cloud teams and their required skills are completely developed.

In a recent Gartner survey of technical professionals based primarily in North America, 40% of respondents indicated that their organizations would be spending the majority of new or additional funding on the cloud. However, the survey also found that the cloud is the most common area for talent gaps.\(^1\)

Overcoming these cloud implementation problems requires a sound process. The starting point for developing this process is Gartner’s “Solution Path for Implementing a Public Cloud Strategy,” which provides a high-level cloud-first adoption framework (see Figure 2). This framework can be used to identify the investments and steps necessary to successfully implement your cloud initiatives. However, even organizations using the adoption framework must be aware of the rapidly evolving trends in the public cloud market and adapt accordingly.
Figure 2. Solution Path for Implementing a Public Cloud Strategy

1. Develop Strategy
   - Develop Cloud Skill Sets
   - Create Application Assessment Methodology
   - Develop Business Case, and Document Strategy

2. Build Cloud Foundations
   - Select Cloud Providers
   - Adopt Native Tooling
   - Integrate Core Infrastructure

3. Architect and Mitigate Risks
   - Design for Multicloud
   - Architect for Availability and Performance
   - Architect Security Best Practices

4. Enable Governance
   - Develop Governance Methodologies
   - Develop Self-Service Strategy
   - Create Financial Management Processes

5. Achieve Operational Excellence
   - Automate and Orchestrate Workloads
   - Monitor and Optimize Consumption
   - Implement Multicloud Management Tools

Source: Gartner (October 2018)
This Planning Guide assesses the major technology planning trends in 2019 for cloud computing, and outlines important planning considerations for developing successful cloud strategies. The following trends are examined in this report:

- Organizations will advance cloud-first strategies with multicloud adoption.
- Optimizing workloads for IaaS, PaaS and SaaS will be an increasingly critical priority.
- Hybrid IT strategies will continue to mature across organizations.
- Organizations will invest in developing cloud skills across disciplines.

Organizations Will Advance Cloud-First Strategies With Multicloud Adoption

Gartner recommends that organizations continue to mature their cloud-first strategies — where the cloud is primary, prioritized and promoted. If you have not developed a cloud-first strategy yet, you are likely falling behind your competitors. IT organizations have moved past asking whether applications can be deployed or migrated to the public cloud. Instead, they are commonly accepting the pace and innovation of the cloud providers as foundational to their business.

Cloud architects are prioritizing cloud-first approaches by asking organizations to justify why applications should be deployed on-premises instead of in the public cloud.

This is a sign of maturity for the public cloud, and IT organizations have experienced this situation before with virtualization. When server virtualization first matured, many virtualization architects told IT organizations that they needed to justify a physical server or it would get virtualized.

IT organizations have surrendered to the reality that the move to the public cloud will likely be across more than one cloud provider. Most organizations are already using multiple cloud providers for SaaS offerings. Many have also already invested in a single cloud provider for infrastructure as a service (IaaS) or platform as a service (PaaS). However, the expanding cloud market is causing some 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 one. These organizations are looking at the cloud for particular applications, rather than considering wholesale migration of cloud applications from one provider to another.

Organizations will give preference to a single provider for the majority of their workloads (up to 70%). However, they are likely to diversify a portion of their application portfolio, up to 30%, on a secondary provider. As a result, the adoption of multicloud strategies, architectures and management solutions will increase.
Multicloud is no longer a matter of “if” — it’s a matter of “when.”

In addition to advancing their cloud-first strategies, organizations must plan for multicloud adoption. This requires investments in skill sets, provider knowledge across the business, and cloud management and governance expertise.

Planning Considerations
Because building, implementing and maturing cloud strategies will continue to be a top priority in 2019, IT organizations must take the steps needed to:

- Develop a cloud-first and multicloud strategy
- Continuously practice workload placement analysis
- Plan for cloud adoption maturity
- Establish multicloud governance and management processes
- Develop a multicloud management tooling strategy
- Evaluate multicloud SaaS integration requirements

Develop a Cloud-First and Multicloud Strategy

“Cloud first” does not mean “cloud always.” For some organizations, the long-term goal may be to move all applications out of their data centers. For others, cloud-first may mean moving a subset of applications to the public cloud. Regardless of your approach, it is important to prioritize investments to advance the organization’s use of cloud services.

A cloud-first strategy should extend 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 the merits of cloud to business leaders to help them develop and extract business benefits that will yield a competitive edge and greater profitability.

As technical professionals begin to evangelize cloud in the organization, some concerns and challenges will arise that they will have to address. A multicloud strategy can help by providing a mechanism to:

- **Mitigate risk:** As organizations begin to rely on cloud providers for production workloads, and as they begin to migrate a significant amount of their assets to public cloud providers, the question of risk mitigation will inevitably arise.
- **Reduce lock-in:** Public cloud computing has several service models, and the higher up the stack you go — from IaaS, to PaaS, to SaaS — the more locked-in you become to that cloud provider. For example, if you are using virtual machines (VMs) and containers, you can migrate these assets and their data relatively easily. However, as you start to consume PaaS services, such as function as a service (FaaS), analytics, queuing services and proprietary databases, it becomes harder to move between cloud providers. Lock-in is not necessarily a bad thing, since it often allows clients to access many innovative features and capabilities. It is also not necessarily permanent, since organizations can always exit a lock-in situation. However, such exits can be operationally challenging, time consuming and costly. For more information, see “A Guidance Framework for Architecting Portable Cloud and Multicloud Applications.”

- **Enable business continuity (BC) and disaster recovery (DR):** Many organizations look to the public cloud for BC/DR purposes. However, when they begin migrating their production assets to a public cloud provider, the BC/DR question surfaces again, and a secondary provider may be required for that use case.

- **Benefit from cloud provider innovation:** One reason organizations find the public cloud attractive is the rapid feature and service innovation that it offers. Organizations that opt to use a single public cloud provider may miss out on a game-changing service or feature from another provider that could offer a significant competitive advantage.

- **Reconcile different teams selecting different cloud providers:** Political and cultural differences have always existed between developers and infrastructure and operations (I&O) teams. For many organizations, these challenges were exported to the cloud and resulted in each team selecting a different cloud provider. As the organization’s cloud adoption matures, the organization may realize that its cloud choices must be reconciled under a unified multicloud strategy to truly maximize the benefits of cloud.

- **Address mergers and acquisitions (M&As):** Many organizations that adopt a cloud-first strategy early on subsequently face situations where a secondary public cloud provider is brought into the organization due to an M&A situation.

- **Leverage Microsoft Office 365 adoption:** Office 365 is a good example of how multicloud is being manifested in organizations. Gartner frequently hears from clients that they have been using Amazon Web Services (AWS) for their public cloud initiatives. However, they are also in the process of migrating to Microsoft Office 365, and they plan on using Microsoft Azure ExpressRoute for dedicated connectivity to Azure. This scenario alone puts the company in a multicloud deployment at the infrastructure level — without any kind of planning and with little to no infrastructure integration.

It is important for technical professionals to adhere to architectural disciplines that promote portability and multicloud design. Organizations must architect to mitigate lock-in. They must avoid practices that unwittingly cement their cloud deployments to a particular cloud provider’s services, or that inhibit architects from using multicloud designs where appropriate. These factors are forcing technical professionals to rethink their cloud-first strategies and to begin considering a multicloud-first strategy early on in the process, even if they don’t plan to leverage multicloud immediately. For
more information, see “Decision Point for Selecting Single or Multicloud Workload Deployment Models.”

**Continuously Practice Workload Placement Analysis**

With few exceptions, workloads aren’t deployed within an organization and then left alone. Workload reassessments have always been an important periodic function for IT organizations to perform (often in conjunction with business owners). Reassessments ensure that application capabilities continue to meet the needs of the organization and provide sufficient competitive differentiation.

Historically, assessments have been performed with a heavy focus on feature comparisons to alternative solutions, because the placement of the workload (e.g., in the on-premises data center) was typically a foregone conclusion. However, in the era of cloud, new expanded options for placement and ownership of stack elements come into play. Thus, established workload life cycle management models must be evolved. No longer is it sufficient to simply assess whether an application still meets the necessary features required to support the business. Workloads must now also be assessed to determine whether they are in the best execution venue, or if a change is warranted.

Additionally, the marketplace of potential execution venues — such as the public cloud, private clouds, hosting or colocation — lends itself to greater flexibility overall for workloads, but not without trade-offs. Uncertainty about unfamiliar deployment models and unknown risk factors tend to delay organizational decision making, largely to the detriment of modernizing systems over time. IT organizations need to resist the temptation to stick to familiar data processing models. Instead, they should consider all available delivery options for workloads, based on what provides the best overall outcome for the organization’s mission.

Broadly speaking, the marketplace of cloud computing offerings has reached a maturity level that warrants organizations moving toward a practice of continuous, iterative workload placement analysis. Although cloud computing providers fell short of meeting many mainstream enterprise IT requirements over the past decade, this will no longer be the case in 2019. In recent years, technical and go-to-market improvements in cloud providers of all types have dramatically closed the gap between what enterprise customers would typically expect, and what cloud providers could supply.

Gartner’s [Cloud Decisions](https://www.gartner.com/en) tool can help you compare different cloud provider services, features, SLAs and pricing. Additionally, Cloud Decisions’ intuitive modeling engine, CloudMatch, lets you define your workloads based on your specific requirements and priorities (such as cost, performance and feature requirements). It then offers custom recommendations based on these requirements.

Continuous workload placement analysis involves reassessing workloads on a regular cadence and evaluating whether:
The current execution venue sufficiently meets the organization's needs.

Migration to an alternative model may provide higher value without adding significant risk to the organization’s operations.

Over an application’s life span, an application may move between execution venues more than once, based on the market maturity of relevant cloud offerings and the organization’s needs. For example, an organization that wants to move its email “into the cloud” may end up assessing Office 365 as an alternative solution to running Microsoft Exchange on-premises. Following this assessment, the organization may:

1. Determine that Office 365 is insufficient for its needs today
2. Opt to move Exchange into VMs on an IaaS provider instead
3. Plan to reassess Office 365 again in a few years

This method of using multiple iterations of workload placement analysis and migration is depicted in Figure 3.
Figure 3. Long-Term Multistep Cloud Migration Strategy

Source: Gartner (October 2018)
As organizations iteratively reassess workload placement over time, they need to take multiple performance and risk factors into consideration during each analysis cycle. In “Moving Enterprise Workloads to Public Cloud, Hosting, or Colocation — How to Decide and Execute,” Gartner provides a framework for performing workload risk analysis. The report also contains detailed technical and nontechnical criteria that organizations should apply to each layer of the cloud computing market (as well as hosting and colocation) when evaluating alternate execution venues.

**Plan for Cloud Adoption Maturity**

Cloud projects are complex, and it takes time for the organization to develop the skill sets necessary across all of the functional areas impacted. Organizations must also continuously improve processes to progress through their path to maturity. Therefore, organizations must adopt a structured approach to continuously advance their use of cloud services. In “Solution Path for Implementing a Public Cloud Adoption Maturity Plan,” Gartner provides a framework for maturing cloud initiatives (see Figure 4). This maturity plan provides guidance across five workstreams:

- Organizational
- Governance
- Architecture
- Provider brokerage
- Cloud operations

Each workstream is defined on the basis of four cloud stages:

1. Elementary Cloud
2. Specialized Cloud
3. Multicloud
4. Brokered Multicloud
Figure 4. Solution Path for Implementing a Public Cloud Adoption Maturity Plan

Source: Gartner (October 2018)
Organizations may vary in completeness of tasks by workstream, meaning one workstream may be in the Elementary Cloud phase while another one may be in the Multicloud phase. Organizations should determine their desired cloud maturity end state, develop plans and align investment strategies to their unique cloud goals.

Organizations often wonder, “How far along are we in adopting cloud in comparison to other companies?” This Solution Path framework includes a tool for architects to rate their organization by workstream. The tool computes a maturity index so that organizations can calculate their current maturity. Organizations can set a quantifiable goal, and then use the guidance in the Solution Path to develop a plan and identify the investments needed to meet that goal.

Establish Multicloud Governance and Management Processes

In 2019, more public cloud initiatives will reach the production stage, and central IT will be tasked with taking control of new heterogeneous workloads, deployed in multiple providers and at different layers of the cloud. These workloads will be sourced from multiple IaaS and PaaS providers and potentially dozens of SaaS solutions. At the same time, organizations will still have compliance, governance and security requirements that will have to be met, regardless of the sourcing model or provider used. As a result, the development of multicloud governance and management processes will be critical to success.

The complexity of cloud governance and management increases significantly when more than one cloud is in use. Even if the cloud industry tends to advocate cloud services as commodities, Gartner believes that they’re far from that definition. Even through the course of 2019, the major IaaS, PaaS and SaaS providers will offer little standardization among their offerings, providing instead very different feature sets, consumption workflows, interfaces and API definitions.

Multicloud requirements will directly impact the choice of cloud management and governance strategies. SaaS cloud providers’ management tools will continue to focus only on their own solutions. IaaS and PaaS cloud providers’ native tools will minimally extend to supporting other provider services.

Governance of cloud computing is challenging even with a single cloud provider involved, and becomes exponentially more challenging as organizations move toward multicloud. The cloud providers offer on-demand, self-service resources with endless capacity, making it difficult for organizations to gain visibility into, and manage, what is being consumed. As a result, organizations must govern not only consumption of cloud services by provider, but also consumption across cloud providers (see Figure 5). Without visibility into consumption, it is impossible to govern and manage your environment.
Establishing governance enables the organization to consume cloud services while ensuring that IT maintains compliance and operational excellence for the environment. By defining and establishing policies (whether automated or not), IT enables the business to use cloud computing wherever possible. This is a paradigm shift from the past, when organizations would try to limit or control the use of cloud services. Instead, IT should be promoting public cloud computing and making it the preferred deployment model.

Steps for achieving public cloud governance include the following:

1. Identify your governance team, and document your goals.

2. Define the high-level governance principles and policies that can be programmatically enforced (aka the “guardrails”). These types of programmatic controls can come in many different forms, such as identity and access management (IAM) systems, role-based access controls, resource policy controls and financial auditing controls.

3. Develop audit processes for compliance and performance, and continuously evolve your governance processes based on an established feedback loop.
For more information on achieving public cloud governance, see “Solution Path for Enabling Governance of Public Cloud Computing.”

When defining guardrails for public cloud governance, technical professionals must focus first on controlling who has access. Access policies must describe entitlements to cloud services. For example:

- A policy can allow a certain user to access the Amazon Elastic Compute Cloud (EC2) service from AWS, but only in the U.S. East (Northern Virginia) region.
- Another policy may allow the same user to access Workday ERP for its HR functions, as an employee.

To manage access policies in a multicloud scenario, a fundamental step is to share identities between cloud providers through a federated identity architecture. With such an architecture in place, policies can be enforced by leveraging the native cloud provider’s tooling. Most cloud providers allow for programmatic policy configuration. Therefore, policy configuration should be automated as much as possible as part of the access enablement. More information on automated access enablement and policy configuration can be found in “Identity Next: Rethinking Identity Governance and Administration” and “5 Approaches for Public Cloud Self-Service Enablement and Governance.”

Once access to cloud services has been granted, technical professionals must achieve governance by auditing workloads and user behavior, identifying policy violations, and automating the course of action. Organizations must maintain visibility over their cloud deployments and audit configurations, and the activities occurring with them. Policy definitions must span availability monitoring, performance monitoring, change management, cost management, security and compliance. In multicloud scenarios, it will be common to use a mix of tools to enforce guardrails, as Gartner has not yet seen the emergence of tools for end-to-end multicloud governance.

For more information on these topics, see the following research:

- Multicloud cost management and governance — “How to Manage Public Cloud Costs on Amazon Web Services and Microsoft Azure”
- Public cloud security monitoring and compliance — “Implementing Cloud Security Monitoring and Compliance Using Amazon Web Services”
- Discussion of capabilities and policy examples for public cloud governance — “Implementing Governance for Public Cloud IaaS and PaaS”

**Develop a Multicloud Management Tooling Strategy**

The growing acceptance of public cloud and the increased usage of multicloud are driving the need for consistent cross-platform management. Rapid adoption of cloud services is introducing a new set of management challenges for technical professionals responsible for managing IT systems and services.
Traditional on-premises management tools provide a familiar administrator experience, but usually offer limited public cloud management functionality. Cloud providers are constantly releasing new native tools and services. New independent software vendors (ISVs) are also providing cloud management tools and platforms that help manage multiple cloud environments consistently.

However, the meaning of the term “cloud management platform” (CMP) has dramatically evolved over the past decade. Consequently, the precise definition of this term is often unclear in discussions of management strategy. One vendor using this term may mean something completely different than another. Selecting the right management approach for cloud services is therefore a complex task.

In this context, organizations must develop a cloud management tooling strategy by selecting and adopting the most appropriate cloud management solutions. Creating a coherent cloud management tooling strategy requires a well-defined, systematic approach to solidify requirements, and to match tools to these requirements. The aim is to minimize the number of tools needed while fulfilling all management needs.

As described in “A Guidance Framework for Selecting Cloud Management Platforms and Tools,” organizations must start by defining their management requirements. These requirements can be:

- **Cross-platform**: Required functionality must be delivered across multiple cloud platforms with a consistent interface.

- **Platform-specific**: Required functionality is specific to one cloud platform, and it must allow for access to all the granular controls available in that specific platform.

Only after defining and prioritizing their management requirements should organizations conduct the assessment, selection and comparison of cloud management tools. “Evaluation Criteria for Cloud Management Platforms and Tools” provides technical professionals with 215 criteria to produce a comprehensive assessment of tools that manage private, hybrid and public cloud IaaS and PaaS. Organizations can use the evaluation criteria to assess tools across the eight categories (in blue) and four cross-functional attributes (in orange) depicted in Figure 6.
Figure 6. Evaluation Criteria Categories and Attributes: The Cloud Management Wheel

Source: Gartner (October 2018)
Gartner recommends adopting a combination of these types of solutions, based on the required degrees of cross-platform consistency and platform-specific functionality. In all cases, organizations should prioritize the use of the cloud platform’s native toolset, augmenting that where needed with third-party CMPs, cloud management point tools, do-it-yourself (DIY) solutions and outsourcing. For more information, see “A Guidance Framework for Selecting Cloud Management Platforms and Tools.”

**Evaluate Multicloud SaaS Integration Requirements**

As organizations seek to enable digital business, they continue to grow their SaaS portfolios in areas such as CRM and content and collaboration. With portfolios reaching an all-time high in terms of size, the need to integrate and orchestrate across disparate SaaS applications is mounting. Having an integration strategy in place is critical to addressing this need.

SaaS providers are enhancing their solutions to be more competitive and to help address the need to integrate with other SaaS applications. One way they are doing this is by providing application and integration capabilities or platforms, thus blurring the lines between SaaS and PaaS. These capabilities can range from offering support for professional developers or integrators only, to supporting ad hoc and citizen developers and/or integrators. While this is happening, concurrent technology convergence and innovation continue to reshape SaaS markets, causing new best-of-breed solutions. This means that organizations will need to continuously evaluate when they should use integration and development features provided by a SaaS provider, and when they should use an IaaS or PaaS technology.

By continuously evaluating requirements, organizations can present the optimal choices to those responsible for extending and integrating SaaS solutions. Many SaaS providers that offer integration and application development capabilities or platforms do not charge an additional fee to their SaaS consumers. Thus, organizations may get a better return from a SaaS offering by shifting some applications and integrations to it, instead of using a PaaS technology (such as integration PaaS or application PaaS) that might have a cost per solution. However, organizations need to continuously evaluate their requirements and compare them with the capabilities of a SaaS offering to maintain the optimal mix of SaaS-provided capabilities and PaaS technology.

For more information on how to integrate SaaS applications with cloud-hosted and on-premises applications, see “How to Integrate Cloud-Hosted, SaaS and On-Premises Applications.”

**Optimizing Workloads for IaaS, PaaS and SaaS Will Be an Increasingly Critical Priority**

Historically, Gartner has rated cloud providers based on their capabilities at each cloud tier — IaaS, PaaS and SaaS. These traditional market segments are blurring, however, as the providers move into different tiers. Each provider is approaching this evolution differently.

Organizations must think beyond the capabilities at a single tier and, in the future, seek providers that offer multiple cloud services across cloud tiers (IaaS, PaaS and SaaS). Today, organizations must architect for networking, identity and security as they connect to cloud provider services. Because there is no standardization, this work must be repeated for each cloud provider.
As the cloud market continues to evolve and the providers mature in service capabilities, organizations will benefit from choosing a cloud provider that offers services across cloud tiers, streamlining the initial setup. A cloud provider that offers a common portal of services across cloud tiers will provide an organization with a common identity, common networking and common security services, as well as a single bill. The fact that providers offer services across cloud tiers doesn’t mean that organizations will use only one strategic provider, however. Rather, organizations can utilize whatever type of cloud service makes sense based on the application requirements. Organizations will still continue to deploy multicloud strategies.

Planning Considerations

In the future, organizations will stop thinking about cloud providers and their offerings in terms of tiers, such as IaaS, PaaS or SaaS. In 2019, organizations should begin prioritizing providers that have, or are developing, portfolios of cloud services that are as comprehensive as possible. To manage through this market transition, IT must:

- Expect and plan for provider lock-in, especially at the SaaS tier
- Embrace both IaaS and PaaS
- Prioritize providers with integrated IaaS and PaaS
- Design for portability
- Develop automation strategies

Expect and Plan for Provider Lock-In, Especially at the SaaS Tier

Lock-in exists at all cloud tiers, but increases as you move from IaaS to PaaS, and increases again from PaaS to SaaS. The more you move up the cloud stack, the less control and choice you have over the technologies being used. You also become further locked in to that cloud provider. If portability is a key priority, Gartner recommends remaining at the bottom tier with IaaS. However, in that case, you minimize the innovation the cloud provider offers and the savings you ultimately could achieve through movement to the public cloud. Plan to embrace the innovation the cloud providers offer, and expect a level of lock-in as an inevitable result.

Most organizations move upstack quickly and leverage more of the provider’s native services, because such services deliver additional innovation and allow organizations to differentiate. While you should expect to maximize the cloud services you consume by a provider, do so cautiously. Many applications, especially complex ones, benefit from access to a mix of raw infrastructure resources, application PaaS (aPaaS) functionality, management capabilities, application infrastructure services and higher-level solutions.

Other applications will be completely replaced by SaaS offerings, commonly driven by the application vendors. This replacement will occur because cloud is a less expensive alternative and may be the only deployment model in the future. The more organizations leverage SaaS solutions and build integrations into the existing environment, the more lock-in will occur. Lock-in is inevitable.
and, arguably, has always been part of data center strategies. Plan accordingly by mitigating the risk through multicloud strategies, establishing provider exit strategies and creating portable cloud architectures. See “Designing a Public Cloud Exit Strategy.”

**Embrace Both IaaS and PaaS**

Organizations have options when migrating applications to the cloud, including:

- Rearchitecting an application for PaaS
- Rehosting an application on IaaS
- Using a combination of strategies that leverage both IaaS and PaaS, for larger, more complex applications

There is a spectrum of computing options in the cloud that should be used appropriately based on the goals of migrating the application (and its dependencies) to the cloud. IaaS and PaaS deliver unique benefits. One is not inherently better than the other, so it is important to understand the discrete benefits of these capabilities.

Many organizations are developing cloud strategies to execute data center consolidation initiatives. While cloud can be a viable method to rehost applications, colocation facilities and hosting providers have also been enabling this task for decades. It is important to first ask if an application truly needs to leverage the characteristics of cloud — on demand, scalable and elastic, metered for use, and pay as you go. The answer to this question may be that you need all of those characteristics or only a subset. In either case, your choice to migrate the application to the public cloud is first determined by identifying the needs of the application. It is important to align the business expectations accordingly with the target cloud delivery model.

Both IaaS and PaaS allow users to spin resources up and down quickly, scale into new regions, and enable an operating expenditure (opex) model. However, of the two options, IaaS offers users more control and flexibility to migrate applications to cloud services with the fewest architectural changes possible. Typically, once organizations start using IaaS services and declare some level of success, they quickly move upstack and begin using additional services from the provider, such as identity or networking services. These aren’t considered full PaaS capabilities, but they are beyond the capabilities of pure IaaS.

Organizations must also consider what is possible from an application architecture perspective. Specifically, consider commercial off-the-shelf (COTS) applications. You can’t rewrite COTS applications, because you don’t own the source code. If there is no SaaS alternative and you are migrating the application out of your traditional data center environment, rehosting that application in IaaS may be the best or only alternative. The vendor may offer a SaaS version of that application in the future.

Conversely, custom-developed applications may be rehosted or refactored. Or, you may opt to rearchitect or rebuild the application to be truly cloud-native. Whether choosing to rehost to IaaS, rearchitect for PaaS or a combination, you will need to embrace different cloud delivery models to execute these strategies. As you continue to move to more complex, larger applications that are
custom-developed and dependent on COTS applications, this need increases even more (see Figure 7). There are several trade-offs and decisions that must be accounted for in this scenario.

**Figure 7. Application Migration Options**

<table>
<thead>
<tr>
<th>Rehost to Containers or VMs</th>
<th>Refactor</th>
<th>Rearchitect</th>
<th>Rebuild</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Cost savings and density</td>
<td>- Add new API, and use API management</td>
<td>- Increased scalability and elasticity</td>
<td>- Cultural change</td>
</tr>
<tr>
<td>- Consistent deployment contract</td>
<td>- Open up new interface for channel</td>
<td>- Share-nothing architecture</td>
<td>- Independent teams</td>
</tr>
<tr>
<td>- Closer proximity to other apps</td>
<td>- Use additional backing services</td>
<td>- Resiliency patterns implemented</td>
<td>- DevOps initiative</td>
</tr>
<tr>
<td>- Container orchestration required</td>
<td>- Implement load balancing</td>
<td>- CI/CD pipeline</td>
<td>- Commitment to automation, autonomy and immutable infrastructure for full cloud-native capabilities</td>
</tr>
</tbody>
</table>

As organizations let go of the responsibility for managing their infrastructure and begin rearchitecting their applications, many naturally gravitate toward application deployment in PaaS environments. By embracing PaaS, organizations delegate much of the control they have in the data center today to the cloud service provider. This represents a significant cultural shift in traditional IT organizations that have established many best practices for managing, hardening, monitoring, patching and securing servers, operating systems, middleware and databases. Relinquishing control of these traditional practices requires a shift in roles and skill sets. To better understand cloud-native architecture and principles, see “A Guidance Framework for Architecting Highly Available Cloud-Native Applications.”

As organizations refactor, rebuild and rearchitect their applications for cloud environments, they are also embracing the trend of building the more granular, independently deployable application
services known as “microservices.” The goal of microservices architecture (MSA) is to improve development agility with deployment flexibility, scalability and portability of application features. MSA is more costly and complex, however, than delivering a well-structured, nondistributed application. Achieving the benefits of MSA requires a high degree of development and operational maturity and automation.

PaaS platforms achieve resilience against failure by utilizing the abundance of resources in a cloud environment. Your traditional applications must also change to address failure through architecture and design — and, therefore, take advantage of the abundance of resources in PaaS — by employing cloud-native principles. Gartner describes these architecture principles using the mnemonic LIFESPAR (see Figure 8).

Figure 8. LIFESPAR Defined

LIFESPAR stands for:

- **Latency-aware**: Applications remain operational despite variable and extended latency for services accessed across public networks, and between cloud provider data centers.
- **Instrumented**: Sufficient telemetry data is available from applications to determine health and other operational and performance characteristics.
- **Failure-aware**: Applications are resilient to occasional or extended failures of underlying infrastructure components or dependent services.
- **Event-driven**: Programs are structured as a set of handlers, waiting for events and responding in a choreographed way, rather than with sequential, determined and synchronous orchestrations.

- **Secure**: The application protects the information and systems, guarding against data loss or SLA violations caused by malicious or accidental events.

- **Parallelizable**: Data processing can be scaled out to multiple simultaneous or redundant instances of system components as required by an SLA.

- **Automated**: Applications are packaged, deployed and executed without manual steps or complex dependencies.

- **Resource-consumption-aware**: Applications can be adapted to different algorithms, data structures and system architectures in response to resource cost changes.

### Prioritize Providers With Integrated IaaS and PaaS

Integrated IaaS and PaaS (aka integrated IaaS+PaaS, or integrated cloud platform services) allows customers to mix IaaS and PaaS elements seamlessly. The hyperscale cloud providers — AWS, Microsoft Azure and Google Cloud Platform — are providers whose services exist on a continuum between IaaS and PaaS. These IaaS+PaaS providers can deliver a single portal, common identity, common networking and streamlined billing across the service tiers.

In addition to pure IaaS and pure PaaS, there are capabilities that exist along the spectrum between the two. These capabilities have a combination of IaaS and PaaS traits, as shown in Figure 9.
Integrated IaaS and PaaS capabilities fall into four broad categories:

- **Runtime environments**: These environments are where the customer’s application code executes. A runtime environment can be either of the following:
  - An IaaS compute resource (a VM, OS container or bare-metal server)
  - An aPaaS runtime construct (which could be based on either instances or more abstracted fabrics)

- **Software infrastructure**: Middleware, databases, content management systems and other software infrastructure can be delivered in multiple models.
Management functions: Traditional IT operations management capabilities, as well as DevOps-oriented capabilities, can be delivered in multiple models. Monitoring, logging, backup, orchestration, continuous configuration automation (CCA) and CI/CD pipelines are part of this general category.

Domain-specific solutions: Higher-order solutions, such as those for data warehousing and machine learning, can be delivered in multiple models.

When evaluating and selecting a provider for strategic adoption, cloud architects should strongly favor an IaaS+PaaS provider, even if the organization does not intend to immediately use the PaaS capabilities. Moving upstack allows the organization to become more efficient and agile, and to realize higher levels of cost optimization. However, cloud architects should be aware of the trade-offs between ease of integration and operations, and greater lock-in. Selecting a provider that offers services at both tiers enables maximum choice and flexibility in deployment approaches.

Design for Portability

The initial benefits of cloud computing are typically demonstrated by a small team in an organization, which chooses its favorite cloud provider and delivers an application quickly to take advantage of the cloud’s elasticity, shared infrastructure and global reach. This can be an enchanting moment for executive teams that are witnessing these benefits firsthand. The challenge, however, is that this application scenario is not designed to move between providers, and is not portable without substantial rearchitecting or refactoring. This isn’t a problem if the organization decided not to prioritize portability, and deliberately chose to make the application nonportable. It is a problem, however, if the lock-in was unintended.

Unanticipated vendor lock-in is particularly critical because the very nature of the public cloud computing model makes the consumers of applications more vulnerable to dependencies. Every piece of your application or service is dependent on the platform components underneath it, and in the public cloud, these components may be entirely portable, entirely proprietary or somewhere in between. Exacerbating this challenge is the fact that cloud providers may be at risk of leaving the marketplace unexpectedly. Thus, it is important to assess your portability posture and to balance your organization’s use of the cloud provider’s built-in features with the inherent trade-off of vendor lock-in that comes with this decision.

Solution architects must make a conscious decision about whether or not to prioritize portability during the design phase of an application. When portability is prioritized, they must adhere to architectural disciplines that promote portability. This will enable applications to move between providers without substantial rearchitecting or refactoring.

Where you determine portability to be an important priority, you should design cloud applications to be contextually independent. As an end state, contextual independence is difficult — and sometimes impossible — to achieve. The three characteristics of contextual independence are:

- Few dependencies: Contextually independent systems can be deployed almost anywhere because they don’t depend on much else to function. They are relatively self-contained.
- **Well-defined interfaces:** The means of interfacing with contextually independent systems are very well-defined and easily understood.

- **Easily satisfied dependencies:** The few dependencies that the contextually independent systems have are also easy to satisfy.

As Table 1 shows, contextual independence becomes more possible as you move down the cloud stack, from SaaS (with no characteristics) to IaaS (with all three). Hence, portability is easiest to achieve at the IaaS tier.

<table>
<thead>
<tr>
<th></th>
<th>Few Dependencies</th>
<th>Well-Defined Interfaces</th>
<th>Easily Satisfied Dependencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>SaaS</td>
<td>✘</td>
<td>✘</td>
<td>✘</td>
</tr>
<tr>
<td>PaaS</td>
<td>✘</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>IaaS</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
</tbody>
</table>

Source: Gartner (September 2018)

To assess the portability priority, consider the nature of each application in terms of how it will be used and how long it is likely to endure. This assessment can be aided by considering the two modes of a bimodal IT approach:

- **Mode 1** focuses on delivering reliability. This mode employs strictly governed practices to shepherd sustaining technologies and process innovations that must remain stable over long periods of time.

- **Mode 2** focuses on delivering agility. This mode emphasizes results over processes, experimentation over stability, and disruptive innovation over the status quo.

If your application is more suited to the Mode 1 delivery model, portability should be front and center in your planning, even if you choose to implement portions of the application using agile development methodologies. Portability priorities are depicted in Figure 10, and summarized in the bullets that follow.
Portability is a higher priority when applications have a systematic or highly strategic nature, require a high degree of development effort, and/or will endure for an extended period. For these applications, the organization is taking on a huge risk if it doesn’t make explicit choices about portability in its cloud application strategy.

Portability is a lower priority when applications are more opportunistic, require relatively minimal development time and effort, and/or will likely be short-lived. In these cases, “starting over” will likely be a less expensive and better option. Low-code-oriented applications fall into this category (see “Architecting Low-Code Cloud Applications With High-Productivity aPaaS”).

Containerizing applications and services can increase portability, as the build, packaging and deployment mechanisms have a well-defined, standard interface regardless of the cloud provider you use. Portability is facilitated by the adoption of application container images (e.g., Docker/Open Container Initiative images) as the unit of deployment. Container IaaS offerings provide a high degree of portability when you are managing applications and services at enterprise scale, because the container is the common deployment currency across all of the services. Examples of container IaaS offerings include Amazon Elastic Container Service for Kubernetes (EKS), Azure Kubernetes Service (AKS) and Google Kubernetes Engine (GKE). Application components and backing services that cannot be packaged with your application or service become the limiting factor, thus increasing the need to rigorously manage external dependencies.
Develop Automation Strategies

Automation is the cornerstone of modern, agile IT operations across data centers and the public cloud. It is central to all the changes that are happening to enterprise IT. Public cloud IaaS is a key enabling technology for infrastructure automation. For many traditional IT organizations, automation is one of the primary benefits they gain by moving to the public cloud. Automating public cloud IaaS offers two advantages:

- **Software-defined infrastructure**: The public cloud infrastructure and platform are software-defined by default. Services are available and accessible via API.
- **Native tooling**: Many public cloud IaaS providers also provide native automation tools for use with their infrastructure.

The workflow for automating a compute instance in the public cloud is not materially different from the workflow for automating a VM on private infrastructure. However, because of the built-in advantages of modern cloud infrastructure, the actual work involved may be much less. When you are automating on-premises servers, the majority of your time and labor is consumed in modernizing the underlying infrastructure and rationalizing the workflows to make full life cycle server automation possible. By contrast, in public cloud IaaS, the difficult problems associated with automation are largely solved.

Automation Tools

The tools used to automate public cloud IaaS may be entirely different — and, in many cases, much better. As Gartner’s “How to Automate Server Provisioning and Configuration Management” notes, any task in a server automation workflow can be broken down into three constituent parts:

- **Trigger**: This is the catalyst that starts the workflow.
- **Specification**: This is a programmatic description of the desired state of the system. Specification management tools must be able to bring the system into compliance with the state described by the specification, and keep it there.
- **Behavior**: This is the actual work that needs to be done to bring the system into the desired state. Behavior management tools should be able to execute arbitrary code on the endpoints they manage. Although modern configuration management tools prefer to operate according to specifications, not scripts, some scripting will always be necessary.

Major public cloud IaaS providers have built native tools for each of these constituent parts. Table 2 lists these tools, alongside some third-party equivalents that could also be used to instrument public cloud IaaS automation.
### Table 2. Native Automation Tools for Public Cloud IaaS

<table>
<thead>
<tr>
<th>Goal</th>
<th>AWS</th>
<th>Azure</th>
<th>Google</th>
<th>Third Party</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trigger (Autoscaling)</td>
<td>EC2 Auto Scaling</td>
<td>Azure Autoscale</td>
<td>Managed instance groups</td>
<td>Native “adaptive response” systems</td>
</tr>
<tr>
<td>Trigger (Autoremediation)</td>
<td>Systems Manager Automation</td>
<td>Azure Automation webhooks</td>
<td>Cloud Pub/Sub CCA tools</td>
<td>Event-based automation</td>
</tr>
<tr>
<td>Specification (Provisioning)</td>
<td>CloudFormation</td>
<td>Azure Resource Manager</td>
<td>Cloud Deployment Manager</td>
<td>Terraform</td>
</tr>
<tr>
<td>Specification (Configuration Management)</td>
<td>Systems Manager State Manager</td>
<td>Azure Automation DSC</td>
<td>Cloud Deployment Manager</td>
<td>CCA tools (Ansible, Chef, Puppet and others)</td>
</tr>
<tr>
<td></td>
<td>Systems Manager Run Command</td>
<td>Run Command</td>
<td>gcloud CLI</td>
<td>CCA tools</td>
</tr>
<tr>
<td>Behavior Management</td>
<td></td>
<td>gcloud CLI</td>
<td>CCA tools</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Script engines (BMC TrueSight Server Automation, Microsoft SCCM and others)</td>
<td></td>
</tr>
</tbody>
</table>

CLI = command line interface; DSC = Desired State Configuration; SCCM = System Center Configuration Manager.

This table is a representative sample of the tools available, not an exhaustive list.

Source: Gartner (October 2018)

There are many critical differences between the tools competing in each category. These differences must be evaluated carefully to ensure a tool meets the unique needs of the use case and the IT organization.

Tool selection grows more complicated in a hybrid or multicloud architecture. A cloud provider’s native tooling may have the shortest onramp for new users and the tightest integration with the cloud infrastructure. It will also entail little to no maintenance work for the end user. However, it is useful only for infrastructure in that cloud provider. Third-party tools, by contrast, have the potential to create cross-cloud workflows for multiple providers. This flexibility comes at the cost of increased complexity for the end user, who must build and maintain the third-party tool. Third-party tools are also likely to provide only the lowest common denominator of functionality among the cloud targets.
If there are features unique to one public cloud IaaS provider, they cannot be included in a unified workflow that is designed to be portable to many providers.

**Immutable Infrastructure**

Operating in the public cloud also requires technical professionals to change their mindset on how they manage their environment. The cloud is all about constant change and optimization. While traditional data center best practices focus on optimizing assets for longevity — often by updating and troubleshooting the same server or VM — efficient use of cloud resources requires a more pragmatic, utilitarian approach to the resource life cycle.

When your automation capabilities have advanced to the point that it is easier to destroy and recreate cloud resources than to change them, your infrastructure can be considered immutable. Immutable infrastructure is an architectural pattern in which the system and application infrastructure, once instantiated, is never updated in-place. Instead, when changes are required, the infrastructure is simply replaced.

Although counterintuitive, immutable infrastructure can simplify change management. In the server automation case, three common catalysts for change are:

- Operating system patch management
- Middleware or platform software updates
- Application releases

These three processes often include very different orchestration tools and workflows, each of which needs to be validated and maintained. In even the most rigorously controlled environments, managing drift is challenging. When organizations adopt immutable infrastructure, these three processes can be reduced to a single orchestrated workflow — the automated validation of the intended change, followed by the replacement of the affected compute instances.

Use of containers as a packaging and deployment mechanism naturally follows an immutable paradigm, but containerization is not a requirement. For more on immutable infrastructure and its benefits, as well as implementation guidance, see “To Automate Your Automation, Apply Agile Practices and DevOps Tools to Infrastructure and Operations” and “How to Automate Server Provisioning and Configuration Management.”

**Hybrid IT Strategies Will Continue to Mature Across Organizations**

“Cloud first” does not mean that organizations should take everything in their data centers and migrate it to public clouds. Data centers will live on in most companies for the foreseeable future, so organizations must augment their processes and tooling to integrate their data centers with the public cloud. 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, the term “hybrid” is often used inconsistently. Hybrid architectures will 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.

Planning Considerations

In 2019, organizations must plan for a hybrid IT environment. Most organizations have already accepted that hybrid will become their end state. The public cloud should be woven into the organization’s IT data center modernization strategy and treated as an extension of its data center resources. This will require the evaluation of new architectural approaches and investments. To be successful, IT organizations must:

- Integrate traditional data centers and public cloud platforms
- Rethink your network for hybrid and multicloud
- Extend your strategy for data compliance into the public cloud
- Extend your data availability strategy into the public cloud
- Extend your security control practices into the public cloud

Integrate Traditional Data Centers and Public Cloud Platforms

Most Gartner clients are facing the challenge of adopting public cloud services while maintaining existing IT responsibilities for on-premises infrastructure and private clouds. IT departments must become brokers of IT-based services, blending traditional services, public cloud services and private cloud services. Gartner calls this evolution “hybrid IT.”

As shown in Figure 11, the challenge for I&O is to simplify access to the multiple environments and to maintain visibility across them, without impacting the agility of lines of business and developers. These users have become accustomed to self-service and almost instant access to cloud resources, but organizations also need to apply consistent policy, minimize cost and monitor activity across all the services.
For each environment in which services run, you can have visibility and control into multiple layers: the hardware/utilities layer, the virtualization layer and the application/data layer. Integration can happen at each of these layers for each environment. In addition, a management layer sits over all the other three layers. Thus, there are four possible levels at which integration can occur:

- Infrastructure (below the cloud/virtualization layer)
- Orchestration (the cloud/virtualization layer)
- Applications and data (above the cloud/virtualization layer)
- Management (operation, governance and monitoring of all silos)

The list of required hybrid capabilities can now be ordered and sorted into types based on each of these four levels of integration (see Figure 12).
Understanding the four different types of hybrid integration leads to four possible hybrid architectures:

- **Hybrid infrastructure**, where the connections occur between silos purely at the hardware/utility layer
- **Hybrid orchestration**, where the integration occurs at the virtualization, container or cluster orchestration layer across silos
- **Hybrid applications/data**, where the integration happens purely between application modules and data sources via APIs
- **Hybrid IT management**, where the integration is handled by a management layer providing operation, monitoring and brokering across the silos

For more information, see “Utilizing Hybrid Architectures for Cloud Computing.”

By adopting this terminology, organizations can discuss and plan their journey to hybrid IT in far greater detail and with more granularity than simply saying “We will implement hybrid cloud.” Understanding the possible hybrid architectures, as well as mapping the implementation of each over time, allows organizations to plan for specific technology and organizational requirements effectively. Key actions to take include the following:
- Implement an application and service placement decision framework to help select the best location to host applications and data.
- Create a map of your journey over time across the hybrid architectures of infrastructure, orchestration, applications/data and management integration.
- Identify key inflection points on the journey where significant changes to skills requirements, organizational structure, procurement, governance and toolsets will occur.

Begin transforming your organization now. Invest in the skills and technologies to integrate public cloud services with your traditional offerings.

**Rethink Your Network for Hybrid and Multicloud**

In the precloud era, enterprise wide-area networks (WANs) were optimized for workloads running in the data center. Internet access was often centralized, and internet-bound traffic needed to traverse the enterprise WAN and go all the way to the data center to reach the internet. Multiprotocol Label Switching (MPLS) was king. When critical workloads started moving to the cloud, the latency created by this traffic backhauling became unacceptable. The enterprise WAN needed to be readjusted.

Gartner recommends that technical professionals take the following critical steps to cloud-enable their enterprise WANs (see Figure 13):

1. **Transform your transport by using the right combination of internet, MPLS and cloud interconnects.** Organizations need to decide whether to use the internet or MPLS to access their cloud resources. The state of their current network often drives that decision. An organization with centralized internet access will often extend its cloud resources to its MPLS network by leveraging a cloud interconnect such as AWS Direct Connect, Azure ExpressRoute or Google Cloud Interconnect. There are multiple ways to deliver interconnects, including using a colocation hub such as Equinix, a network service provider (NSP) offering such as AT&T NetBond or a software-defined interconnect such as Megaport. Most Gartner customers have a hybrid MPLS architecture, where sites have a mix of MPLS and internet links. These sites will use a mix of direct internet access and MPLS connectivity.

2. **Rearchitect your WAN access, and adopt software-defined WAN (SD-WAN).** SD-WAN allows for greater control, service availability and agility at the enterprise WAN edge. Sites subscribing to hybrid MPLS architecture are great candidates for SD-WAN. They can use SD-WAN centralized policies to route traffic between direct internet access and MPLS in concert with interconnect. The policies can be based on security, performance or availability rules. An increasing number of organizations leverage the availability controls of SD-WAN to replace a hybrid MPLS architecture by using two internet links from different internet service providers. This approach helps control costs while guaranteeing performance and availability.

3. **Become proficient in your provider's virtual network constructs and network services.** Organizations should evaluate whether their cloud provider's native network constructs meet their requirements before looking at third-party constructs such as routers and load balancers. Then, they should implement third-party tools to fill gaps such as deep packet inspections or
advanced routing. The various data transfer costs can greatly affect the expense of networking in the cloud. Organizations should make the costs of transferring data into and out of their virtual private cloud (VPC) and virtual network (VNet) a design parameter. The costs can quickly escalate if left unmanaged.

4. **Look for network solutions that provide consistent policies across multiple clouds and data centers.** As enterprise adopt multicloud and hybrid approaches, creating network policies across multiple clouds and on-premises becomes unwieldy. Most SDN overlay solution and data center fabric vendors now extend their offerings into the cloud. Some offerings, such as VMware NSX, require each VM workload to install a virtual switch. With these solutions, most of the features that exist on-premises are extendable to the cloud. Other solutions, like Cisco ACI, leverage the cloud platform’s API. These solutions are easier to install, but only the features realizable using the cloud provider API can be extended. Gartner foresees a lot of activity in this area. Organizations should keep a close eye on this market, including emerging cloud-native solutions.
Extend Your Strategy for Data Compliance Into the Public Cloud

Now that the 25 May 2018 compliance deadline has passed, the hype and attention around EU General Data Protection Regulation (GDPR) has noticeably settled down. The take-away from the whole GDPR craze is that data residency and compliance issues continue to cause increasing questions about the regulatory impact of storing data in public clouds. Technical professionals tasked with cloud security will need to ensure that they understand and comply with all relevant regulations in all cloud services that they consume.

Leading cloud providers continue to assist clients in meeting specific compliance requirements by providing the following artifacts and features:
**Shared assessments and compliance reports:** Cloud providers share certifications and audit reports with clients. Shared assessments and compliance reports are really intended to assist the organization in meeting specific compliance requirements, and don’t mean that all cloud resources leveraged by an organization will automatically meet compliance requirements. The scope for certification covers only the portions of the workload above the cloud provider’s handoff point. Clients can leverage the benefit of being “compliant by inclusion” by incorporating the cloud provider’s published attestations into their own — thus limiting the scope. Figure 14 illustrates the security handoff points in the IaaS, PaaS and SaaS cloud models. IaaS offers the most control, with the commensurate security responsibility left to customers. SaaS offers the least control, with the cloud provider taking on most of the security responsibility. Items in orange boxes are below the handoff point and covered by the cloud provider’s compliance reports and certifications. Items in blue boxes must still go through client-facilitated audits and certification.

Figure 14. Shared Responsibility Model: The Division of Security Responsibility/Risk Alignment in the Cloud

---

**The Cloud’s Shared Responsibility Model**

<table>
<thead>
<tr>
<th>Traditional DC</th>
<th>Cloud</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data</td>
<td>IaaS</td>
</tr>
<tr>
<td>Application</td>
<td>PaaS</td>
</tr>
<tr>
<td>Runtime</td>
<td>SaaS</td>
</tr>
<tr>
<td>Middleware</td>
<td></td>
</tr>
<tr>
<td>OS</td>
<td></td>
</tr>
<tr>
<td>Virtual Network/Storage</td>
<td></td>
</tr>
<tr>
<td>Storage</td>
<td></td>
</tr>
<tr>
<td>Server</td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td></td>
</tr>
</tbody>
</table>

**IaaS**
- Data
- Application
- Workload Infrastructure
- Cloud Infrastructure
- Physical Infrastructure

**PaaS**
- Data
- Application
- Workload Infrastructure
- Cloud Infrastructure
- Physical Infrastructure

**SaaS**
- Data
- Application
- Workload Infrastructure
- Cloud Infrastructure
- Physical Infrastructure

**CSP Controls**

**Shared**

ID: 361515

CSP = cloud service provider; DC = data center

Source: Gartner (October 2018)
**Data residency controls:** Cloud providers often support clients in defining and enforcing data residency requirements. Organizations that need to align with these requirements will need to look for a cloud provider that allows the implementation of constraints on the geolocation of their data. The best data residency support goes beyond enabling the selection of regions in the cloud console or API. It also includes a set of easy-to-use controls that ensure data residency requirements are enforced at all times and cannot be circumvented.

**U.S. government cloud regions:** AWS and Azure have further developed specialized cloud offerings by building government-only cloud regions that are designed to meet government-specific security requirements. AWS GovCloud and Azure Government, respectively, host specific government systems that are too sensitive to be hosted within the generally available public cloud infrastructure. Examples of government systems that must be hosted in separate government cloud offerings include, but are not limited to, the following:

- Systems that need to meet the U.S. International Traffic in Arms Regulation (ITAR)
- Systems that need to meet Federal Risk and Authorization Management Program (FedRAMP) High certification requirements
- Systems that fall under the Criminal Justice Information Services Division (CJIS) security policy

**Security services and controls:** These are the controls that clients will require to fulfill the compliance obligations for the workloads and data under their control. Examples include:

- Data discovery and classification capabilities
- Encryption key management backed by Federal Information Processing Standards (FIPS)-evaluated technology

For translating compliance requirements into controls and orchestrating them across multiple cloud providers, cloud security posture management (CSPM) offerings are useful tools that continue to gain traction. Figure 15 illustrates the control coverage of CSPM, compared with cloud access security brokers (CASBs) and cloud workload protection platforms (CWPPs). For more detailed information about CSPM, see “Comparing the Use of CASB, CSPM and CWPP Solutions to Protect Public Cloud Services.”
If your organization has applications and data that are in scope of compliance frameworks, follow these best practices:

- **Leverage the benefit of being “compliant by inclusion.”** This is achieved by incorporating the cloud provider’s published attestations into your own. The scope of work for certification covers only the portions of the workload above the cloud provider’s handoff point. The certification process will focus on the requirements for which customers are responsible, such as encrypting data at rest.

- **Take full responsibility for workload and data security.** Configuring and managing workload and data security are entirely the responsibility of the subscriber. For example, applications and operating systems that are not properly secured, configured or maintained are a dominant pathway for attackers into workloads. The good news is that leading cloud providers offer a strong set of cloud-native controls, which also integrate with other cloud provider security services via APIs.

- **Prioritize cloud provider offerings and built-in controls when securing applications, workloads and data.** Security continues to be an area where Gartner observes more “lift and
The "shift" of traditional enterprise-grade controls from on-premises data centers into the cloud. This often makes security the showstopper that prevents enterprises from reaping the benefits of otherwise cloud-native applications. Gartner recommends that you prioritize cloud-native (i.e., cloud-provider-offered) security controls first, since these won’t mutate into showstoppers later on when you become more mature in cloud.

- **Select cloud providers that offer strong data residency controls that cannot be unintentionally circumvented.** Leading cloud providers allow organizations to define data residency constraints. However, these controls are not as intuitive and easy to configure as some of the other cloud-native security capabilities.

- **Evaluate CSPM tools to augment cloud-native visibility and control capabilities.** Although leading cloud providers offer strong controls to secure your workloads, your organization’s risk profile may warrant additional layers of security. Purpose-built CSPM tools focus on integrating with cloud subscriptions to provide enhanced security capabilities and to ease risk management in cloud environments. Administrators can use CSPM tools for:
  - **Assessment:** Review of the subscription and the deployed environment configuration against best practices and hardening guidance
  - **Monitoring:** Ingestion of log feeds from cloud subscription and deployed environment sources; alerting capabilities
  - **Compliance:** Assessment against defined standards, such as the Payment Card Industry Data Security Standard (PCI DSS), the Health Insurance Portability and Accountability Act (HIPAA) Security Rule or the National Institute of Standards and Technology (NIST) Cybersecurity Framework
  - **DevOps integration:** Exposure of service APIs to support deeper DevOps automation
  - **Incident response:** Alignment with monitoring and alerting, and capabilities to handle and mitigate incidents
  - **Risk identification:** Combination of monitoring, assessment and compliance information to provide a means to identify and prioritize risks with the cloud subscription
  - **Risk visualization:** Visualization of identified risks, including drill-down capabilities that provide lower-level information and details to support operations, triage and incident response

**Extend Your Data Availability Strategy Into the Public Cloud**

In 2017, the Amazon Simple Storage Service (S3) experienced an outage in the AWS U.S. East (Northern Virginia) region. This outage caused major disruptions to on-premises infrastructure and cloud-based services, resulting in service downtime, lost revenue and, often, lost data. From power outages causing canceled flights to human error resulting in inaccessible cloud storage, systems can fail no matter where they are located or who is managing them. Mission-critical service availability and protection of corporate data are essential no matter where services reside.
Protecting this data, often the most important asset that an organization owns, is a fiduciary responsibility that requires a comprehensive data availability strategy.

IT services are no longer delivered wholly on-premises. Hybrid configurations leveraging public cloud services are becoming more widespread. Although IaaS, PaaS and SaaS providers offer excellent data resiliency, most do not offer native backup or automated failover. These distributed-architecture deployment models are forcing IT managers and business continuity planners to rethink traditional backup and DR strategies. Existing data center solutions, as shown in Figure 16, offer robust, mature data protection, but must be re-evaluated to ensure support for all cloud-based components. Furthermore, heightened awareness of cyberattacks and ransomware threats is driving organizations to review their DR capability and DR readiness plans.

Figure 16. Extend the Data Center to the Cloud for Backup and DR

Extend the Data Center to the Cloud for Backup and DR

Primary Customer Data Center

<table>
<thead>
<tr>
<th>VMs or Physical Servers</th>
<th>Primary Storage</th>
<th>Database Replication</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMs or Physical Servers</td>
<td>Primary Storage</td>
<td>Backup Data Replication</td>
</tr>
</tbody>
</table>

DR Site (AWS Region)

<table>
<thead>
<tr>
<th>EC2 VMs</th>
<th>EBS Storage</th>
</tr>
</thead>
<tbody>
<tr>
<td>S3 Storage</td>
<td></td>
</tr>
</tbody>
</table>

AZ = Availability Zone; EBS = Amazon Elastic Block Store; EC2 = Amazon Elastic Compute Cloud; S3 = Amazon Simple Storage Service

Source: Gartner (October 2018)
Cloud providers are not responsible for user data or corporate content placed within their services. They are focused on the availability of their services, but you are responsible for data availability.

Cloud providers continue to invest in their architectures to make them highly resilient and available. However, resiliency and availability are not enough to protect against data loss or corruption due to accidental deletion, unforeseen outages, malicious intent or poor software. Currently, native cloud provider recovery tools are limited and immature, with notable gaps with respect to data protection. While cloud providers will make every effort to preserve the data, these providers do not generally offer enterprise-grade backup with centralized policy-based schedules and retention, or granular data restore options.

The customer service agreements for the large hyperscale providers — AWS, Microsoft Azure and Google Cloud Platform — indicate that customers are responsible for their own data. These providers do, however, offer point-in-time storage snapshots, versioning capabilities and database transaction archive capabilities. But, these capabilities alone are not a substitute for backup.

The same is true for SaaS-based service providers. Organizations have no recourse for data recovery (or compensation). They are solely responsible for the backup/recovery of their data, regardless of whether data loss is due to a service outage, hardware failure, data corruption, malicious action or accidental deletion. Partial service credit may be offered for SLA breaches, but reducing monthly fees does not cover potentially large data replacement efforts and costs, or damages due to legal compliance penalties.

In 2019, Gartner advises that organizations re-evaluate their data availability and DR strategies to support both on-premises and cloud-based workloads. Recommendations include:

- **Leverage cloud-based IaaS services to augment on-premises backup and DR solutions.** Cloud-based object storage can often replace off-site, tape-based backup data, and failover to a public cloud can be a viable option for many workloads. Integration with public cloud storage has become standard for enterprise backup solutions. Disk-to-disk-to-cloud (D2D2C) backup methodologies allow for maintaining on-site backup images for quick recovery of large datasets, while placing less frequently accessed, long-term retention data in a cloud storage tier.

  Solutions that currently back up remote-office or endpoint user data to local tape can be replaced by lower-cost and more manageable solutions that back up data directly to the cloud.

  Cloud-based DR and DR as a service (DRaaS) extend this concept further. These approaches enable workloads to run in the cloud by leveraging the cloud-based backup data or primary data that is replicated directly to cloud storage. Such approaches have become popular among organizations with fewer than 100 production systems or VMs that were previously shipping tapes off-site for DR. In addition, these approaches are starting to gain significant traction with larger organizations. Cloud recovery, as an alternative to a secondary on-premises data center,
can eliminate facility costs and minimize standby DR IT infrastructure, thereby reducing capital expenses and management overhead.

- **Assess current on-premises data availability tools and processes — including backup, data replication and DR orchestration capabilities — to determine whether they can be extended to support cloud-based workloads and data.** As more mission-critical workloads are migrated to, or born in, the cloud, standard operational processes such as backup/restore and DR are necessary to support them. IaaS-, PaaS- and SaaS-based data may be as important as, or more important than, on-premises data. Traditional on-premises backup solutions include robust functionality and mature management capabilities, but they were not designed for cloud deployment or on-demand licensing models. Although many of these solutions have agent-based options that support public cloud VMs, customers must typically bring their own licenses and need to purchase upfront capacity-based software. Furthermore, much of the recent focus on hypervisor-based backup and integrated snapshot management is not applicable to cloud-based workloads. Technical professionals should leverage newer backup as a service (BaaS) providers’ offerings, which can be deployed with subscription, usage-based consumption models and can align with cloud practices. Separate solutions may be needed for IaaS and SaaS, so look for providers that support the leading SaaS-based applications, including Google G Suite, Microsoft Office 365 and Salesforce offerings.

DR for cloud-based workloads does not come for free with IaaS or PaaS, but users should expect service resiliency for unplanned outages to be included from their SaaS vendors. Data replication options are available for IaaS and PaaS that ensure critical data is available in more than one cloud region from the same provider. However, DR orchestration, automation and testing, along with application design considerations, are the responsibility of the client. Technical professionals should leverage cloud-friendly DR orchestration tools that include replication capability to meet their organizations’ recovery time and recovery point objectives. Microsoft’s Azure Site Recovery enables Azure-to-Azure failover capability. In addition, third-party vendors such as Actifio, CloudEndure and Veritas Technologies provide broader support for orchestrating IaaS workload DR across cloud providers.

Given the sensitivity and importance of data availability, rethinking and rearchitecting the protection of all data center and cloud-based data must be a top priority.

**Extend Your Security Control Practices Into the Public Cloud**

Workloads and data in the cloud must be secured to the same level as workloads and data on-premises. The difference is that you may not find an identical cloud-native control in every case. In such cases, you will need to adopt an equivalent cloud-native control — one that you may not be familiar with yet — instead. Nevertheless, the control stack you will have in the cloud will be very similar to the one that you have on-premises.

It can be taken for granted that major cloud service vendors such as AWS, Google, Microsoft and Salesforce are secure, but technical professionals must architect and configure the appropriate controls to have their organizations use them securely. While leading cloud providers offer many cloud-native controls to help you use their services securely, these controls are not necessarily easy

The Gartner clients that will have the most success in rising to the cloud control challenge will organize themselves around the following control priorities:

- Foundational controls
- Basic controls
- Risk-based controls

**Foundational Controls**

Foundational controls are the baseline security capabilities you always need. Operationalizing cloud deployments requires organizations to achieve excellence in foundational controls. While the categories and nature of controls are similar to what you have on-premises, the tooling required for foundational controls generally differs from the on-premises counterparts.

The foundational controls are:

- **Cloud management plane/console security:** This part is a new responsibility. Cloud services have consoles and APIs that allow clients to create and destroy. Gartner recommends that clients tightly control console accounts and the creation of API keys that are used for automation. For example, API keys with limited rights should be created, and multifactor authentication should be used for privileged accounts.

- **Architectural considerations:** Cloud services have high levels of redundancy built in. However, you still need to architect your cloud deployment to meet your availability and redundancy requirements. For example, you can deploy certain services into multiple availability zones to mitigate the risk of outages due to catastrophic events in one zone. Other architectural considerations are backup and DR, and also the general layout — such as how many virtual networks you will use and how many security zones you require.

- **Asset management:** Clouds allow quick instantiation of systems. Some systems are short-lived, but they still need to be protected equally. This is where asset management becomes important. It shows you what systems, IP addresses and other IT assets you actually have. Forms of asset management can be found in AWS CloudWatch and CloudTrail, Azure Security Center, or third-party applications such as CloudCheckr or Dome9.

- **IAM:** Gartner recommends that clients develop a solid strategy for provisioning identities (e.g., for login and authorization in the cloud). Every login action must be accountable and trace back to a unique known user. The major cloud providers offer a variety of possibilities to integrate with your existing directory service.

- **Monitoring:** Gartner recommends that clients monitor cloud systems with the same due diligence as on-premises systems. One possibility is to use cloud provider offerings such as Azure Security Center (although the log analysis is not free). Other possibilities include using
cloud security information and event management (SIEM) products such as Sumo Logic. For more information, see “Security Monitoring and Threat Detection in Public Cloud Environments.”

Basic Controls

Basic controls are security controls that are accepted best practices — but not for all use cases. For instance, instead of deploying an endpoint protection platform (EPP) on high-performance database servers, clients may choose to patch those servers more frequently, or they may choose to deploy, for example, a self-updating Oracle autonomous database.

The basic controls are:

- **Network access controls:** Cloud services offer built-in security groups that very closely resemble modern microsegmentation. Gartner recommends that clients deploy security groups, unless they have a company policy stating, for example, that a Layer 7 firewall is required.

- **Traditional EPP for cloud instances:** You can align this with your on-premises strategy. For example, if you have EPPs on all your on-premises servers, you should use the same products in the cloud. If your EPP vendor does not support the cloud yet, you should select a new product that is cloud-ready.

- **Vulnerability management:** If you use vulnerability management on-premises, you should also use it in the cloud. However, not all vulnerability management products are cloud-native. CSPM tools can be helpful third-party additions for visualizing and managing cloud assets, security and vulnerabilities. Larger CWPPs, such as Trend Micro, can also be a good solution.

Risk-Based Controls

Risk-based controls are specialized controls that are configured according to the outcome of a structured risk assessment, and are used to mitigate identified risks. The list of risk-based controls below is not exhaustive; many clients will have capabilities that are not listed. Examples of risk-based controls are:

- **Data-at-rest encryption:** Encryption should be deployed in pockets, wherever you assess that the risk to your data is too big without encryption. While Gartner believes that encryption is not a panacea, we have seen some clients treat encryption as foundational and encrypt all data at rest in clouds. You can do this by using built-in encryption features and managing the encryption keys yourself. Alternatively, depending on your requirements, you can let the cloud provider generate and manage the encryption keys for you.

- **Application security testing:** Many clients have custom applications, such as MSAs, deployed on top of containers in the cloud. The security of the custom application very much depends on the application itself and whether it was developed securely. For example, if the application was developed using vulnerable libraries, it will be more at risk. To enhance the security of deployed microservices (and traditional applications), successful clients frequently use software
composition analysis products. For more information on securing applications in containers, see “Container Security — From Image Analysis to Network Segmentation, Options Are Maturing.”

Organizations Will Invest in Developing Cloud Skills Across Disciplines

Organizations often underestimate how steep the skills ramp can be for technical professionals as they expand their specialization for cloud. There are new roles and new responsibilities. Some skills gaps can be filled by evolving existing professionals’ training, while others require experienced resources that may not be available in the organization.

IT is no longer about the technology but rather the culture and skills needed to consume new technologies. The technology problems are being solved for us.

Additionally, an organization’s cloud adoption strategy could dictate new teams, such as:

- A cloud center of excellence (CCOE)
- Site reliability engineers
- “PlatformOps”

Furthermore, organizations are already leveraging, or will soon leverage, multicloud strategies. This will have a skills impact as well, as technical professionals will need to learn about more than one cloud provider’s public cloud platform. It is important to allow time and budget for skilling up, certification and potentially new hires as your organization matures in its public cloud adoption. For more information, see “Analyzing the Role and Skills of the I&O Professional in DevOps.”

Planning Considerations

In 2019, IT organizations must begin to execute on their plans to update their technical professionals’ skill sets and get them ready for the cloud. They must also implement the right roles and build the necessary teams that can be held accountable for cloud projects. To plan and execute efficiently, organizations must take the steps needed to:

- Build a cloud center of excellence
- Identify a cloud architect, and hire or train cloud engineers
- Align operations skills and approaches to the cloud
- Evolve IT into a broker of services
Build a Cloud Center of Excellence

A cloud center of excellence is a centralized cloud computing governance function for the organization as a whole. The CCOE serves as an internal cloud service broker (CSB), and typically oversees functions such as:

- **Policy**: The CCOE oversees the creation of, and ongoing updates to, the organization’s cloud computing policies.

- **Vendor selection and workload placement**: The CCOE works with the sourcing and vendor management organization to choose cloud computing vendors, and to put master service agreements in place. The CCOE’s architects help end users in the organization choose appropriate cloud solutions and adopt the organization’s best practices.

- **Governance**: The CCOE selects and configures organizationwide tools for cloud computing governance. This will typically include, at a minimum, selecting and configuring a cloud service expense management (CSEM) tool. This may also include setting policies for automated governance, such as the policies in the AWS Config and Azure Policy services.

- **Knowledge base**: The CCOE creates, maintains and solicits contributions to a cloud computing knowledge base. This serves as a repository of institutional knowledge and best practices.

- **Code repository**: The CCOE creates, maintains and solicits contributions to a code repository that contains orchestration templates, CCA recipes and other infrastructure-as-code artifacts. The goal is to instantiate best practices in code, to encourage technical professionals to use this code as the basis for their own solutions, and to motivate technical professionals to contribute code improvements back to the repository.

- **Community of practice**: The CCOE brings together technical professionals across the organization to share best practices and lessons learned. It typically follows the format of other best-practice councils and communities of practice within the organization, using internal collaboration tools on an ongoing basis, in conjunction with occasional in-person meetings.

The CCOE is typically attached to the office of the CIO, the enterprise architecture discipline or other centralized IT functions that operate under the authority of the CIO. In distributed organizations with business unit or division-level CIOs, there may be both a central CCOE and an ancillary CCOE (under one or more of the other CIOs). It is also possible for only a single business unit to have a CCOE — a common pattern in organizations that have a distinct digital business division.

The CCOE is normally led by a senior-level enterprise architect who functions as the organization’s chief cloud architect. Initially, the CCOE may consist of just a single cloud architect. The architect typically chairs a cloud computing policy council, which has representatives from:

- Sourcing, vendor management and IT finance
- Infrastructure and operations
- Security, regulatory compliance, risk management and legal functions
- Application development
- Other technical end-user teams, such as researchers, scientists and engineers
- Business management, especially leadership from digital businesses

The CCOE typically consults with members of this council, but these members are not part of the CCOE. The CCOE usually consists purely of cloud architects, though during the early stages of cloud adoption, there may be also some centralization of cloud engineers within the CCOE.

The CCOE is intended to provide governance rather than control. Self-service is typically the most effective way to adopt cloud computing (for more information, see “5 Approaches for Public Cloud Self-Service Enablement and Governance”). However, most end users seek the fastest, easiest path to the business result they are seeking. Consequently, the CCOE’s most important job is to ensure that best practices are readily available, highly attractive and easy to implement. Because best practices for cloud services are constantly evolving and the organization needs flexibility to innovate, the CCOE must produce the least-restrictive, most-effective guardrails it can to ensure that self-service does not create undue risks for the organization.

**Identify a Cloud Architect, and Hire or Train Cloud Engineers**

Cloud projects often involve complex integration between on-premises services and cloud platforms and services. These projects require skilled technical professionals who are proficient in both on-premises technologies and modern cloud platforms. The complexity of cloud adoption requires at least one accountable architectural leader to guide the organization through the transformation that cloud computing warrants. This is the task of the cloud architect.

The cloud architect is responsible for the entirety of cloud computing initiatives in an organization, and for directing the architectural aspects of an IT broker group’s cloud work across all aspects of IT and the business. A cloud architect must evangelize, strategize and delegate. He or she must also primarily architect, design, facilitate, lead and direct cloud initiatives on multiple fronts.

The cloud architect has three main responsibilities:
- Lead cultural change for cloud adoption
- Develop a cloud strategy and facilitate adoption
- Develop and coordinate cloud architecture

For more information, see “Analyzing the Role and Skills of the Cloud Architect.”

While the cloud architect focuses on cloud leadership, architecture, vision and business engagement, the cloud engineer is responsible for the tactical implementation and operationalization of the strategy. Depending on the organization and structure of the cloud team, cloud engineers are either part of the cloud architect’s core team or part of the cloud architect’s virtual team. The cloud engineer’s main responsibilities include:
Translating the cloud strategy and architecture into an implementation design that meets business requirements in accordance with best practices

Continuously tracking progress and optimizing the cloud implementation for technical and cost efficiencies

Continuously supporting and collaborating with other teams and projects as needed

For more information, see “The Cloud Engineer: An Evolutionary Role for a New IT Era.”

**Align Operations Skills and Approaches to the Cloud**

In the era of cloud and digital business, IT operations needs to adapt to a faster delivery cadence. Product developers are transferring the pressure they feel to react more quickly to changes and to deliver on the promise of the cloud and digital business (see Figure 17). If I&O is unable to deal with the volume of change demanded, or if updates are so delayed that business initiatives are obsolete before they are deployed, a new approach is needed.
Figure 17. The Last Barrier to Agility

The Last Barrier to Agility

Products/Development:
- Scrum
- Agile
- CI/CD
- Sprint

I wonder what they're doing?

Infrastructure and Operations:
- ITIL
- Backup
- DR
- Performance
- ITSM
- Security
- Virtualization
- Storage
- Networks

ID: 361515

ITSM = IT service management
Source: Gartner (October 2018)
Development teams and I&O staff require the ability to safely provision, configure, deploy, monitor and decommission environments at will. To satisfy this need, organizations require self-service portals, scalable platforms and repeatable processes that allow product teams to own the entire lifecycle of their products. Early adopters of cloud services, containers, microservices and DevOps have shown real progress toward this goal. However, the use of these new models is not yet commonplace, and many I&O organizations still deliver infrastructure in traditional processes. This situation has prompted some business groups to engage in “shadow IT” — i.e., circumvent internal I&O entirely and go directly to cloud providers for infrastructure and services.

This scenario is both a challenge and an opportunity for I&O professionals. It means that their performance objectives, tooling, roles and organizational boundaries must change. It also means that some individuals may move from central I&O functions to join product teams as members.

However, Gartner does not believe that the importance of I&O specialists is declining in any way. These specialists merely need to adapt their skills to be in demand in the era of cloud, agile development and DevOps.

New cloud and infrastructure technologies do not obsolete I&O roles. However, operation of these technologies requires roles and skills that are different from the ones established when all IT infrastructure was built inside the data center.

To better align their operations skills to the cloud, organizations should ensure that their I&O professionals are specialists who understand the nuances of the underlying technology and the complexity beneath the abstractions. That way, they can help their product development colleagues and users be more productive. In addition, these organizations should prepare for the possibility that their cloud adoption strategy could dictate the need for new operations-related teams, such as:

- Site reliability engineering (SRE)
- PlatformOps

**Site Reliability Engineering**

Many organizations striving to mature DevOps-oriented cloud operations are turning to the set of principles and practices known as SRE, which was pioneered by Google. In “Hype Cycle for DevOps, 2018,” Gartner defines SRE as “a collection of systems and software engineering principles used to build and operate resilient distributed systems at scale.” An SRE team applies these principles — usually in combination with DevOps and agile practices and tools — to responsibilities such as risk management, release engineering, monitoring, self-healing, incident management and problem management. An SRE team collaborates with developers to design, build and continuously improve systems to meet SLAs. These SRE capabilities align very well with cloud-operations-related tasks.
An SRE team performs operations work, but it is staffed by developers who are focused on reliability. Reliability and resilience are shared responsibilities that require collaboration between the SRE team and the application developers. The engineers in the SRE team are experts in driving continuous reliability improvements through feedback loops. Operations are managed to explicit SLAs. The SRE team should not spend most of its time on operational firefighting. If an application is unstable enough to consume significant SRE time, the application developers are responsible for remediating the issues, and they may become directly responsible for excess operational labor.

PlatformOps

The term “PlatformOps” does not have a standard industry meaning. Gartner uses it here to denote a team that provides, as an internal service, cloud-based application infrastructure capabilities to multiple application development teams for self-service consumption. Frequently, the PlatformOps team is not purely an operations team. It often needs significant software engineering skills because the platforms it offers to internal customers as self-service are complex and software-defined. In some cases, this group may be primarily an engineering team that develops what is effectively middleware as a service. Engineers in PlatformOps typically have cloud engineering and DevOps skills.

Gartner encourages organizations to implement PlatformOps with a product mindset for the platform they offer.

A PlatformOps team may perform purely cloud-based work, but some teams may operate on-premises services as well. PlatformOps typically has one or more of the following responsibilities:

- Deploying and operating a PaaS framework, such as Cloud Foundry, or a container-based PaaS, such as OpenShift.
- Delivering some form of middleware as a service, such as the Apache Cassandra database as a service. (Usually this will be something that the cloud provider doesn’t offer as a native service.)
- Deploying and operating a CMP.
- Developing and operating a proprietary platform.
- Developing and operating unique application infrastructure services (custom middleware).

Evolve IT Into a Broker of Services

Business users have no interest in buying technology; they want a set of services enabled by technology and are unconcerned with the details of the underlying infrastructure. The role of the internal IT organization must change from provider to broker as multicloud strategies are adopted. Specifically, the role of IT is evolving from a mere deliverer of technology to become the broker to the business of all IT-based services. As discussed earlier, this paradigm is called “hybrid IT,” and its aim is to blend traditional IT services, public cloud and private workloads into a consistent offering. This transformation means that technical professionals must adapt organizational structures, roles, governance, skills and toolsets.
Most organizations start with ad hoc adoption of cloud services both inside and outside the governance of IT. The journey to hybrid IT from this state requires a brokering function to centralize interactions, decision making and governance. The role of a service broker is twofold:

- Enable developers, consumers and lines of business to quickly access technology services
- Safeguard the interests of the business through the application of centralized policies and procedures

If there is too much intermediation, users will avoid the brokering function and go straight to the providers. If there is too little, the brokering function will add no value to the organization.

Brokerage involves adding value by aggregating, integrating and customizing the underlying technologies. There are two approaches to implementing a brokering function:

1. Outsource the broker function to an external managed service provider
2. Deliver the brokering function from within the organization’s internal IT team

Whether you build the capability internally or outsource to a service provider, centralized brokering has the following advantages over a decentralized approach to service adoption:

- A uniform approach consistent with business goals and initiatives
- A consistent user experience and service request interface
- Standardized, reusable reference architectures and templates
- Well-thought-out, centrally governed application and service placement
- Coordinated, proactive platform security consistent across external and internal silos
- Consolidated provider contracting, procurement and management
- Cross-silo expense management and control
- Cross-silo monitoring and operations management
- Cross-silo automation and orchestration capability

In addition to external IT services, the brokering function will also cover internal or private IT technology silos. These silos range from traditional IT systems in the data center (e.g., mainframe, UNIX, virtualized and nonvirtualized x86, storage and networks) to colocation facilities, managed hosting, and private IaaS and PaaS implementations. A key requirement is to understand which environments are strategic for your organization and which are planned to be closed down, consolidated or stabilized. The brokering function should be designed to encompass only strategic technology silos. Spending time on engineering, portals and provisioning across nonstrategic technologies is a poor use of valuable resources.

Software tools alone are not sufficient to implement brokering. While CSB tools and CMPs are important, attention must also be paid to organizational structure, functional roles, skills,
procurement, finance and governance changes. For more information, see “Adapting IT to Become the Broker of Cloud Services.”

### Setting Priorities

Most organizations will not be able to tackle every planning consideration described in this document within a single year. 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 to advance the use of cloud services across the business.
- Continuously evaluate moving workloads to public clouds. The providers’ services are constantly evolving and maturing.
- Establish a multicloud strategy, and begin the process of onboarding a second strategic IaaS or PaaS provider, if you have not done so already. Evaluate and give preference to providers that offer cloud services at multiple cloud tiers. Look for a common foundation of capabilities — networking, identity, security and billing.
- Develop a management strategy, and include multicloud management and hybrid cloud as part of this strategy. Invest in learning your providers’ native services, and evaluate third-party tooling options to address specific gaps in requirements.
- Develop a multicloud governance strategy. Define principles and policies to govern the guardrails around cloud service consumption. Continuously audit your workloads, and automate remediation of policy violations.
- 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.

**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. Empower the cloud architect to work across functional teams, and start building expertise across all functional areas.
- 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 SaaS solutions to start freeing IT from the burden of managing and maintaining a large portfolio of 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.

- Augment data center backup services with tools that support recovery of cloud-based data. Include a DR strategy when migrating workloads to the public cloud or developing new cloud-native applications.

- Start designing for hybrid architecture, and prioritize this infrastructure. Hybrid infrastructure will become 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 Enabling Governance of Public Cloud Computing”

“5 Approaches for Public Cloud Self-Service Enablement and Governance”

“Analyzing the Role and Skills of the I&O Professional in DevOps”

“Identity Next: Rethinking Identity Governance and Administration”

“How to Manage Public Cloud Costs on Amazon Web Services and Microsoft Azure”

“Implementing Cloud Security Monitoring and Compliance Using Amazon Web Services”

“Implementing Governance for Public Cloud IaaS and PaaS”

“How to Evaluate Public Cloud SaaS Providers and Their Solutions by Developing RFP Criteria”

“How to Integrate Cloud-Hosted, SaaS and On-Premises Applications”

“Designing a Public Cloud Exit Strategy”

“A Guidance Framework for Architecting Portable Cloud and Multicloud Applications”

“Utilizing Hybrid Architectures for Cloud Computing”


“Adapting IT to Become the Broker of Cloud Services”
Evidence

1 Gartner Technical Professional Study, 2017. Results are based on a Gartner study conducted to provide an overview of how technical professionals are dealing with changes related to digital business. The research was conducted online from 30 March 2017 through 2 May 2017 among 555 respondents, primarily in North America. A subset of Gartner for Technical Professionals seatholders was invited to participate. Respondents were required to be a member of their organization's IT staff or department (or serve in an IT function). Furthermore, they could not serve as a member of the board, as president, or in an executive-level or IT leadership position. The survey was developed collaboratively by a team of Gartner analysts who follow technical professionals, and was reviewed, tested and administered by Gartner’s Research Data and Analytics team. The results of this study are representative of the respondent base and not necessarily of the market as a whole.

2 “Summary of the Amazon S3 Service Disruption in the Northern Virginia (US-EAST-1) Region,” Amazon Web Services.

More on This Topic

This is part of two in-depth collections of research. See the collections:

- Research Roundup: Building and Marketing Cloud-Based Offerings — 3Q18
- 2019 Planning Guide Overview: Architecting Your Digital Ecosystem