Although the goal of corporate strategic planning is to envision changes over the long term, the stark reality for IT in many organizations is that only incremental change seems possible in the short term. IT’s ability to implement the changes needed to alter the competitive playing field might be limited by the siloed nature of most IT departments, where separate teams enact deployment cycles implemented on a product-by-product basis with each product set purchased and managed separately. Customization is usually the rule, with different servers selected for different applications by different teams. Attempts to integrate data center infrastructure and applications have been manual, time-consuming, and expensive efforts. With traditional data centers of the past limited to maintaining the status quo, this scenario often led to a breakdown and disconnect between corporate planning and IT capabilities.

Fortunately the situation is changing with the advent of cloud computing; CIOs have been freed from having to settle for incremental change, and IT can now be the enabler of line of business (LOB) requirements for faster innovations, new business models, and new revenue streams.

Because today’s cloud computing architectures are designed to capitalize on change, more expansive opportunities exist for IT to become an internal strategic partner. By enabling holistic improvements across technology infrastructures, cloud computing is creating dramatic innovations that rewrite the rules of competition. Instead of a plethora of customization arising from siloed teams, IT organizations are beginning to standardize their infrastructure to create a highly agile IT foundation with integrated layers designed to adapt to changing requirements. The opportunity to use both private cloud and public cloud services—termed “hybrid IT”—provides enterprises more choice and speed in implementing new innovations.

As the Gartner perspective that follows this article frames it: “Hybrid IT is the mission and the operational model for IT in a cloud
computing world…Fundamentally, hybrid IT requires working with the enterprise, including business leaders, to change the working relationship between the enterprise and IT to one where IT is the trusted broker and value-added supplier for all IT-based services, whether they are internal or external.”

If IT can act as a services broker, it will address a set of common needs in the industry: simplification, information transparency, and control of services selected, provisioned, and consumed from several sources—private, public, and hybrid.

The potential for deep and wide flexibility frees organizations to think big, literally out of the box, beyond the constraints of the past. When considering potential breakthroughs to change the competitive playing field, instead of asking “why,” IT can dare to ask “why not?” This path to transformational change requires five major steps.

**Step 1: Develop a Future Vision of How to Conduct Your Business**

The first half of this step is to be bold: Leave your memory of operational obstacles at the door and develop a vision of how you want your operations to run to deliver competitive advantage to your business. After that vision is clear, the second half is to be rigorous: Systematically identify the obstacles within your organization that prevent your vision from becoming a reality. Ask yourself and your organization questions such as:

- What processes need to be reengineered?
- What new capabilities need to be developed?
- How much faster are you seeking to get to market?

Because the IT organization is best able to identify the technology gaps between the processes the organization wants and the processes it has in place, the CIO plays a pivotal role during this step. And, unlike the past, IT organizations can now implement the transformational cloud architecture they need to accomplish a transformational vision to satisfy the requirements of their LOB stakeholders.

IT leaders are expressing the need for increased transparency and control for cloud services to make sure they can effectively drive value while directly managing risk. They desire secure, seamless, intuitive access for end users to the services required to increase business agility, using the right service at the right time across the various organizational functions.

End users and LOB leaders speak to the need to rapidly select and launch IT services from on-premise and/or cloud vendors, in comparison to the days or weeks needed to receive approval for services based upon legacy infrastructure and approval processes.

Approaching transformational architecture discussions can be addressed within the Cisco Domain TenSM framework, which covers ten major areas an organization should consider to successfully transform IT into a more agile, cost-effective business resource. Whether you want to take advantage of virtualization or move to cloud-enabled services, Cisco Domain Ten covers important aspects of infrastructure, virtualization, and automation to map your transformational journey. And, in addition to technology considerations, Cisco Domain Ten covers security, compliance, process, and governance implications. (See Figure 1.)
This paper will focus on considerations for the three cloud-enabled “building blocks” within the Cisco Domain Ten℠ framework of infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS). Each building block is essential for a comprehensive cloud solution, and each is designed to integrate with the other two in conjunction with the other domains to enable greater business agility and speed.

Although the cloud building blocks will next be outlined in a chronological order often followed by organizations like yours, you might want to focus on a different order. Regardless of your preferred approach, it is important to keep in mind the need to look holistically at your organization’s requirements in each block before you make purchase decisions in any one area. Looking at the bigger picture helps to make sure solutions you standardize at one level, say, for IaaS, are capable of meeting your requirements for security and compliance when you implement SaaS.

**Step 2: Develop the IaaS Building Block**

The second step is to plan an agile IaaS foundation, enabling infrastructure services to be managed by IT in a highly automated fashion and delivered to users in minutes. Standardizing on compute, storage, and networking elements designed for virtualization and cloud will, when integrated together, deliver greater value than each provides independently. Avoid products not designed for easy integration, or you will be hampered when you attempt to automate resource virtualization, which will be required if you want to gain the flexibility to quickly adapt to changing business demands.

By standardizing on agile, integrated assets, IT can also create resource packages in a self-service catalog, empowering customers (whether LOB stakeholders or external end users) with the resources they need to support new initiatives in minutes. To make sure IT can operate as a “business within the business,” the IaaS building block needs to enable IT to set up and track usage-based billing so customers know and can plan for the cost basis of the services.
they are consuming. Proper monitoring and metering of service usage for show back or charge back to the LOBs is another area of differentiation between IT truly acting as a broker of services, in comparison to legacy IT operating models. The self-service catalog of authorized applications and services, plus the associated service provisioning, monitoring and metering, are core capabilities required of any solution for the brokering of IT services.

Organizations often will create a Cloud Program Office, consisting of IT leaders and LOB leaders, to drive the selection and authorization of services available in the catalog. The Cloud Program Office will manage the full lifecycle of the service assets, be they sourced from on-premise/private data center and cloud infrastructure or from public providers of SaaS, IaaS, and PaaS. (See Figure 2.)

![FIGURE 2](image)

Building blocks of cloud brokerage: SaaS, PaaS, and IaaS

Source: Cisco

The IaaS layer should be designed to facilitate innovation from outside the company. Creating an infrastructure for innovation might require the integration of services delivered via the public cloud. By enabling a hybrid cloud environment in the IaaS layer, IT can play the strategic role of “cloud services broker” within a cloud model for the organization, helping departments make the decision about how to access mission-critical services, whether delivered internally or via the public cloud or a combination of both. (Organizations making significant process innovations to promote different business models will likely choose a mix of both.) IT can add significant value by making sure the IaaS layer can dynamically aggregate, integrate, and customize the delivery of cloud services to best meet the needs of the business.

If you think usage of public cloud services does not apply to your organization, think again. As we have rolled out assessment and optimization services on cloud consumption to assess the world of “shadow IT” within the realm of the “hidden cloud,” our customers have found 5x, 10x, and even 40x more cloud service utilization than they estimated.

Indeed, one governmental organization with strict cloud services usage guidelines limited to 11 authorized providers found in fact that over 220 different cloud services were in use throughout its departments. Getting a handle on hidden cloud utilization and finding what its stakeholders truly need to run the business have opened a powerful dialog for IT to increase its relevancy and step up to help manage the total picture for the stakeholders to minimize risk, cut costs, and optimize the user experience.

Step 3: Add the PaaS Building Block

The platform as a service (PaaS) building block uses the agility in the IaaS foundation by automating the provisioning of operating systems, middleware, and databases, ultimately delivering greater efficiencies and flexibility in the development and deployment of cloud workloads. By adding the PaaS layer, IT gains the advantages of an underlying infrastructure to mask the complexity of the IaaS foundational elements so it can more efficiently write and test new initiatives at lower cost.

Without PaaS, when an organization wants to develop and test initiatives that need large amounts of compute and storage, it would require dedicated capacity to be allocated by IT and enabled with appropriate software. Developing the PaaS building block allows your organization to instantly begin developing the program using hosted or cloud assets using APIs.

After the testing phase is complete, the PaaS foundation allows IT to instantly reallocate the capacity. PaaS accelerates the development and deployment of applications to market significantly more quickly than IaaS alone, making it possible to launch new capabilities sooner. Benefits accumulate from hardware, software, and maintenance savings, as well as productivity improvements, particularly for those companies in which speed to innovation is paramount.

Step 4: The SaaS and Infrastructure Security Building Block

New applications accessible via SaaS can empower organizations to quickly test new business concepts and implement new business models in furtherance of their transformational goals. To facilitate implementation of SaaS solutions, the next building block of agile infrastructure enables the automated provisioning of applications for faster business intelligence and processing of transactions.
Although SaaS can offer organizations an exceptional way to speed innovation, the innovation generated will be limited if it is not fully integrated into the company’s overall IT strategy to meet required availability, manageability, security, and compliance standards. It is in this building block where IT’s ability to act as a cloud service broker within an overall cloud governance model plays a particularly critical role.

Regardless of whether a service is delivered in-house from a private cloud or through a cloud service provider, the business is accountable for always making sure of the security of corporate and customer data, always complying with regulations, and always making the data available to other applications that need it. For these reasons, applications and associated data acquired through SaaS should not be viewed in isolation. For the integrity of the organization, cloud-based services—regardless of sourcing—are best managed as one cohesive infrastructure, meeting identical governance, security, performance, and availability standards. (See Figure 3.)

Acting in the role of service broker, IT can help LOB organizations analyze potential SaaS providers to determine if they are suited to be an integrated part of the company’s cohesive cloud strategy. IT can best determine whether the SaaS provider is in full compliance with the regulations to which the company must adhere. IT also needs to make sure the SaaS-driven application provides adequate performance, including speed and availability of data access, so other applications relying on SaaS-supplied data can perform effectively.

In addition, the IT organization will be able to evaluate the SaaS provider’s ability to meet the organization’s security requirements. In contrast to the traditional model of directing network traffic to a stationary security device, today’s data center security must be more fluid and intelligent to adapt to changing traffic and user conditions. The ideal cloud security solution is designed to facilitate ease of provisioning, maximize performance, and deliver pervasive protection across physical, virtual, and cloud-based environments.

Security strategies should address services delivered via the private cloud to make sure IT has the ability to:

- Authenticate end users/customers and give them specific rights based on their relationship, creating a secure zone so the business can respond to requests immediately.
- Make sure of secure multitenancy, so end users/customers can access only their specific data.

- Protect access to customer data by creating a secure environment from the endpoint to data storage using policy-based solutions that limit access to authorized users, dynamically encrypt sensitive data, block data from being uploaded to external devices, and prevent customer data from being stored on employee or contractor devices.

Whether a business rents capacity from an external service provider or has a SaaS application that needs to access its data center, the IT security strategy should include:

- The ability to detect unexpected or unusual behavior. For instance, if a user is accessing a large number of files, IT needs to be alerted immediately, with the ability to stop that activity.
- The ability to control who has access to a SaaS application by using web security tools that manage all certificates to SaaS vendors. Such control makes sure that, if someone’s role changes or they leave the company, IT can immediately revoke their privileges.

To accomplish these objectives, the entire IT infrastructure must deliver speed, agility, and security together. Identity and context-aware policies and strong encryption capabilities can build trusted links and extend a chain of trust from the user all the way to the application.
Because Cisco security technology is integrated directly into the infrastructure, Cisco security solutions are designed to meet those requirements. Further enhanced by Cisco’s massive threat telemetry security operations center, which constantly drives real-time threat updates to Cisco’s security solutions every three to five minutes, IT departments using Cisco security can identify and block threats before they disrupt services.

**Step 5: Implement Transformational Change**

After you have constructed your agile and secure infrastructure, you can begin to reengineer and develop business processes to convert your vision into reality. (See Figure 4.)

![FIGURE 4](source)

The Five Steps for IT Leadership

1. **Think Big — What is your vision for changing the playing field**
2. IaaS: Rationalize/standardize your data center infrastructure
3. PaaS: Incorporate OS, middleware, databases for PaaS
4. SaaS plus adaptable, integrated security infrastructure
5. Redefine business processes

When it comes to making transformational changes, best practices are as important as best-in-class technology. It’s ability to fully use the agility of its technology infrastructure and partner with business units to develop and implement new processes is the linchpin in the company’s ability to change the competitive playing field.

To be successful, your organization might want to rely on the expertise of others who are experienced in this unique combination of technological and organizational change. If you are seeking a trusted partner to successfully help you define and implement your transformational vision, consider Cisco® Services.

Cisco Services have defined a comprehensive strategic framework known as Cisco Domain Ten that helps organizations like yours implement industry best practices to reflect their specific requirements, building block by building block. Cisco Services help IT develop the customized evaluation criteria to effectively play the role of cloud service broker, so IT can quickly make decisions about when to purchase innovative services from the public cloud and when to have them reside within the private cloud. We also have extensive experience working with companies around the world to implement new processes and organizational change.

**Changing the Strategic Planning Process**

As CIOs use these five steps, their cloud computing architectures can permanently change the corporate strategic planning process—making what was once impossible, possible. Rather than being consulted after a strategic plan is developed, CIOs should be included in the earliest strategic planning discussions to brainstorm game-changing plans. IT leadership is the cornerstone to use the power of cloud computing to align strategic business and IT objectives under a cloud model. When undertaken holistically, the destination point of IT acting as services broker enables a more agile business, more satisfied end user populations, greater degrees of data security and control, and the reduced total cost of ownership promised by cloud.

**For More Information**

- Cisco Domain Ten
- Cisco Services for Cloud

**Customer Success Stories**

- Canadian Managed Service Provider OnX Realizes Cloud Goals with Cisco Cloud Services
- Healthcare Benefits Administrator CareCore National Moves Business to the Cloud
- Improving Business Processes and IT Delivery for Aviation Leader Thales UK
- IT Services Provider Earthlink Deploys Cloud-Ready Infrastructure
- Microsoft Enhances Service Delivery with Private Cloud
- Savvis Creates New Class of Enterprise-Cloud Services (Video)

Source: Cisco
Cloud computing is taking multisourcing to a new, more dynamic level, changing the mission and operational model for IT and I&O in particular. Being a competitive IT provider isn’t good enough — the new core competency is being the trusted broker for services delivered from many, changing providers.

**Key Findings**

- Hybrid IT requires new organizational roles and structure, where the infrastructure and operations (I&O) organization can take on and/or delegate responsibility to external IT service providers, multisourcing service integrators (MSIs) and cloud services brokerages (CSBs) to deliver the needed IT services for its organization.

- The hybrid IT function within an organization will become one of the most critical technology and partnering investments made by enterprises, and will influence how IT makes decisions on all technologies and IT services used by the enterprise.

**Recommendations**

- Organizations must decide how the hybrid IT mission will be fulfilled: by the I&O organization, by external brokers and integrators, or some combination.

- The I&O organization must evolve its organization model and skills to handle new roles for service interfaces, brokerage, governance, integration, etc., or build relationships with external providers that can do the same.

- Enterprises must actively drive alignment across key roles (including business leaders, procurement and sourcing departments) and IT, and educate internal teams to adapt their role and mission within the enterprise in support of hybrid IT models.

- Employ a strategic approach in the deployment of cloud management platforms (CMPs) and CSBs as enablers. Create an organization, operational processes, business relationships and technologies that deliberately make multisourcing (cloud and non-cloud, on-premises and off-premises, and private/public/hybrid cloud) transparent, dynamic, efficient and effective for IT’s customers.

**Analysis**

As cloud computing matures as a style of IT service delivery, the mission for IT — and especially I&O — is changing. The term “hybrid IT” describes the new function and operational model for IT in a cloud computing, dynamically multisourced, heterogeneous world. A hybrid IT organization is a trusted broker, interface and provider for all IT services, whether private or public, which will be a combination of services provided by the IT organization and external providers, using both cloud computing styles and traditional styles of computing that are integrated, aggregated, customized, managed and governed to meet enterprise IT requirements.

**The Road to Hybrid IT**

In the past, IT’s mission was to be the provider of the IT services needed for an enterprise to meet its goals. Outsourcing offered the ability to source some or all IT services from an external provider. In 2005, as outsourcing matured, Gartner described multisourcing as the state of the art in leveraging multiple external providers of IT services, and since then, Gartner has provided a rich foundation of research for effective and efficient management of multisourcing and multisourcing integration.

The cloud computing style takes multisourcing to a new, broader, much more dynamic real-time and granular level. The fundamental difference is the low barrier to entry that is at the heart of cloud computing services — the ability to turn it on quickly, scale it rapidly up or down, and (ostensibly) turn it off, on demand. Service provider relationships in a cloud computing market can potentially be temporary, and usage can vary dramatically. This not only changes the nature of provider relationships (forming and possibly dissolving rapidly, more dynamically, more automatically and indirectly), but it also completely changes the nature of the usage of IT by the business. The cloud computing style is not simply another way to deliver the same IT services; it enables experimentation and innovation by the enterprise, by reducing the risk and entry expense of using IT services. This is true both for public cloud computing (where startup expenses are replaced with usage-based pricing) and for on-premises private cloud computing (where risks and expenses are shared across the organization).

The automated service interface of cloud computing services also creates a new dynamic — the ability for relationships and usage to be brokered and managed in a policy-based and automated manner. Additionally, the services themselves can be delivered in a dynamic and multisourced manner, from a combination of internal, external, cloud, noncloud, private cloud and public cloud services. Similar to the more static role of MSi, a new and more dynamic role of CSB has emerged in parallel. A hybrid IT organization will encompass both roles and abstract sourcing styles for any service.

By lowering the barrier to services, cloud computing also makes it easier for anyone to purchase and access the services that they need. However, easy access does not eliminate the requirement for solution and provider selection, contracting and/or payment, usage and cost governance, service-level assurance, risk and security management,
compliance management, integration and customization, problem management, disaster recovery, solution migration, etc. In hybrid IT, the role of I&O is to be the value-added enabler for the most effective and efficient use of services, across the enterprise — when those value-added services are needed. IT eliminates the requirement for enterprise users to be concerned about how a service is being implemented and acquired — allowing them to focus strictly on using the service. The challenge for I&O is to provide these value-added services without creating tremendous latency in the process; speed and agility are critical to avoid the IT organization being bypassed by a do-it-yourself IT service user of cloud computing.

**Hybrid IT and the Enterprise**

When functioning correctly, the role of hybrid IT changes the relationship between IT and the enterprise. Less mature relationships position I&O as a custodian of IT resources, where the enterprise is intimately involved in implementation details. More mature relationships are service-oriented, where I&O is considered by the enterprise as a service provider that delivers based on service levels. However, as cloud computing matures, the enterprise can potentially consider IT as just another provider among many. Hybrid IT requires the relationship to expand, where IT becomes the trusted broker for all (or at least most) IT-based services, regardless of provider sourcing, or style of service delivery. It will continue to take responsibility for service delivery and service levels, even when those services are delivered by other providers, but they should shield the enterprise from provider selection, style of computing choices and integration issues, and should ensure compliance with corporate and industry governance requirements. Successful hybrid IT organizations are outcome-driven, and understand the dynamic relationship between business requirements and results.

The I&O organization must actively work with its internal customers to change its role and mission within the enterprise. This requires both the stick (the executive mandates about what business units can and cannot do with respect to using IT-based services), and the carrot (the benefits that users receive by using enterprise IT as the trusted broker). Successful IT organizations will identify the problems that need to be solved (i.e., cost control, security, inefficiency in governance, compliance, etc.), and will identify and prioritize where they can provide value-adds (i.e., ease of billing, reduced complexity, single sign-on, service-level management, etc.). The proof will always be in the results; identifying and solving a specific problem as an interface and broker, for specific enterprise customers, will create buy-in.

**Hybrid IT and the I&O Organization**

Hybrid IT requires new organizational roles and responsibilities, and, in most cases, the existing I&O organization is best-suited to implement these roles. Previously, organizations were likely to use an internal procurement group or an external MSI to manage their multisourcing needs. In the hybrid IT model, there is the potential for every group to act as a broker of services. This, in turn, has the potential to lead to chaos in the organization, because of the loss of governance over technology procurement and consumption. Two roles are critical to address this problem:

- The IT broker group
- The public cloud management group

The IT broker group acts as the intermediate supplier when the enterprise requests a new service or business outcome, and determines, among other things:

- Service architecture (traditional, private cloud, hybrid cloud, public cloud, etc.)
- Sourcing methods and policies (internal, external providers, or some combination)
- Service duration (immediate, short term, long term, etc.)
- Enterprise requirements (compliance, security, disaster recovery, etc.)
- Service integration (single sign-on, data portability, pricing, etc.)
- Runtime policies (runtime sourcing decisions based on workload, resource utilization, security, compliance, etc.)
- Service quality demand (performance and availability requirements)
- Service economics (flexibility and cost)

These decisions are not necessarily static. For example, a service might be designed that leverages several external cloud providers that change over time, or where usage is based on pricing or availability of internal resources. The IT broker group sets policies...
for how multisourcing or hybrid cloud services are dynamically provisioned. When brokering between multiple cloud providers (including private), the IT broker group is taking on the role of the CSB. However, the IT broker group will also take on the interface role for traditional services, which may be insourced, outsourced, hosted, etc.

The IT broker group should also be proactive in identifying changes in the market or requirements that may require changes in the service architecture, sourcing methods and policies. For example, the services delivered by cloud computing providers may mature to the point where it is more cost-effective and efficient to use external services, rather than sourcing those services from an on-premises private cloud.

A public cloud management group will take on primary responsibility for:

- Identifying potential cloud providers (including identifying cloud services that can and should be leveraged by the enterprise, and being proactive with the enterprise when opportunities arise)
- Forging relationships with cloud providers (including evaluating their capabilities and contracting for their services including integration into the CMP or CSB marketplace). This would include having an up-to-date list of providers that could be used on-demand for a short duration
- Managing and monitoring service delivery (including problem management)
- Displaying and communicating risks (i.e., integration) including the risk mitigation
- Understand the minimum requirements for services that can be quickly leveraged
- Determining whether or not to use external third-parties for brokerage roles
- Performing cost comparisons between providers over time and ensuring cost-effective solutions

Hybrid IT for the Midmarket

Smaller enterprises will find they require multiple providers of services, possibly with varying levels of isolation/privacy, and integration across those providers. However, many midmarket enterprises will turn to third parties that take on the MSI, value-added reseller (VAR) and/or CSB roles. In those cases, the trusted broker of multiple services will likely be a third party, but the strategy and requirements will be the responsibility of the enterprise. These third-party entities will provide hybrid IT capabilities generally and CSB specifically, particularly as the consumption of public cloud services increases. Although the market for CSBs is still young and emerging, Gartner believes it will grow substantially during the next few years.

Hybrid IT and Technologies to Watch

Hybrid IT will be enabled by a variety of technologies that deliver integration, governance, contract management, service catalogs, etc. Some services managed by hybrid IT will be traditional — modernized, virtualized and automated, but not cloud. However, with respect to cloud services (both public and private), there are two emerging technology centers of gravity that enable hybrid IT. The first is the CMP, which is essentially the service interfaces and service automation needed to create and deliver a cloud service. All cloud services are built around CMPS. Many enterprises are building private clouds today based on CMPS. Very simple CMPS are focused on the delivery of a single service. The second technology area is CSB enablement. These are technologies that specifically enable aggregation, integration and customization across multiple cloud services — essentially, working with multiple CMPS.

While these are two different technology areas, a natural evolution of the CMP being used for private clouds is hybrid cloud interoperability and orchestration — mainly the aggregation function of CSB. Some CMPS are very general-purpose, intended to manage and deliver many cloud services, and also to handle a broad CSB role between those cloud services and external cloud services.

I&O organizations need to be strategic in their plans for CMPS and CSB enablement. Tactically, the goal may be to enable a specific cloud service, enable a specific hybrid cloud service or manage a specific brokering capability. However, tactical solutions can lead to islands of technology, processes and organizations. Strategically, I&O should set its sights higher. Plan for hybrid IT by creating an organization, operational processes, business relationships and technologies that deliberately make multisourcing (cloud and noncloud, on-premises and off-premises, private/public/hybrid cloud) transparent, dynamic, efficient and effective for IT’s customers.
Why Cisco Services?
With more than 28 years of experience, more than 50 million installed devices, and 6 million customer interactions each year, Cisco has the expertise and proven track record to help you successfully migrate applications to the Cisco Unified Computing System.

With Cisco Services, you’ll know more, save more, and innovate more. Delivered by Cisco and our Cisco channel partners, service engagements result in measurable business gains for our customers, who have achieved benefits such as 15-20% faster acceleration to revenue; 30% lower infrastructure costs; 50% faster disaster recovery; and 90% reduction in deployment time. For information about Cisco Services, visit www.cisco.com/go/services.

About Cisco
Cisco (NASDAQ: CSCO) is the worldwide leader in IT that helps companies seize the opportunities of tomorrow by proving that amazing things can happen when you connect the previously unconnected.

Evidence
1 CMPs are integrated products that manage public, private and hybrid cloud services and resources.

2 CSB is an IT role and business model in which a company or other entity adds value to one or more (public or private) cloud services on behalf of one or more consumers of that service via three primary roles: aggregation, integration and customization brokerage.

Gartner Research Note G00245906, Thomas J. Bittman, Drue Reeves, Ed Anderson, 28 June 2013