OPEN DATA CENTER ALLIANCE℠ USAGE MODEL: CLOUD SERVICE BROKERING REV. 1.0

TABLE OF CONTENTS

CONTRIBUTORS

Mustan Bharmal – T-Systems
Anand Chaganty – Infosys
Sudip Chahal – Intel IT
Bernd Henning – Fujitsu
Iain Macrae – National Australia Bank
Prasanna Raman Sridhar – Infosys
Tom Scott – The Walt Disney Company
Jeff Sedayao – Intel Corporation
Avi Shvartz – Bank Leumi
Ryan Skipp – Deutsche Telekom
Stephanie Woolson – Lockheed Martin

LEGAL NOTICE

This "**Open Data Center Alliance℠ Usage Model: Cloud Service Brokering**" document is proprietary to the Open Data Center Alliance (the "**Alliance**") and/or its successors and assigns.

NOTICE TO USERS WHO ARE NOT OPEN DATA CENTER ALLIANCE PARTICIPANTS: Non-Alliance Participants are only granted the right to review, and make reference to or cite this document. Any such references or citations to this document must give the Alliance full attribution and must acknowledge the Alliance's copyright in this document. The proper copyright notice is as follows: "**© 2014 Open Data Center Alliance, Inc. ALL RIGHTS RESERVED.**" Such users are not permitted to revise, alter, modify, make any derivatives of, or otherwise amend this document in any way without the prior express written permission of the Alliance.

NOTICE TO USERS WHO ARE OPEN DATA CENTER ALLIANCE PARTICIPANTS: Use of this document by Alliance Participants is subject to the Alliance's bylaws and its other policies and procedures.

NOTICE TO USERS GENERALLY: Users of this document should not reference any initial or recommended methodology, metric, requirements, criteria, or other content that may be contained in this document or in any other document distributed by the Alliance ("**Initial Models**") in any way that implies the user and/or its products or services are in compliance with, or have undergone any testing or certification to demonstrate compliance with, any of these Initial Models.

The contents of this document are intended for informational purposes only. Any proposals, recommendations or other content contained in this document, including, without limitation, the scope or content of any methodology, metric, requirements, or other criteria disclosed in this document (collectively, "Criteria"), does not constitute an endorsement or recommendation by Alliance of such Criteria and does not mean that the Alliance will in the future develop any certification or compliance or testing programs to verify any future implementation or compliance with any of the Criteria.

LEGAL DISCLAIMER: THIS DOCUMENT AND THE INFORMATION CONTAINED HEREIN IS PROVIDED ON AN "**AS IS**" BASIS. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE ALLIANCE (ALONG WITH THE CONTRIBUTORS TO THIS DOCUMENT) HEREBY DISCLAIM ALL REPRESENTATIONS, WARRANTIES AND/OR COVENANTS, EITHER EXPRESS OR IMPLIED, STATUTORY OR AT COMMON LAW, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, VALIDITY, AND/OR NONINFRINGEMENT. THE INFORMATION CONTAINED IN THIS DOCUMENT IS FOR INFORMATIONAL PURPOSES ONLY AND THE ALLIANCE MAKES NO REPRESENTATIONS, WARRANTIES AND/OR COVENANTS AS TO THE RESULTS THAT MAY BE OBTAINED FROM THE USE OF, OR RELIANCE ON, ANY INFORMATION SET FORTH IN THIS DOCUMENT, OR AS TO THE ACCURACY OR RELIABILITY OF SUCH INFORMATION. EXCEPT AS OTHERWISE EXPRESSLY SET FORTH HEREIN, NOTHING CONTAINED IN THIS DOCUMENT SHALL BE DEEMED AS GRANTING YOU ANY KIND OF LICENSE IN THE DOCUMENT, OR ANY OF ITS CONTENTS, EITHER EXPRESSLY OR IMPLIEDLY, OR TO ANY INTELLECTUAL PROPERTY OWNED OR CONTROLLED BY THE ALLIANCE, INCLUDING, WITHOUT LIMITATION, ANY TRADEMARKS OF THE ALLIANCE.

TRADEMARKS: OPEN DATA CENTER ALLIANCE℠, ODCA℠, and the OPEN DATA CENTER ALLIANCE logo® are trade names, trademarks, and/or service marks (collectively "**Marks**") owned by Open Data Center Alliance, Inc. and all rights are reserved therein. Unauthorized use is strictly prohibited. This document does not grant any user of this document any rights to use any of the ODCA's Marks. All other service marks, trademarks and trade names reference herein are those of their respective owners.

OPEN DATA CENTER ALLIANCE℠ USAGE MODEL: CLOUD SERVICE BROKERING REV. 1.0

EXECUTIVE SUMMARY

As cloud computing becomes an increasingly important aspect of enterprise IT operations, the complexities of obtaining secure, efficient, and cost-effective cloud services have given rise to a new entity: the cloud service brokerage. These intermediary services—positioned between the cloud subscriber (and/or consumer) and one or more cloud providers—can ideally help businesses to achieve their computing objectives as they consume and maintain cloud services, often relying on multiple providers to do so. Meeting these objectives entails obtaining IT services on demand, provisioned remotely by a third party, scaled precisely to meet business demands in real time, and with cost benefits derived from critical mass processing levels, operated by experts in their fields, with shared development costs. Clearly, many different factors are involved, requiring expertise and decision making to reach resolution.

Numerous approaches are available for addressing the use of cloud services as a part of IT operations. Provisioning IT operations is a key role that could be accomplished by a cloud broker, although there are many different interpretations of what a cloud broker's function should be and whether this role should be an ongoing technical function or an ad hoc consultancy service. As such, the Open Data Center Alliance (ODCA) recognizes the need for clarification—a paper to assist organizations in identifying and evaluating options for their own potential use of this type of function.

Each of the various models for incorporating a cloud broker function could foster different business benefits. These models also suggest a range of organizational objectives to be considered. Some of the approaches may favor the use of an internal (IT-based) broker, the use of a consulting organization, the use of a neutral, trusted third party, or the use of a contracted service provider, among others. Cloud brokers can make it simpler for cloud consumers to acquire cloud services. The cloud broker can collect information about available cloud services, analyze the information, and use the outcomes of the analysis to streamline the decision making process when determining which cloud provider to use. Naturally, it follows that there may be various "degrees of implementation" of the cloud broker function. For simplicity, this paper focuses on a full-fledged implementation (according to a number of potential models), at the following levels:

- Technology
- Services
- Processes
- Commercial aspects

However, each individual organization needs to evaluate its own objectives and needs to determine what variation or possible subset of a cloud broker can efficiently and effectively satisfy its requirements.

Some of the dimensions to consider in leveraging cloud-based services to achieve business objectives are also encapsulated within the ODCA Cloud Maturity Model (CMM). With this in mind, this paper includes a set of cloud-maturity considerations in the context of a cloud broker.

This document describes a usage model for establishing and engaging a relationship and function between a cloud service broker (broker), cloud service provider/s (provider), a cloud services subscriber (subscriber), and a cloud services consumer (consumer) for the provision of cloud services.

This document serves a variety of audiences:

- Business decision makers looking for specific frameworks
- Enterprise IT groups involved in planning, operations, and procurement
- Solution providers and technology vendors, to help them better understand customer needs and tailor service and product offerings
- Standards organizations, that may find the information useful in defining standards that are open and relevant to end users

> "A CSB [cloud service broker] can make cloud services more valuable because they work closely with cloud providers to get price breaks or access to more information about how a service works. In addition, they have more experience working with multiple providers and across many consumer scenarios. Instead of spending time and money to address these problems internally, consumers can leverage solutions offered by CSBs that allow organizations to focus on other pressing business needs instead. A viable CSB provider can make it less expensive, easier, safer and more productive for companies to navigate, integrate, consume and extend cloud services, particularly when they span multiple, diverse cloud services providers."
>
> *– Daryl Plummer, managing vice president and Gartner Fellow at Gartner and chief of research for cloud computing*[1]

Purpose

This document offers a definition of the cloud broker's role and describes the value that a cloud broker brings to the service chain by acquiring cloud services from a cloud provider. The document is agnostic to the cloud consumer's level of maturity in the adoption and governance of cloud services.

For enterprises with a high level of maturity in the adoption and governance of cloud services, we anticipate that a number of the models and scenarios outlined are not necessarily consistent with the full range of models and scenarios in use within the enterprise.

For enterprises with a lower level of maturity, the models and scenarios included in this usage model offer guidance for establishing an operating model or service model that facilitates the engagement of a cloud broker, a cloud provider, a cloud subscriber, and a cloud consumer for the provisioning of cloud services.

This document includes workflow diagrams and processes, service management and governance considerations, and a set of key performance indicators (KPIs) to assist a cloud consumer in determining how to engage with a cloud broker or how to establish an internal cloud-broker capability.

This usage model targets these goals:

- Define the basic elements of cloud service brokering for infrastructure-as-a-service (IaaS) and platform-as-a-service (PaaS) cloud services.
- Apply the baseline work on the "ODCA Usage Model: Service Catalog"[2] and the "ODCA Master Usage Model: Service Orchestration."[3]
- Identify the usage scenarios, characteristics for engaging a cloud broker, KPIs, and processes relevant for cloud service brokering.
- Align with the "ODCA Master Usage Model: Commercial Framework"[4] and "ODCA Master Usage Model: Compute Infrastructure as a Service"[5] to underpin cloud services provisioning.
- Define a standard set of brokering models and processes that can be used as a reference model for improving interoperability between cloud brokers, cloud providers, and cloud subscribers.

[1] Plummer, Daryl. Excerpt from "Cloud Services Brokerage: A Must-Have for Most Organizations" (2012). www.forbes.com/sites/gartnergroup/2012/03/22/cloud-services-brokerage-a-must-have-for-most-organizations

[2] www.opendatacenteralliance.org/library

[3] Ibid.

[4] Ibid.

[5] Ibid.

Taxonomy

Table 1 lists the standard terms and their corresponding description that are used in this document.

Table 1. Terms and descriptions.

Term	Description
Agent-Based	Refers to agent-based cloud computing, in which software agents have been designed and developed to facilitate the delivery of cloud services. The agents may be proprietary (specialized) APIs or open APIs.
Agentless	Refers to the use of standard programming interfaces (open APIs) to discover a cloud service through which a remote API is exposed by the cloud service or direct analysis of a communication network operating between the cloud provider and/or the cloud broker.
Cloud Broker	A person or organization that consults, mediates, and facilitates the selection of cloud-computing solutions on behalf of an organization. The cloud broker is further described in the Cloud Broker Definition section below. The cloud broker may be an external person or organization or may be an internal function or role within an enterprise.
Cloud Consumer	A person or organization (typically the business units or lines of business) that actually consumes cloud services from a cloud provider in the context of the subscriber's framework, either by means of a cloud broker or by means of a direct engagement with a cloud provider to receive cloud services.
Cloud Provider	An organization that charges cloud subscribers for providing cloud services over a network. Under a cloud services brokering model, the cloud provider may charge a cloud broker for the cloud services and the cloud broker in turn will charge the cloud subscriber. A cloud provider delivers services through a communication network, such as the Internet, an intranet, a LAN or a WAN.
Cloud Subscriber	An organization that has been authenticated to a cloud and maintains a business relationship with a cloud provider or cloud broker. Also sets policies, guidelines, and frameworks for the organization's use of cloud services.
Solution Provider	A technology vendor selling technology elements that can be used to build a cloud or other service, usually specializing in either a specific software product, a specific hardware product, or by providing consulting services.

WHAT IS A CLOUD BROKER?

Cloud Broker Definition

Within the context of this usage model for cloud services brokering, the vision of the cloud broker is:

To support the effective and efficient translation of a demand (from a cloud subscriber) and to discover services (from one or more cloud providers), which translate to or directly match that demand (in either a direct or aggregated format) to enable the cloud subscriber to then select the final cloud provider(s) from a resulting list (created by a cloud broker) of (discovered and offered) cloud services to meet the stated requirements, and to then instantiate and operate the selected cloud service(s) and aggregate from that selection of one or more cloud providers, a resulting service which meets the cloud subscriber's requirements at a technology, service, and commercial level.

A number of potential definitions exist, two of which are offered below. The definitions tend to be variations on the basic theme outlined above.

What Does the Term "Cloud Broker" Mean?

According to Techopedia:[6]

A cloud broker is an individual or organization that consults, mediates and facilitates the selection of cloud-computing solutions on behalf of an organization. A cloud broker serves as a third party between a cloud service provider and organization buying the provider's products and solutions. A cloud broker is also known as a cloud agent.

Techopedia Explains Cloud Broker

"A cloud broker generally works on typical brokerage process principles. They assist cloud buyers with decision making by helping them evaluate, shortlist, and select a cloud vendor or solution based on specific requirements. Typically, cloud brokers collaborate and have mutual agreements with different cloud vendors, where, if selected, discounts and faster deployment and migration are provided.

A cloud broker also negotiates terms and conditions, pricing, delivery, deployment, and other details with a cloud vendor on behalf of a buyer. Although primarily considered a sales and marketing oriented service provider, a cloud broker also may provide consultation, deployment, integration, and migration monitoring services."

[6] www.techopedia.com/definition/26518/cloud-broker

Gartner: Three Types of Cloud Brokerage Will Enhance Cloud Services[7]

1. **Cloud service intermediation.** An intermediation broker provides value-added services on top of existing cloud platforms, such as identity or access management capabilities.
2. **Aggregation.** An aggregation broker provides the "glue" to bring together multiple services and ensure the interoperability and security of data between systems.
3. **Cloud service arbitrage.** A cloud service arbitrage provides flexibility and "opportunistic choices" by offering multiple similar services to select from.

This usage model considers the full potential scope of a broker, although real-world implementations may adopt only selected or limited portions of that complete scope.

Cloud Broker Composition

The cloud broker definition established in the preceding section offers a context in which to better understand the role of a cloud broker that is external to the cloud consumer's organization. The definition more closely depicts the role of the cloud broker as presented in the linear model (see the Cloud Broker Engagement: Role of the Cloud Broker in the Cloud Service Chain section).

A cloud broker can also be an internal role or function within a cloud consumer's organization. In such a case, the model for engagement of the function can be customized to suit the organization's operating model. This approach is closer to the matrix or the sharing between partners models, which are described in the Models section.

Regardless of the engagement model (linear, matrix, or sharing between partners), the cloud broker's role includes a number of key elements, shown in Figure 1, with the focus on the cloud broker in the center block.

All the elements shown in the figure are not necessary to qualify a cloud service broker. The deployed elements of the broker may vary depending on an organization's current needs, maturity levels, and specific functional requirements.

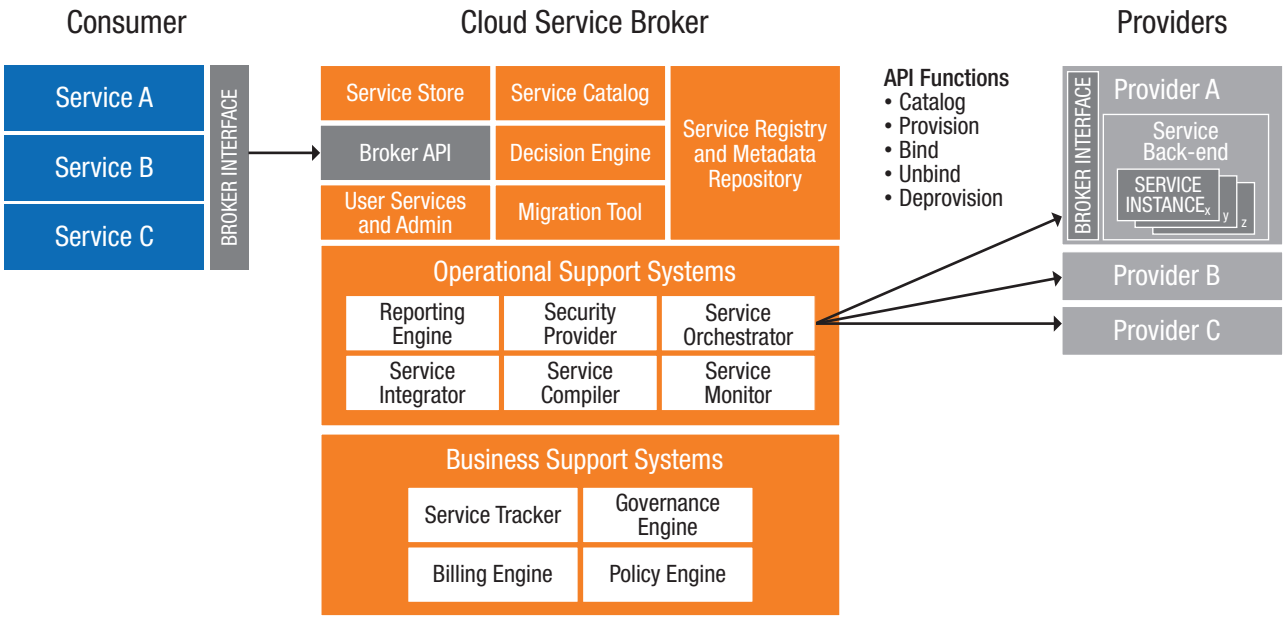

Figure 1. Key elements of a cloud service broker. Note: Not all elements are necessary to qualify a cloud service broker.

[7] D. C. Plummer and L. F. Kenney, "Three Types of Cloud Brokerage Will Enhance Cloud Services" (2009). Gartner. www.gartner.com/doc/973412

The interactions between the cloud broker and the cloud consumer or cloud providers can be based on a number of technologies, as follows:

- Agent-based
  - Proprietary API providing specialized functionality
  - Proprietary API providing specialized calls or using specialized instructions and interfaces
  - Open API
- Agentless:
  - Command line interface
  - Open API
  - Web interface

Typically, the cloud broker will use the cloud providers' API to invoke and operate the provided services. This makes it much easier to integrate new developments and services from that cloud provider. Some cloud brokers, however, deploy their own proprietary agent at selected participating providers to interface to the available services. Similarly, consumers may be expected to deploy and integrate the brokers' API or agent on their side of the service.

WHY USE A CLOUD BROKER?

Cloud Broker Engagement: Role of the Cloud Broker in the Cloud Service Chain

The objective of a cloud broker is to translate consumer service demands into a search for a cloud provider offering the appropriate technologies, find appropriate matches against various criteria from a range of cloud providers, and then triage the resultant options and deploy an appropriate service with a selected cloud provider. From there, the broker may continue to be the intermediary for ongoing service delivery between consumer and providers throughout the service lifecycle.

The first important aspect to consider is the scope of responsibility, as shown in Table 2. The cloud broker is involved at all stages, as indicated by the "X" in the columns and assists the cloud consumer's organization in its use of cloud services by:

- Simplifying the service acquisition process
- Aggregating disparate cloud services into a "single" service from the cloud broker
- Integrating public and private cloud services (hybrid cloud)
- Centralizing governance of the cloud service(s)

The row headings represent the layer of the cloud service, and the column headings represent the lifecycle phase of that layer of the service.

The broker may be positioned in different ways within the service chain. In addition to defining the positioning of the broker, actual access to the services facilitated by the broker may be either by means of the broker or directly to the service provider, once the broker invokes the service.

Table 2. Cloud service layers and corresponding lifecycles.

	Discovery of Services	Negotiation of Services	Deployment of Services	Operation of Services	Change of Services	Termination of Services
Commercial Service Elements (contract, billing, and so on)	X	X	X	X	X	X
Services and Operation of the Managed Cloud Service (service management, incident, problem and change management, and so on)	X	X	X	X	X	X
Technology Deployment of Hardware and Software	X	X	X	X	X	X

WHERE IS THE CLOUD BROKER POSITIONED IN THE SERVICE CHAIN?

Broker Process

Figure 2 shows the end-to-end steps in the cloud brokerage process, starting with the cloud consumer defining the demand and continuing with the cloud broker searching for a match and recommending the options. The process leads to the cloud consumer selecting an option and initiating the service orchestration process and finally to the end of the lifecycle of the service, which includes metering, billing, chargeback, service reporting, and service termination.

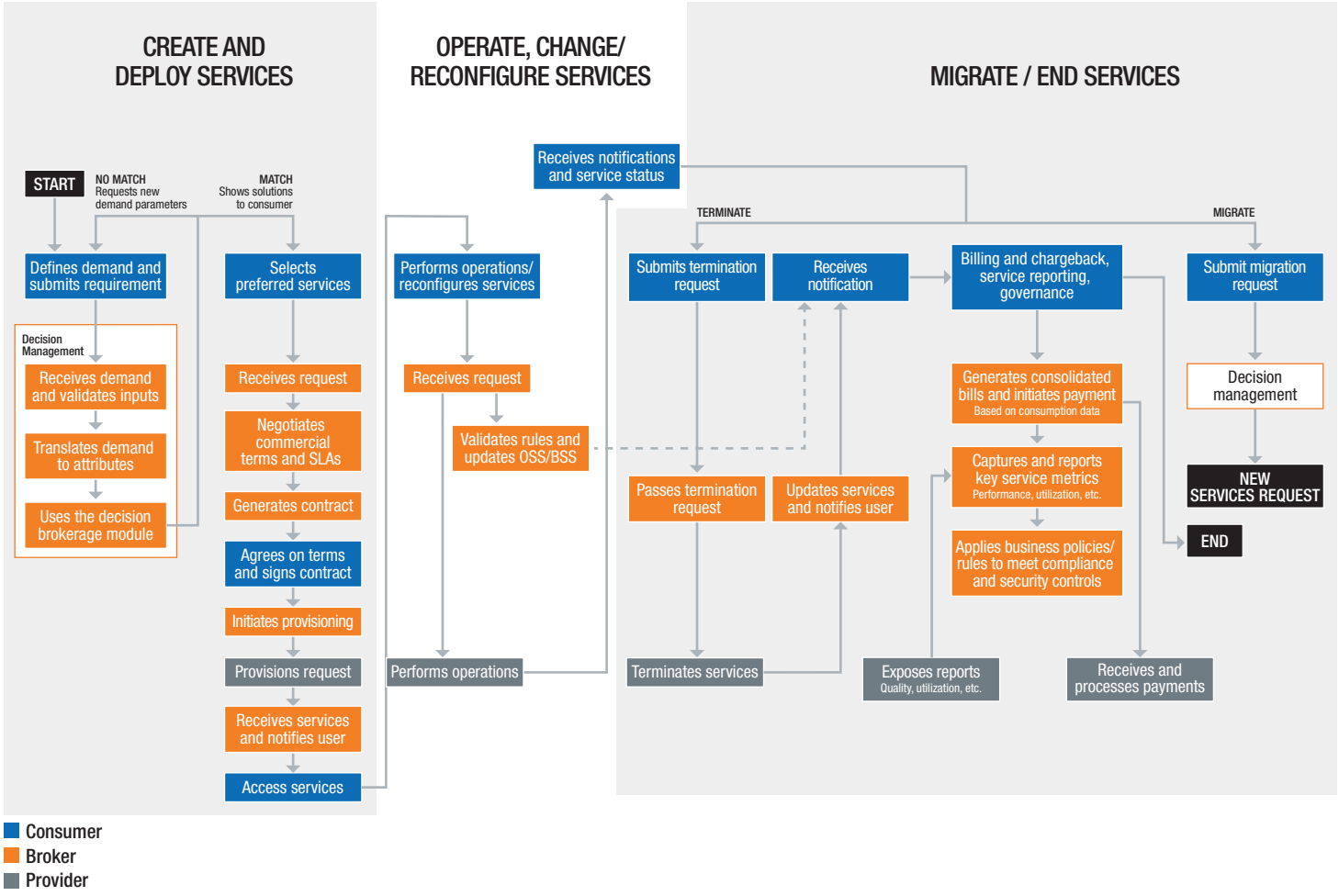

Figure 2. Typical broker process.

Decision Management

In the context of the cloud broker, there are two primary models for decision management. Common to both is the need for the cloud consumer to define the demand and requirements. The cloud broker then searches among the available cloud providers for a match. The cloud broker typically provides a mechanism to help choose the right cloud services. The metadata of these cloud services are made comparable to the cloud broker's decision management. The broker provides decision recommendations based on the request context, involving several parameters.

Once the potential supply matches have been identified, these options exist for final provider selection:

- The cloud broker selects a final cloud provider and satisfies the cloud consumer's requirement by invoking those services. With this model, a number of considerations arise:
  - The cloud broker uses a consistent set of decision criteria, including both the consumers' requirements and the brokers' requirements.
  - The cloud broker may be trying to establish critical mass with certain cloud providers to negotiate better terms or leverage.
  - The cloud broker assumes risks and responsibilities in the context of the contractual framework between it and the cloud consumer.
  - Selections made by the cloud broker may not always be advantageous for the cloud consumer.
  - Reports relating to transparency on the selections and process behind them should be available to foster compliance requirements.
- The cloud broker passes the resulting matches to the cloud consumer to make a final selection regarding the service provider for which the new service demand is to be satisfied. This approach leads to these considerations:
  - The risk relating to the selection of the final service provider may transfer to the consumer.
  - There may be some further negotiation between the consumer, broker, and provider before the services are finally selected and invoked.
  - Selections made by the cloud consumer may not always be advantageous for the cloud broker.
  - The cloud consumer may begin to compare options that the cloud broker provided to other options that the cloud consumer may be aware of and as a result the value proposition of the cloud broker will be under regular review.

To electronically select services and to make decisions to select supply options to match demand requirements, a cloud broker may use human resources or electronic tools.

Given that the (complete) models described provide various options to control the selection, the decision management also spans the lifecycle stages of cloud broker's service chain. A company may elect to deploy a full or partial version of one of the models based on its specific requirements. The decision management is invoked at various stages (such as discovery, negotiation, deployment, operations, change, and termination) to ensure that the right options are evaluated and presented during the "real-time" operations of the provisioned cloud services. Ideally, this results in the appropriate actions being performed to maintain the cloud service deployments at optimal levels.

The decision management process should be pervasive and comprehensive enough to be able to make decisions driven by multiple considerations. We also recommend that several technical and non-technical aspects be considered during the decision management process. Each of these could carry a rating or relative weight specific to each individual enterprise. The decision management process should triage for relevant options based on the following requirements:

- Enterprise's cloud strategy
- Workload quality-of-service requirements
- Cost and financial considerations
- Compliance and regulatory needs

The preceding recommendation is provided to bring a holistic enterprise view into the cloud broker's decision management process. The cloud broker and cloud consumer (enterprise) are responsible for qualifying and evaluating the factors described, based on the maturity of an organization and the ability of a cloud broker to offer a comprehensive set of brokerage capabilities.

Given the current maturity of the industry and the fact that service providers all have to select from a range of possible standards, frameworks, and interpretations of standards, the higher up the cloud stack one moves, the harder it is to electronically interpret, analyze, and select potential matches. Development is evolving in this area, but any cloud broker is dependent on cloud providers adopting and consistently interpreting and integrating common standards and frameworks for defining and advertising their services and the associated variables.

As the industry matures, solution providers and standards development organizations will likely close this gap. Currently, however, full electronic matching takes significant algorithms and compute power, depending on how far up the stack a broker intends to analyze. This means that tools and formulas for creating matches need to be constantly developed and improved—a significant expense for the cloud broker. If, alternately, the cloud broker uses initial electronic analysis, supplemented by manual investigation, the process may be slightly slower with a different set of costs. Alternately the broker may have already identified pre-selected cloud providers who then develop to accommodate the needs of and interactions with the broker, enabling easier analysis higher up the service stack. However, to remain compliant in these scenarios, the cloud broker may have to apply a consistent set of criteria to its interpretations.

Once the cloud consumer receives a set of options from a cloud broker (as per the matrix model), it should make decisions based on:

- Cost
- Quality
- Features
- Other considerations

In offerings where interpretation is involved, this type of decision may sometimes be more difficult. Offerings that are defined differently by different providers suggest the need for further evaluation. For example, determining whether an infrastructure demand specified "up to providing a managed operating system level" is satisfied by a cloud provider could be made based on cost, or further investigation might show that the operating system on the offer from provider 1 enables the consumer to upload its own management and monitoring agents. In comparison, provider 2 might already include routable agents, and provider 3 might include an entire management and monitoring ecosystem.

To foster equitable comparisons, when passing decisions to the cloud consumer, maximum transparency should be applied so that the cloud consumer understands the implications and consequences (for example, if the consumer makes a decision based on cost and then receives less than expected).

On the cloud broker side of decision making, close communication with the cloud consumer is necessary to understand the nature of the original consumer service demands and to help ensure that a satisfactory service is delivered on an ongoing basis.

Models

With an understanding of the broker's position in the selection process, it is useful to consider the value proposition that the broker brings to the service chain.

Figure 3 show three models depicting the positioning and potential implied value of incorporating a cloud broker in the discovery and delivery of cloud services. An overview of each of the three models follows the figure.

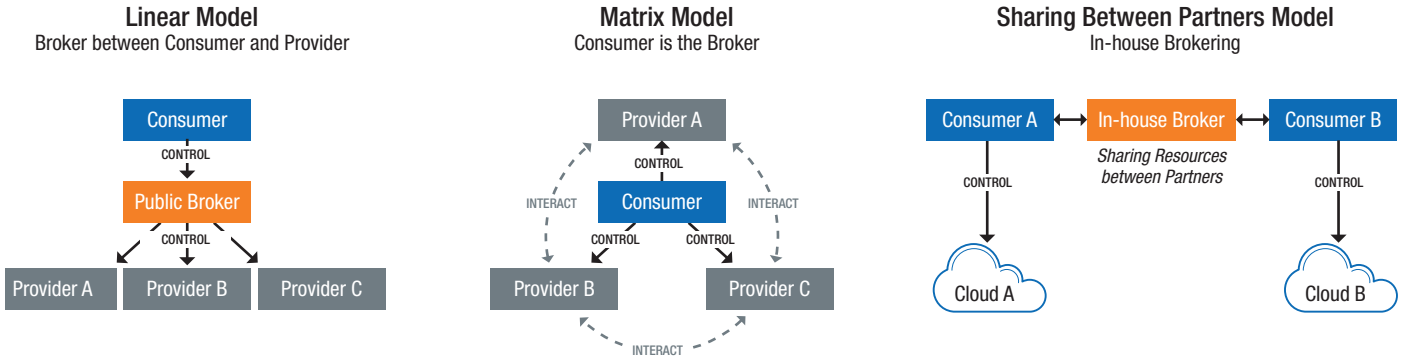

Figure 3. Three models of cloud brokering.

Linear Model

Of the three models shown in Figure 3, the linear model is the one most commonly used when engaging a cloud provider by means of an external cloud broker.

With the linear model, the cloud consumer is able to manage the lifecycle operations of the cloud services—from the cloud provider through the cloud broker. The cloud broker acts as the intermediary between the cloud consumer and the cloud provider and ensures that access to the cloud provider can be achieved through only the cloud broker. The cloud broker may also create an additional layer of abstraction that hides the underlying cloud provider from the cloud consumer. In such a case, the cloud consumer may be unaware of the source of the cloud service.

This model has multiple advantages:

- Provides a single interface view for consuming and managing services from all providers. These could be services provided by individual providers or a combination of services from multiple providers.
- Allows the consumer to select from a list of providers offering services. Alternatively, the broker can manage the decision making on behalf of the consumer based on the consumer's requirements for the service.
- Uses a common pricing and billing model for all providers.
- Relies on a unified service catalog from different providers with various billing and pricing plans to suit various provider services.
- Offers a common integration layer to manage disparate cloud provider interfaces—either directly or through a third-party enterprise service bus (ESB) application.
- Provides a layer of governance for consuming cloud services.

The linear model works well for large enterprises looking to control the proliferation of cloud services within the enterprise. Large enterprise IT organizations also look toward a linear model, which makes it possible for provider access to be restricted at multiple levels using access control mechanisms. The model is also suitable for aggregating and reporting usage metrics across multiple providers, which help track and manage costs.

Matrix Model

The matrix model involves a cloud consumer performing all of the cloud broker functions internally within an organization. The cloud consumer interfaces directly with the cloud provider(s).

To simplify the deployment of applications to multiple clouds, the architecture can include an orchestration layer on the cloud consumer. This layer can feature one API to use, aligning business requests with applications, data, and infrastructure by translating and transmitting requests to different external cloud APIs.

When the cloud broker receives requests under the matrix model, a single API is typically used, so if another provider is added, consumer code written to that API does not have to change. A cloud abstraction API (acquired from an increasing number of cloud libraries) can effectively provide a container around a number of clouds that delivers an understanding of the differences between the various clouds. From the abstraction API, drivers communicate with the cloud provider's proprietary (or open) API, removing the need for the cloud consumer to understand the specifics of the cloud provider's API(s).

This model can also be relevant in a "cloudbursting" scenario, in which an enterprise has multiple internal (private) clouds and needs to access one or two public clouds to deal with unexpected spikes in traffic. In cases where an enterprise has multiple private clouds and operates under the matrix brokering model, the private clouds may be tightly coupled. Individual user IDs could work across all of the internal clouds, implying the clouds in this model would likely operate within single security domains.

Sharing between Partners Model

In this model, business partners share cloud resources for each organization's mutual benefit. Each partner makes a pool of resources available for use by one or more organizations. Use cases for this model include joint development between partners and supply chain integration between customer and supplier. The broker in this model manages access to resources, paying particular attention to the origin of the requestor. Coupling between the clouds will typically be tight, based on the relationship between the organizations sharing resources.

HOW DO I USE A CLOUD BROKER?

Cloud-Broker Service Models

Once the value of the role of a cloud services broker is understood, despite the fact that much of the commentary about cloud classifies clouds into private, public, and hybrid clouds, cloud-brokering models operate differently and can apply to any of the classifications. For this reason, providers are shown in the following figure as providers A, B, or C, any of which may be public, private, or hybrid providers, depending on the consumer organization's specific requirements.

Figure 4 compares three different service models for cloud brokering.

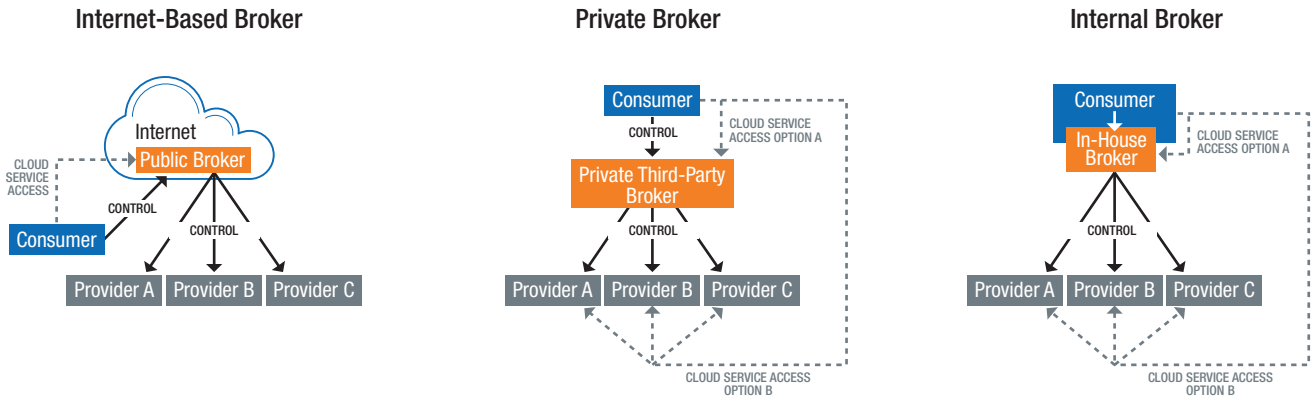

Figure 4. Comparison of cloud brokering service models (with or without agents). NOTE: The term "Cloud Service Access" refers to path(s) by which a cloud consumer/subscriber can access cloud services.

Internet-Based Broker

This category of cloud broker, as depicted in the figure, presumes access to some number of public cloud providers and is generally engaged only by cloud consumers/subscribers with an Internet connection. To use services such as cloud resource acquisition, unified billing, and application deployment, the consumer goes through the cloud broker. Within this Internet-enabled engagement model, the public broker aggregates all services regarding resource acquisition and disposal.

With this category of cloud broker, the Linear Model for engaging a cloud broker is typically used. The Internet-based broker can provide all three kinds of services described in the Gartner: Three Types of Cloud Brokerage Will Enhance Cloud Services section: Intermediation, Aggregation, and Arbitrage/Customization. Only one service access path exists from the cloud consumer to the provider of the cloud service(s), by means of the cloud broker, and there is no direct interaction between the cloud consumer or subscriber and the cloud provider.

Private Broker

Another category of cloud broker is most typically accessed by means of an organization's corporate intranet and provides access to some number of private and public cloud providers. To use services like cloud resource acquisition, unified billing, and application deployment, the corporate consumer engages the third-party cloud broker, using proprietary processes and controls.

Within this model, the private broker aggregates all services regarding resource acquisition and disposal. The linear and matrix brokering models can be used with this class of service broker.

Like the Internet-based broker, the private broker can provide all three kinds of services mentioned in the Gartner: Three Types of Cloud Brokerage Will Enhance Cloud Services section: Intermediation, Aggregation, and Arbitrage/Customization.

Within the private broker model, the cloud consumer may access the cloud services by means of a third-party broker (option A) or through direct engagement with the cloud provider (option B).

Internal Broker

The internal broker—sometimes referred to as an enterprise broker—is a person or organization within an enterprise that consults, mediates, and facilitates the selection of cloud computing needs between segments with an organization.

In providing access to cloud services, the scope of responsibility of the internal broker varies, depending on the requirements of the segment within an organization and its stated needs for cloud services.

An internal broker can be accessed in much the same way as a private broker, through the corporate intranet and typically can provide all three types of services mentioned in the Gartner: Three Types of Cloud Brokerage Will Enhance Cloud Services section: Intermediation, Aggregation, and Arbitrage/Customization.

A number of the key responsibilities of the internal broker (inherent in "external broker" services) are services procurement, service level agreements, security, quality of service (qos), liability and indemnity, internal policy compliance, and federation of services.

Within the internal broker model, a cloud consumer can access the cloud provider either through the internal broker function (option A) within the enterprise or by means of a direct access path to the end cloud provider (option B). Option A typically involves a higher level of centralized internal control of access to cloud providers than option B.

Blueprints and Best Practice Summary

Blueprint of Cloud Broker Capabilities

The blueprint shown in Table 3 depicts the capabilities of a cloud service broker and its various models. This table encompasses the functionalities that a broker should offer and the capabilities that a consumer should expect from a cloud broker.

Fundamentally, this blueprint aims at highlighting the various business and functional elements of a broker. The key capabilities addressed in this blueprint help foster higher benefits and promote visibility, compliance, and governance and minimize the risks of technology and vendor lock-in.

Table 3. Blueprint of broker capabilities.

Business Element	Description of Capabilities
Unified Integration Layer	• Common aggregation platform for integrating various cloud services across multiple providers • Brokering interfaces to multiple cloud providers through a variety of cloud management platforms to foster secured portability/migration of services among providers • Integration with enterprise back-end systems, such as BSS/OSS, help desk and ticketing systems, and automation platforms
Service Catalog (cloud store/service taxonomy)	• A cloud broker requires a service catalog with a wide range of services and a cloud provider ecosystem • Ability to quickly onboard new providers and new services into the catalog for consumption • Ability to offer value-added services over and above the services that providers offer
Decision Framework	• Decision management framework to triage and recommend suitable options across multiple cloud services and providers
Federation	• Ability to offer single sign-on to consume all the cloud services • Federated identity management • Seamless integration with enterprise Active Directory/LDAP systems
Business Process Management	• Business process orchestration engine to orchestrate the provisioning and lifecycle management of the services
Security and Governance	• Granular role-based access control or attribute-based access control • Support standards such as SAML • Encryption of data • Compliance with security standards and regulatory controls
Analytics	• Reporting of standard key performance indicators and metrics

Key Principles to Consider When Engaging a Cloud Broker

- Although it can be tempting (and not initially perceived to be disruptive or to have negative consequences), the consumer should try not to change the cloud broker's functional processes and interfaces. Changing them can lead to a need for proprietary maintenance, and any proprietary customization, in turn, can delay or disable new functionality that the broker will develop. Take full advantage of the broker's core functionality, development focus, and its ongoing stabilization of its core product. Its core focus will always be on this area, and special customized options will tend to run behind the core product.
- If a broker offers a catalog of services available from the providers associated with them, pre-select and define those (or a selection or bundle of them) into the organization's standard service catalog and create a clear process for updating this catalog; providers continually develop and release new products, features, and functions, and review pricing. These changes need to be managed as they find their way into the organization and carefully selected as to which should be released to the consumer and at what advertised price.
- Look for standardization—the use of well-known industry standards and interoperability everywhere—and push for standards-based solutions: in the broker API, in the broker agent, in the processes, in the commercial framework between the consumer and broker, and between the broker and the providers. Standardization leveraging widely adopted industry standards increases portability and reduces lock-in. This approach prevents being locked in to an ineffective relationship and creating the "legacy of the future," where it becomes expensive and costly to extricate the organization from whatever arrangement has been brokered.
- Consumers should onboard their security, compliance, and operating environment standards and controls to ensure the broker is totally aware of the consumer's context and accordingly is able to recommend the right options.

Best Practices to Consider When Adopting Cloud Services through a Cloud Broker

When a cloud broker is contracted to facilitate and negotiate services from various providers on behalf of a consumer, we recommend considering the following important best practices to promote sustainability and operational effectiveness:

- Always try to integrate the service request process to the broker with the consumer organization's procurement and compliance functions so that groups and stakeholders (procurement, risk management, IT, and so on) are kept aware of new services and landscape updates.
- Be absolutely certain when selecting a model for adoption that the cloud broker has experience with the selected model and will be effective in meeting the organization's broad needs. For example, if there is a risk that the broker needs to be replaced, do not consider a linear model, which may lock all the service provisions tied to the broker. However, a linear model may be the best option if one wants fast access to new services from a broad pool of providers.
- Synchronize the planned maintenance slots between the organization and the broker up front; disparate release cycles can create significant disruption and unplanned delays.
- Strictly adhere to compliance, regulatory, and business policies while integrating the broker and when procuring services and managing services from the providers.
- When the broker becomes the primary point of interaction and management of cloud services, ensure that the right authorization rules, entitlements, and usage policies are in place. This approach helps protect the overall integrity and data security of the broker and consumer-specific information.

Cloud Maturity Model and Quality Levels

Services can be rated according to a number of factors, including quality (the depth of service) and maturity (the consistency and completeness of the service in context of fully federated cloud technology). Table 4 defines each of the levels involved.

The following list categorizes these factors as indicated by four quality levels: Bronze, Silver, Gold, and Platinum. In terms of ODCA definitions, as well as related definitions adopted by industry organizations, the quality levels are:

- **Bronze.** Segregation of data through access rights (database privileges) within shared resources (that is, applications, databases).
- **Silver.** Additional segregation through multi-tenancy of resource structures (that is, one's own database plan/schema on a database server) on a shared virtual machine (VM).
- **Gold.** Separate runtime instances and VMs (that is, one's own operating system (OS), databases, applications) on shared hardware, but all hosted tenants at Gold level.
- **Platinum.** Physically separated instances of hardware, VMs, OS, databases, and applications per cloud subscriber.

For more information about Cloud Maturity Model (CMM levels), refer to the ODCA CMM 2.0 model at this URL: www.opendatacenteralliance.org/docs/Cloud_Maturity_Model_Rev_2.0.pdf

Table 4. Quality of service based on the cloud maturity model (CMM). Note that for each quality level, all aspects in the lower CMM level are automatically fulfilled as part of the higher CMM level achievement.

	CMM 1	CMM 2	CMM 3	CMM 4	CMM 5
Bronze	Demands are placed into systems, representing a technology requirement, and suitors are manually sought by people in the back end.	Demands are placed into a system covering technical and service requirements manually, and manually matched providers are found.	Demands are placed into a system covering technical, service and commercial requirements manually, and manually matched providers are found.	N/A	N/A
Silver	Demands are electronically defined with technology, service, and commercial dimensions, and manually selected by people in the back end, from selected providers.	Demands are electronically defined with technology, service, and commercial dimensions, and providers are matched at the technology level electronically, with manual service and commercial matching.	Demands are electronically placed, and providers are electronically matched, at all levels, and based on selection; automatic provisioning is orchestrated.	Demands are electronically placed, and providers are electronically matched, at all levels, with business data protection and compliancy requirements automatically applied, and orchestration of all support systems triggered.	Searches for service matches defined by the provider are automatically conducted across all authorized public and private providers, and automatically matched according to the system element and its associated business rules .
Gold	N/A	Demands are electronically defined with technology, service, and commercial dimensions.	Demands are electronically placed, and providers are electronically matched, at all levels. In addition, business quality rules are applied and based on selection; automatic provisioning is orchestrated.	Demands are electronically placed, and providers are electronically matched, at all levels, with business data protection and compliancy requirements automatically applied and orchestration of all support systems triggered.	Searches for service matches defined by the provider are automatically conducted across all authorized public and private providers and automatically matched according to the system element and its associated business rules.
Platinum	N/A	Demands are electronically defined with technology, service, and commercial dimensions.	Demands are electronically placed and providers are electronically matched at all levels. In addition, business quality rules are applied and based on selection; automatic provisioning is orchestrated.	Demands are electronically placed and providers are electronically matched at all levels, with business data protection and compliancy requirements automatically applied and orchestration of all support systems triggered.	Searches for service matches defined by the provider are automatically conducted across all authorized public and private providers and automatically matched according to the system element and its associated business rules.

WHAT ARE THE PREREQUISITES AND KEY ENABLERS TO USING A CLOUD BROKER?

Key Considerations When Engaging a Broker

Although cloud brokers vary significantly in terms of services and features, there are certain important considerations to keep in mind when engaging a broker:

- **Degree of openness.** The cloud broker's ability to conform to well-defined API interfaces and interoperate easily with cloud providers and cloud consumers.
- **Standards oriented.** The cloud broker's adherence to standards and support for open standards, industry standards, and provider neutrality.
- **Ease of integration.** The degree of integration of the cloud broker's platform with cloud providers and cloud consumers. The integration can be API-based with a two-way integration as follows:
  - Consume the cloud provider's API to be integrated with the cloud broker so that functions, such as service discovery, resource provisioning/deprovisioning, lifecycle management, and so on, can be easily invoked.
  - Expose the cloud broker's own functions in the form of APIs to be integrated with cloud consumers, exposing abstracted, broker-specific functions that are provider agnostic.
- **Minimized lock-in.** This model, in which the cloud broker acts as a bridge, fosters a decentralized operational model; cloud consumers do not have direct access to cloud providers and their resources and have access only through the cloud broker. This also leads to minimizing vendor lock-in, as the cloud consumers will have more options to choose from the cloud broker. As the standards mature, the portability of workloads across providers will become much simpler. This approach minimizes lock-in to the cloud providers. Consumers still need to consider the impact to their organization of being locked in to a particular cloud broker.
- **Federation.** The cloud broker should be able to federate with multiple cloud providers to offer a more seamless cloud-broker ecosystem to cloud consumers. The identity and access can be federated by the cloud broker that can be governed based on policy and enforced to provide single sign-on and seamless integration into the cloud consumer's directory systems.
- **Secured Communication.** The transactions occurring between the broker, consumer, and provider should be secure enough to ensure the integrity and privacy of data passing through these different layers. Make sure that following key security functions to secure the transactions are in place:
  - Strong authentication
  - Entitlements-driven authorization
  - Verification of the integrity of transactions and API calls
  - Cryptographic encryption of data in transit

USAGE SCENARIOS

Figure 5 provides an overview of the typical usage scenarios from the perspective of the cloud services broker, described in more detail after the figure.

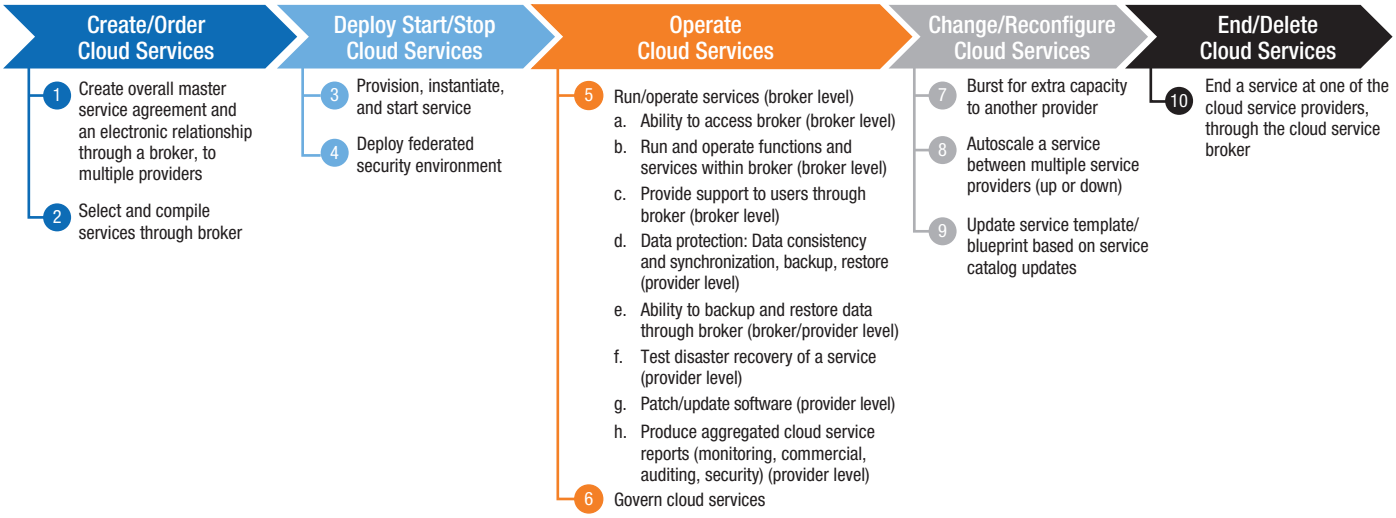

Figure 5. Overview of cloud broker usage scenarios.

Create/Order Cloud Services

Usage Scenario 1 – Create relationship with cloud services broker

Actors
Cloud consumer, cloud subscriber, and cloud broker.

Goals
Establish an electronic relationship through a cloud broker to multiple cloud providers. This establishes a solid foundation for the governance to follow.

Assumptions
- All interactions are API based.
- All commercial and contractual aspects are electronically defined.
- The business strategy for cloud service deployments is defined.
- All required policies for cloud services are defined electronically.
- The consumer has access to a "check-sheet" or set of predefined, menu-options-based commercial service definition input interface to define its service requirements.
- A standard cloud service contract is defined, and procurement processes exist to support the contract.
- The consumer has a relationship with a defined cloud broker, and, in turn, the broker has a defined relationship with a selection of cloud providers.

Success Scenario 1 (instrumented)
The consumer is able to define commercial requirements and pass them to a cloud broker for translation and to perform searches among multiple providers.

The broker is able to create a match between the consumer commercial demand statement and a service created by linking or combining services from one or more providers electronically and at a commercial level.

Failure Condition 1
The broker is not able to interpret the consumer demand statement sufficiently to match it to the commercial offering/s from one or more of the brokers' cloud providers.

Success Scenario 2 (partial)
- The broker is able to match the consumer commercial demand statement to a portion of the service provided by a cloud provider; that is, just the IaaS part of the service, without complete service demand matching.
- Some manual actions are required to satisfy the outstanding part of the demand statement.

Failure Condition 2
The broker is able to interpret part of the commercial demand statement but requires manual interpretation, integration, and mapping to provider offerings.

Failure Handling
For failure 1, review the cloud consumer input interface and update it to align to standard service definitions (including commercial aspects, service aspects, and technology aspects) so that it can be converted and mapped to available offerings from various service providers using a common terminology base.

For failure 2, review the cloud consumer input interface and update it to align to standard service definitions (including commercial aspects, service aspects, and technology aspects), and check whether the correct range of commercial service definitions are available (and advertised electronically) from the cloud provider groups, and update or add providers and services as required.

Usage Scenario 2 – Select and compile cloud services

Actors
Cloud consumer, cloud broker, and cloud provider.

Goals
Select and compile services among multiple pre-identified cloud providers, based on cost, quality, or features, from a broker-provided catalog aligned to the commercial agreement between broker and consumer.

Assumptions
- Cloud consumer provided correct definition for commercial, security, service, and functional requirements.
- Cloud contract and procurement processes exist and are used.
- Federation is facilitated (by a broker) for commercial, services, security, and other required layers to better enable that service requirement.
- The consumer defines requested services based on an agreed service catalog provided by the broker. This may be a federation of provider services, bespoke, restricted, or even include user-defined options.

Success Scenario 1 (instrumented)
- The consumer is able to define its technical and service requirements and pass them to a cloud broker for translation and to perform searches among multiple providers.
- Syntax checks and range limit checks are successful and acceptable from the broker point of view, to both cloud consumer and cloud providers.
- The broker is able to create a match between the consumer demand statement and a service created by linking or combining services from one or more providers, at a technical and service level.

Failure Condition 1
The broker is not able to interpret the consumer demand statement sufficiently to match it to the offering/s from one or more providers.

Failure Handling 1
Review the cloud consumer input interface and update it to align to standard service definitions (including commercial aspects, service aspects, and technology aspects), so that it can be converted and mapped to available technical and service offerings from various service providers, using a common terminology base.

Success Scenario 2 (partial)
- The broker is able to match the consumer demand statement to a portion of the service provided by a cloud provider; that is, just the IaaS part of the service, without complete service demand matching.
- Some manual actions are required to satisfy the outstanding part of the demand statement.

Failure Condition 2
The broker is able to interpret part of the demand statement but requires manual interpretation and mapping to provider offerings.

Failure Handling 2

Review the cloud consumer input interface and update it to align to standard service definitions (including commercial aspects, service aspects, and technology aspects), and check whether the correct range of services are available (and advertised electronically) from the cloud provider groups, and update or add providers and services as required.

Deploy, Start/Stop Cloud Services

Usage Scenario 3 – Deploy, provision, and instantiate cloud service

Actors
Cloud consumer, cloud subscriber, cloud broker, and cloud provider.

Goals
Deploy, provision, instantiate, and start service.

Assumptions

- Cloud provider confirmed resource availability to broker and broker has authorization from cloud consumer to instantiate service with a particular (single, not multiple) provider.
- The service order has been released for automatic deployment. The cloud subscriber cannot make any more changes to the service order. The cloud subscriber has an option to cancel the deployment.

Success Scenario 1
Cloud subscriber releases the service request for automatic deployment.

Steps

1. Cloud consumer issues a defined demand/service request into workflow, which is then approved by the organization.
2. Cloud subscriber releases the service request for automatic deployment to the broker.
3. The service is deployed according to the service definition from the consumers' demand statement.
4. The service is started, and access is provided to the consumer.

Failure Condition 1
The broker submits the service request to the provider but does not receive any further status updates to share with the consumer.

Failure Handling 1
Identify where the service status updates are being lost and route them correctly.

Failure Condition 2
The consumer receives service status updates, but the broker does not.

Failure Handling 2
Review and update the status notification process and engines, as well as the API integration, and correct where needed.

Failure Condition 3
The service is started, but neither the broker nor the consumer can access it due to access or rights issues.

Failure Handling 3
Determine where the restriction is, and reconfigure the access and rights correctly.

Failure Condition 4
The broker or the customer get an error message stating that the service cannot be instantiated or started due to a stated error condition.

Failure Handling 4

- Broker resynchronizes service data in the service catalog.
- The consumer decides whether to reprovision the service.

Usage Scenario 4 – Deploy federated security environment

Actors
Cloud consumer, cloud broker, and cloud provider.

Goals
Deploy federated security environment.

Assumptions

- An agreement exists between the consumer and the broker that facilitates an exchange of security information according to one of the broker models.
- The consumer, broker, and provider have the necessary means and standards-based technology in place to exchange security information and federate environments.
- An agreement exists specifying how providers are selected (precontracted or open public-based on-demand statement), and auditing and control mechanisms are predefined to foster governance of the security environment.

Success Scenario 1 (instrumented)

- A deployed new system is integrated to the consumers' security environment by the consumer granting the broker permission to join the providers' service to the consumers' security domain, enabling the consumer to log on to and access the new service.
- All necessary authorization permissions are in place.
- All audit logs are correctly set.
- All alarming mechanisms (notifications in case of security event) are in place.
- All monitoring mechanisms (such as Get the log, monitor events in real time, and so on) are in place.

Failure Condition 1
The consumer is not able to log on to the new service, because it is not successfully integrated to the consumer's security environment.

Failure Handling 1
An analysis is conducted as to where the security environment integration failed, which is remediated, and the process for future integrations is updated.

Success Scenario 2 (partial)
The system is integrated to the consumers' security environment, and access information is provided to the consumer.

Failure Condition 2
The system is integrated to the consumers' security environment, but the correct access credentials are not identified or provided.

Failure Handling 2
An analysis is conducted to determine where the security environment integration failed, which is remediated, and the process for future integrations is updated, while the access credentials are provided manually for the first failed instance.

Failure Condition 3
All or some of the above-mentioned mechanisms do not set or function properly.

Failure Handling 3

The cloud provider, broker, and consumer analyze and resolve the problem.

Operate Cloud Services

Goal: Run and operate services as a cloud provider.

Usage Scenario 5a – Provide users with access to the broker

Actors
Cloud broker and cloud provider.

Goals
Provide the ability for users to access the broker.

Assumptions

- Users need access to the broker.
- The enterprise or organization hosting the broker has mechanisms to control access to the broker.

Success Scenario 1

- Users within the organization or enterprise will require access to the cloud broker by authenticating against a common Identity provider.
- These providers can include enterprise identity management tools such as directory servers or third-party authentication services.

Failure Condition 1
The users are unable to access the broker despite being authenticated users of the broker.

Failure Condition 2
Unauthenticated users are able to access the broker.

Failure Handling 1 and 2
Identify the source of the problem by checking the connectivity between the broker and the identity provider, as well as the set of users within the identity provider who are supposed to have access to the broker.

Usage Scenario 5b – Provide users with the ability to run and operate functions and services

Actors
Cloud consumer and cloud broker.

Goals
Provide the ability for users of the cloud broker to run and operate the various functions and services within the cloud broker environment.

Assumptions

- Users need access to various functions and services offered by the broker.
- The enterprise or organization hosting the broker requires the broker to have mechanisms to control actions and functions of users within the broker environment.

Success Scenario 1
Users within the organization or enterprise will require access to the cloud broker by using authorizing mechanisms. These authorization mechanisms may include role-based access control or attribute-based access control or some other access control mechanism.

Failure Condition 1
The users are unable to access the service or function even after being provisioned to that service or function.

Failure Condition 2
The users are provided access to the service or function but are not informed about it.

Failure Handling 1 and 2
Compare the set of entitlements given to the users and check it against the audit logs of the broker to identify the discrepancy between the entitlements and the actual access of the function or service to the users.

Usage Scenario 5c – Provide users with the ability to get support for services

Actors
Cloud consumer, cloud broker, and cloud provider.

Goals
Provide the ability for users to get support for the services provisioned to them or administrate services provided to them through the broker.

Assumptions
- Users have access to the broker and have services provisioned to them.
- Users have a mechanism to ask for support from either the broker or the service.

Success Scenario 1
- Users who face issues with either the access to the service or functionality within the service can raise incident requests either through the broker or through offline means.
- Adequate training, in the form of manuals or demos, is provided to the users, enabling them to use the support mechanism.

Failure Condition 1
The mechanism for raising the incident is unavailable.

Failure Condition 2
Users are not informed of the status of the incident when such incidents are raised.

Failure Handling 1 and 2
- An escalation mechanism needs to be in place, either within the system or through an offline mechanism, enabling the users to contact support for addressing their incidents or problems.
- The escalation levels can include support levels provided by the enterprise or third-party support desks or may also include the support desks of the providers.

Success Scenario 2
Users who face issues with functionality within the broker can raise incident requests either through the broker or through offline means.

Failure Condition 1
The mechanism for raising the incident is unavailable.

Failure Condition 2
The users are not informed of the status of the incident when such incidents are raised.

Failure Handling 1 and 2
An escalation mechanism needs to be in place either within the system or through an offline mechanism, enabling the users to contact support for addressing their incidents or problems with the broker.

Usage Scenario 5d – Data protection/restrict access to data

Actors
Cloud consumer, cloud broker, and cloud provider.

Goals
Secure data by restricting access or providing mechanisms to protect data.

Assumptions
- Agreements are signed with all providers when integrating to the provider services.
- API-based interactions are in place for communicating with the service providers.

Success Scenario 1
An agreement is signed with the provider stating the service provider's data protection and security mechanisms, as agreed to with the enterprise that is integrating that service to the broker. Users can rely on these legal agreements as a proxy for application data protection and trust worthiness.

Success Scenario 2
- Authorization mechanisms in place can ensure data access is given based on specific permissions. These include permissions based on access to functions or services or data within the broker.
- Roles can be specified determining who has access to data within the broker and the service—enabled through the use of roles for brokers and service specific roles.
- Roles can be backed up with specific rules or criteria through which users assigned to roles can have access to data within the cloud.

Failure Condition 1
Legal agreements are not followed or authorizations may fail due to incorrect implementation or lack of robust policies governing data protection.

Failure Handling 1
Mechanisms in place to take up disputes with the provider need to be invoked. Implementation issues or incorrect policies in setting up authorization frameworks will need to be checked and improved through an iterative process.

Usage Scenario 5e – Backup and restore data by means of the broker

Actors
Cloud consumer, cloud broker, and cloud provider.

Goals
Establish backup and restoration data services through a broker.

Assumptions
- API-based interactions are established for communicating with the service providers.
- Backup and restore policies are in place to govern backup functionality.

Success Scenario 1
The cloud broker needs to have two levels of policies for backup and restore, specifying:
- What is the type of data to be backed up?
- Who is the provider for the data backup functionality?
- What are the types of services provisioned by the broker that require backups?
- What data protection mechanisms have the provider put in place?
- Does the provider backup-and-restore techniques comply with organizational policies?
- Are the schedules for backup at the organizational and user levels?

Based on the policies defined here, the broker invokes the specified backup on the data within the service provisioned. Policies then determine where the data is backed up to and when and how it can be restored.

Failure Condition 1

- Backup does not take place based on the specified schedule.
- Backup takes place, but the backup is not accessible.
- Backup takes place, but the restore does not work.
- Data backed up does not have integrity.
- Back or restoration takes place beyond the specified service-level agreement (SLA).

Failure Handling 1

- Backup does not take place based on the specified schedule. Check that scheduled jobs are running and fix them if they are not or if improperly configured.
- Backup takes place, but the backup is not accessible. Check the location of the backup and perform the necessary steps with the provider for the restoration of the backup data.
- Backup takes place, but the restore does not work. Check the connectivity and obtain support from the provider, if required.
- Data backed up does not have integrity. Run data integrity tools or take it up with the provider for clauses that can be enforced based on agreements.
- Back or restoration takes place beyond the specified SLA. Take it up with the provider or revise the SLA based on the data type or size or location.

Usage Scenario 5f – Test disaster recovery of service backup and restore data by means of the broker

Actors
Cloud consumer, cloud broker, and cloud provider.

Goals
Test disaster recovery of a service.

Assumptions
Assumes API-based interactions are established.

Success Scenario 1 (instrumented)

- The organization needs to specify the various requirements around the data recovery (DR) for each application or workload within the enterprise.
- These requirements encompass two types:
  - **Recovery time objective** (RTO). The duration of time and the service level to which a business process should be restored after a disaster (or disruption) to avoid unacceptable consequences associated with a break in business continuity. For example, if a disaster occurs at 12:00 p.m. (noon) and the RTO is 8 hours, the DR process would ensure that recovery to the acceptable service level would be possible by 8:00 p.m.
  - **Recovery point objective** (RPO). Describes the acceptable amount of data loss measured in time. For example, if the RPO was 1 hour, after the system was recovered, it would contain all data up to a point in time that is prior to 11:00 a.m. because the disaster occurred at noon.
- The broker should provide a way to enter these values against each service based on the enterprise requirements and take into account the various provider SLAs around the DR practices.
- The DR can then be run by bringing down one service and checking against the policy specified.
- The DR plan should be backed up by the kind of DR to be tested and the appropriate documentation covering the plan specifics and support mechanisms.

Failure Condition 1
The RTO and RPO do not meet the specified criteria.

Failure Handling 1
Identify the failure points and update the DR policy.

Usage Scenario 5g – Patch and update software

Actors
Cloud broker and cloud provider.

Goals
Patch and update software at the provider level.

Assumptions
API-based interactions are established.

Success Scenario 1 (instrumented)

- The cloud broker has the capability to store the index of all the patches and versions of all the software provisioned within the ecosystem of the cloud broker.
- The cloud broker has the ability to define a baseline of the versions for all software based on enterprise policies.
- Users have the ability to view the existing workloads within the system and to apply patches from the patch repository.
- Patches across workloads can be applied as an organization-defined policy schedule or on an ad hoc basis based on user needs.
- Reports and dashboards on the patch and update processes are generated and can be accessed and viewed.

Failure Condition 1
The patch does not get updated correctly.

Failure Handling 1
Raise an incident against the service and identify which patch failed and apply that manually.

Usage Scenario 5h – Produce aggregated cloud services reports

Actors
Cloud broker and cloud provider.

Goals
Produce aggregated cloud service reports (monitoring, commercial, auditing, security) at the provider level.

Assumptions
API-based interactions are established.

Success Scenario 1 (instrumented)
Common reports should be available across cloud brokers. These are subject to the broker/provider/consumer's specific objectives and rationale for producing reports on the cloud services provided. Reports can include:

- **Services.** Service reports give the various users a snapshot of the services that are provisioned and consumed as part of the broker. These reports should cover metrics on both the units of services as well as the costs for services consumed.
  - Units of services consumed
  - Services cost
  - Services onboarded
  - Services depreciated
- **Support.** Support reports provide the various IT service management-related metrics on services provided by the broker. These include support metrics on service provider services or on functionality provided by the broker for operating the service provider services.
  - Number of service requests
  - Number of change requests
  - Number of problems
  - Incident created/resolved/MTTR (mean time to repair)

- **Billing.** Metric reports on the financials of services consumed through the broker.
  - Total cost per service consumed
  - Total value of invoices
  - Total subscriptions billed
- **Audit reports.** Metrics associated with an audit perspective, providing detailed reports on various activities within the broker. This is primarily to meet organizational policies and security norms.
  - Access logs
  - Service logs
  - Administrative logs

Note that the set of reports described are recommendation of the various metrics that a typical cloud broker should capture. The actual set of reports and metrics can vary, based on the model of the broker or the service consumed or the enterprise requirements for the broker.

Also note that for a cloud broker integrated with different service providers (who provide services along with associated metrics), the metrics can be different from each other in terms of content, schema, or in the way they are measured or captured. The broker is expected to take these different sets of data and provide a standardized set and view for the various reports.

Usage Scenario 6 – Govern Cloud Services

Actors
Cloud broker.

Goals
Govern cloud services.

Assumptions
- The cloud broker has the capability to specify IT rules for governance.
- Analysis needs to be performed to interpret the policy and how it affects various processes in the cloud broker.

Success Scenario 1 (instrumented)
- The cloud broker has the ability to store and manage the various governance factors, including policies, business line objectives, and rules.
- The rules are translated to a rules engine present in the broker or a third-party rules engine that the broker leverages.
- These rules can be applied on various objects within the broker, such as users, services, workflows, and so on.

Failure Condition 1
- Rules fail to run or do not run in specified SLAs.

Failure Handling 1
- Consumer is informed of the situation.

Change/Reconfigure Services

Usage Scenario 7 – Bursting for extra capacity

Actors
Cloud broker and cloud provider.

Goals
Bursting for extra capacity can be accomplished through another provider.

Assumptions
- The consumer has purchased access to another provider through the broker.
- The consumer's application has associated metrics that are monitored.
- The above metrics have an SLA established that require additional capacity once an SLA threshold is crossed.
- Capacity can be added manually by means of some interface or programmatically through an API.

Success Scenario 1 (instrumented)
Requested capacity is granted when the SLA passes a defined threshold.

Failure Condition 1
No resources are allocated by the provider to the broker for the consumer.

Failure Handling 1
The consumer is informed of the situation.

Success Scenario 2 (partial)
Some, but not all, of the requested capacity is granted when the SLA passes a defined threshold.

Failure Handling 2
Resources are granted and the users are informed of the shortfall.

Usage Scenario 8 – Autoscale between providers

Actors
Cloud broker and cloud provider.

Goals
Autoscale a service between multiple providers.

Assumptions
- The consumer has access to other providers through the broker.
- The consumer's application has associated metrics that are monitored.
- The above metrics have an SLA established that requires additional capacity once an SLA threshold is crossed (scale up), and there is another SLA that allows removal of capacity once another SLA threshold is crossed (scale down).
- The metrics and metric thresholds for adding to capacity are added manually through some interface or programmatically through an API.

Success Scenario 1 (instrumented)
Consumer receives all of the requested resources when the scale-up SLA thresholds are crossed and has resources removed when the scale-down SLA thresholds are crossed.

Failure Condition 1
Consumer receives no additional resources when scale-up SLA thresholds are exceeded, and it does not give up resources when scale-down SLA thresholds are exceeded.

Failure Handling 1
Consumer is informed of the situation.

Success Scenario 2 (partial)
Consumer receives all of the requested resources when scale-up SLA thresholds are crossed and has some or no resources removed when scale-down SLA thresholds are crossed.

Failure Handling 2
Consumer is informed of the situation.

Success Scenario 3 (partial)
Consumer receives no additional resources when scale-up SLA thresholds are crossed but has resources taken away when scale-down SLA thresholds are crossed.

Failure Handling 3
Consumer is informed of the situation.

Success Scenario 4 (partial)
Consumer receives some of the requested resources when scale up SLA thresholds are crossed but has resources taken away when scale-down SLA thresholds are crossed.

Failure Handling 4
Resources are granted and user is informed of the shortfall.

Usage Scenario 9 – Update service template/service catalog

Actors
Cloud consumer, cloud subscriber, and cloud broker.

Goals
Update service template/blueprint based on service catalog updates.

Assumptions
There is an automated way that the broker can update service templates based on changes from provider service templates. Ideally this would be done programmatically, but that is not required.

Success Scenario 1 (instrumented)
Broker service templates are promptly and completed changed whenever provider service catalogs are changed.

Failure Condition 1
Broker service templates are not changed when provider service catalogs are changed.

Failure Handling 1
Consumer is informed of the situation, and provider forces catalog update.

Success Scenario 2 (partial)
Broker service templates are partially changed when provider service catalogs are changed.

Failure Handling 2
Consumer is informed of the situation, and provider forces complete catalog update.

Success Scenario 3 (partial)
Broker service templates are completely changed when provider service catalogs are changed, but only after a long delay.

Failure Handling 3
Consumer is informed of the situation.

Usage Scenario 10 – End service at a cloud services provider

Actors
Cloud broker and cloud provider.

Goals
End a service at one of the cloud providers through the cloud broker.

Assumptions

- A service exit process is defined in the commercial contract, including a set of steps pertaining to the handling of data, security, and other relevant elements in the service.
- Both the consumer and provider have facilities in place to send and receive the necessary system information to support the defined service exit.
- The necessary auditing and controls are in place to both validate the service exit and review that the exit and service termination has been carried out as per the commercially defined process.

Success Scenario 1 (instrumented)

- The cloud consumer issues an instruction to end and delete a cloud service, and the defined exit processes (as per the contract) are executed automatically. The data is transferred to the consumer, the service is ended, and all resources are returned to the available resource pool at the provider.
- The consumer has a copy of the system data for archiving, and all audits are successfully completed relating to service exit.

Failure Condition 1

- The system is not stopped automatically, and the data is not automatically provided to the consumer.
- Audit data and controls are not performed successfully.

Failure Handling 1

Review the service termination instruction and identify where the problem lies, and remediate the problem (such as in cases in which the consumer or broker have insufficient rights to stop a service). Check the defined audit and control points, and determine how the broker interacts with and translates the audit control information. Then correct the integration so as to generate the necessary reports.

Success Scenario 2 (partial)

- The consumer issues its exit and service termination instruction, and the provider manually hands over a data copy to the consumer through the broker, and then stops the service, deletes the data, and returns the technical resources to the available resource pool.
- A manual audit based on the specific systems' nuances is completed, and documents supporting it are manually completed and exchanged between provider and consumer (that is, data deletion)

Failure Condition 2

- The provider or consumer is not able to pass the necessary data between each other or through the broker.
- Audit data is not available to support the defined processes and controls.

Failure Handling 2

Identify why the consumer and provider are not able to exchange the required data through the broker, and establish a facility to foster this through the broker. Check that sufficient capability exists through the broker to quiesce a service, so that it can be stopped, with all data and transactions committed and written to disk. Complete consistent data sets can then be exported from the provider through the broker to the consumer.

WHAT OPERATING MODEL CHANGES ARE REQUIRED?

Service Management and Governance

The roles and responsibilities of a cloud broker are best described in alignment with the ITIL v3 framework, which remains relevant for cloud services, and in the context of the broker.

The RACI Matrix that follows (Table 5 through Table 8) demonstrates the functional responsibilities for service management in a brokered service context, in which the cloud broker provides value-added services to the cloud consumer. The scenario represents a typical IaaS service.

The elements of the RACI Matrix are as follows:

R = **Responsible** – owns the function

A = to whom "R" is **Accountable** – who must sign-off (approve) the work/function before it is effective

C = to be **Consulted** – has information and/or capability necessary to complete the work/function

I = to be **Informed** – must be notified of the results of the work/function, but need not be consulted

A number of the functions listed in the following can be performed by either the cloud provider or the cloud broker, or both, depending on which cloud broker model has been adopted. For example, in cases in which the cloud broker simply aggregates what the cloud provider offers—making the cloud provider Responsible (R)—the cloud broker may be accountable (A), consulted (C), or simply Informed (I) and the assignment of the elements of the RACI Matrix in the tables will be different from what is presented in this usage model.

The actual element assigned to a particular function (consumer, broker, or provider) in the RACI Matrix in tables 5 through 8 is indicative only. The assignments are based on a default position where the cloud broker offers value-added services to the cloud consumer, in which case the cloud broker is more likely to be Responsible (R) for the function than the cloud provider.

Table 5. Service strategy.

Function	Cloud Consumer	Cloud Broker	Cloud Provider
Financial Management			
Service Valuation	I	A	R
Funding			R
Chargeback	I	A	R
Return on Investment	I	A	R
Service Portfolio Management			
Definition		A	R
Analysis			R
Authorization			R
Charter			R
Demand Management			
Patterns of Business Activity	R		I

Table 6. Service design.

Function	Cloud Consumer	Cloud Broker	Cloud Provider
Service Level Management			
Planning	I	C	R
Capture Service Requirements	R	C	I
Review and Update Operational-Level Agreement	C	R	A
Produce the Service-Level Agreement	C	R	A
Service Catalog Management			
Definition	I	R	C
Scoping	I	R	C
Policy		R	C
Update		R	C
Maintain		R	A
Supplier Management		R	C
Availability Management			
Requirements Definition	C	R	A
Planning	I	C	R
Implementation		C	R
▲ Monitoring	I	C/A	R
Reporting		R	A
IT Service Continuity			
Business Impact Analysis	R	C	I
Requirements Definition	R	A	I
▲ Strategy	R	I/A	A/I
▲ Planning	R	C/A	A/C
▲ Implementation		A/R	R/A
▲ Review	R	C/A	A/C
Invocation	R	A	C
Information Security			
▲ Policy Definition	R	A/I	A
▲ Implementation	A	C/R	R
Monitoring	I	C	R
▲ Analysis	R	C/R/A	A

Note: Rather than create an additional set of detailed RACI charts setting out the many permutations possible, we've added a small triangle in those rows that highlight RACI elements that may have been assigned variably among the cloud consumer, broker, and/or provider.

Table 7. Service transition.

Function	Cloud Consumer	Cloud Broker	Cloud Provider
Service Asset and Configuration			
Planning and Identification	I	C	R
Control	I	C	R
Status Reporting	I	I	R
Verification and Audit	I	I	R
Housekeeping	I	I	R
License Management	R	C	A
Change Management			
Registration and Categorization	C	I	R
Assessment and Authorization	C	I	R
Plan and Control	I	I	R
Schedule Changes	I	I	R
Measurement and Reporting	I	A	R
Service Evaluation	I	R	A
Emergency Change	C	I	R
Release and Deployment			
Planning	C	C	R
Preparation	C	I	R
Build and Test Cycles	C	I	R
Pilot and Deployment	C	I	R
Retirement		I	R
Early Life Support			R
Release Review		C	R
Knowledge Management			
Record and Approve		C	R
Monitoring		I	R

Table 8. Service operation.

Function	Cloud Consumer	Cloud Broker	Cloud Provider
Request Fulfillment			
▲ Logging	R	A/R	I
Monitoring			
Workflow Automation	C	R	A
▲ Fulfillment	I/R	A/R	R/A
Closure	I	R	A
Incident Management			
▲ Identification and Logging	I	I/R	R
Categorize	C	I	R
Prioritize	C	C	R
Diagnose	I	I	R
Resolution and Recovery	I	I	R
Closure	I	I	R
Problem Management			
Detect and Logging	C	I	R
Categorize	C	C	R
Prioritize	C	C	R
Analysis and Diagnosis	I	I	R
Resolution	I	I	R
Closure	I	I	R
Review	C	C	R
Event Management			
Design and Event Modeling	C	C	R
System Configuration		I	R
Response and Closure	I	I	R
Review	C	C	R
Access Management			
Request Logging	R	A	I
Request Verification	C	R	I
Provide Access Rights	A		R
Restrict/Remove Access Rights	A		R
Maintain Roles and Groups	A		R
Associated Functions			
IT Operations Management	I	A	R
Technical Management		C	R
Application Management	R	C	C

Note: Rather than create an additional set of detailed RACI charts setting out the many permutations possible, we've added a small triangle in those rows that highlight RACI elements that may have been assigned variably among the cloud consumer, broker, and/or provider.

Service management is not only a machine-level activity. People are needed to translate machine information between provider, broker, and consumer. Any governance structure should be overlaid with the machine-level information, explaining what it means from the provider side, from the consumer side, and as intermediary—in both directions—with the broker.

For example, if an incident occurs, someone needs to be assigned from each of the groups, taking care of the communications, planning, and coordination of the groups that are involved. This is the case no matter who bears the responsibility. Without this level of human service management overlaid onto technology, misinterpretation, misrepresentation, and ill-informed opinions may occur.

With a well-structured governance framework in place, correct interpretations, priorities, and interventions will help contribute to improve sustainability of the service relationship across the service chain.

KPI Measurements

KPIs are control tools that facilitate the measurement of the following aspects of a service:

- Progress
- Compliance
- Effectiveness
- Efficiency

Measuring these four aspects is a vital part of controlling and improving the process.

KPIs are defined and employed within the context of the metrics tree, as shown in Figure 6.

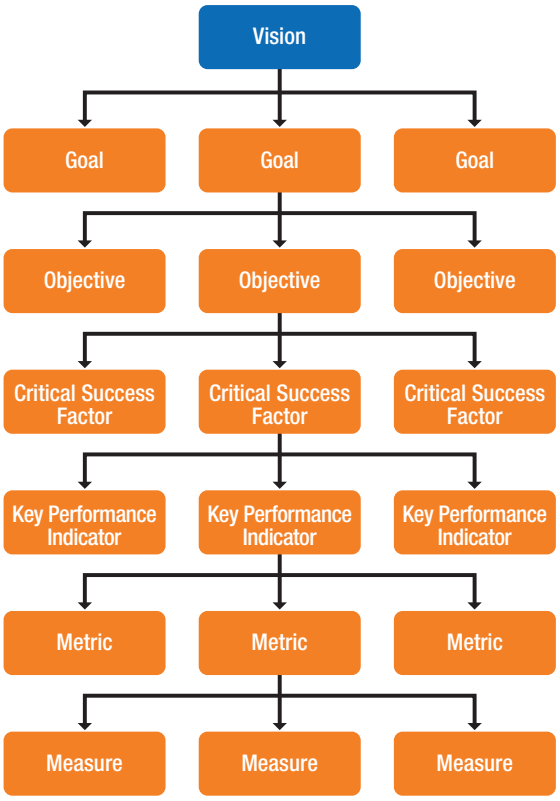

Figure 6. Metrics tree.

A defined KPI has the following five basic elements:

- A basic and clear statement of the KPI
- A formula for calculating the KPI
- Suggested targets and threshold percentages
- A statement, if within targets
- A statement, if below/outside of targets

To measure, control, and improve the services and processes associated with service brokering, both cloud service subscribers and providers should define and employ an appropriate set of KPIs. Within the context of the cloud broker, the following basic KPIs are good candidates for controlling and measuring key aspects of a published, composed, and brokered service:

- Service availability
- The speed/timeliness of execution
- The accuracy of the outputs
- The compliance of the brokered service output(s) with applicable legal and regulatory constraints
- The (financial) cost of the brokered service, including orchestration/execution/decommissioning
- Cloud subscriber satisfaction
- Service execution incident business impact ratio

Table 9 through Table 15 describe these suggested KPIs for the cloud broker.

Table 9. Suggested key performance indicators (KPIs) for service availability.

KPI Parameter	Parameter Value
KPI Statement	Average availability of all services orchestrated by a cloud broker service subscriber.
KPI Calculation Formula	$\frac{\textit{Number of broker-supplied services meeting availability targets}}{\textit{Total number of broker-supplied services}} \times 100\%$
	Comparison of the actual service output(s) versus the published service output(s) to assess conformance.
Suggested Targets	• Target = 100% • Threshold = 90%
If Within Targets	Broker-supplied services are available at levels that meet business needs.
If Below Targets	The services provided by the cloud service broker are providing little value and in extreme cases could be putting business revenue (of the cloud service subscriber) and reputation at risk.

Table 10. Suggested key performance indicators (KPIs) for speed of service execution.

KPI Parameter	Parameter Value
KPI Statement	Percentage conformance of the speed of execution of a cloud broker service against published metrics.
KPI Calculation Formula	$\frac{\textit{Number of milliseconds for atomic cloud service execution}}{\textit{Published time (milliseconds) for atomic cloud service execution}} \times 100\%$
Suggested Targets	• Target = 100% • Threshold = 110%
If Within Targets	Broker-supplied services are executing within time periods that meet business needs.
If Below Targets	The services provided by the cloud broker are taking longer than expected to execute and could in extreme cases be placing time-critical business services at risk.

Table 11. Suggested key performance indicators (KPIs) for accuracy of service execution.

KPI Parameter	Parameter Value
KPI Statement	Conformance of the actual service output(s) against published output(s).
KPI Calculation Formula	Comparison of the actual service output(s) to the published service output(s) to assess conformance.
Suggested Targets	• Target = 100% conformance • Threshold = Any non-conformance/unexpected service output(s)
If Within Targets	Broker-supplied services are accurately delivering the outputs as published by the cloud provider.
If Below Targets	The services provided by the cloud broker that do not conform to their service publication as the actual output(s) are non-conformant. The published services are hence not delivering the required value and can put the business at risk.

Table 12. Suggested key performance indicators (KPIs) for legal/regulatory compliance of service output(s).

KPI Parameter	Parameter Value
KPI Statement	Conformance of the service output(s) with predefined and applicable legal and/or regulatory constraints.
KPI Calculation Formula	Comparison of the actual service output(s) with the legal/regulatory constraint model(s) to assess conformance.
Suggested Targets	• Target = 100% conformance • Threshold = Any non-conformance of service output(s) with legal/regulatory constraints
If Within Targets	Broker-supplied services are operating in a legal/regulatory conformant mode.
If Below Targets	The services provided by the cloud broker do not conform to the applicable legal/regulatory constraints and hence service operation should desist immediately until conformance is established and verified.

Table 13. Suggested key performance indicators (KPIs) for cost of service execution.

KPI Parameter	Parameter Value
KPI Statement	The percentage conformance of the actual cost of service execution to the published price list.
KPI Calculation Formula	$\frac{\textit{Actual cost of service execution}}{\textit{Published price for service execution}} \times 100\%$
Suggested Targets	• Target = 100% • Threshold = 101%
If Within Targets	Broker-supplied services are executing within the agreed price list parameters and allocated budget.
If Above Targets	The costs for service execution are exceeding allocated budget and the published price list and are hence not delivering value for the money.

Table 14. Suggested key performance indicators (KPIs) for rating cloud subscriber satisfaction.

KPI Parameter	Parameter Value
KPI Statement	Average cloud subscriber satisfaction survey score for cloud services.
KPI Calculation Formula	Average cloud subscriber satisfaction survey score.
Suggested Targets	• Target = 10.0 • Threshold = 9.0 *Assumes a 10-point scale, 10 = high and 1 = low*
If Within Targets	Broker-supplied services are effectively meeting the stated needs of the cloud service subscriber.
If Below Targets	The services provided by the cloud broker are viewed as problematic and result in a lack of confidence, by the cloud service subscriber, in their capabilities.

Table 15. Suggested key performance indicators (KPIs) for service execution's incident business impact ratio.

KPI Parameter	Parameter Value
KPI Statement	Incident business impact ratio.
KPI Calculation Formula	$\frac{\textit{Number of incidents resolved}}{\textit{Total number of incidents reported to service desk}} \times 100\%$
Suggested Targets	• Target = 100% • Threshold = 90%
If Within Targets	Broker-supplied services are operating without incident and therefore meeting business needs.
If Below Targets	The services provided by the cloud broker are providing little value (or lack of investment in monitoring tools) and in extreme cases could be putting business revenue (of the cloud service subscriber) and reputation at risk.

CONCLUSION

This paper describes the multiple dimensions of a cloud broker with insights into the various roles and responsibilities involved. Before obtaining cloud-brokering services, the ODCA recommends that an organization first consider its own organizational structure, internal needs, and special differences. Then, on the basis of these considerations, select and structure the appropriate cloud broker model, solution, and approaches.

In some cases the "common" business functions are federated between multiple (somewhat different) business units, and in other organizations these common functions may be completely centralized. Examples of the functions associated with the broker include the IT organization, the procurement function, finances, risk management, and others. We recommend that the organization take these factors into account when developing an appropriate broker function and determining how it can foster the achievement of business goals and objectives. There is no "one size fits all" answer, but the ODCA believes that this paper offers useful insights into the factors to be considered and that it also offers pragmatic guidelines for selecting cloud broker services.

RFI/RFP Requirements

Both cloud consumers and cloud subscribers should actively participate in the initiation of a cloud service through a cloud broker to retain control of cloud service and the associated financial commitments and commercial relationships that may accompany it. In some organizations, the process by which a cloud service is procured may be distributed; in others, it may be centralized. However, in all models a formal procurement function that coordinates financial and commercial obligations with external parties is a recommended best practice. The procurement function may need to review its existing processes to be able to both support cloud services adoption and the associated enablement for the organization.

The ODCA recommends that the following critical requirements be considered and included in requests for proposal (RFPs) and requests for information (RFIs) to cloud brokers and/or cloud providers so that the proposed solutions align with the cloud consumer's internal service governance requirements:

- **Principle requirement.** The solution should work on multiple virtual and non-virtual infrastructure platforms and be standards-based.
- **Service requirement.** Define the expected levels of service and capability to be provided (such as availability, execution speed, and service accuracy).
- **Reporting requirement.** Define the expected reporting to be provided by the cloud broker or cloud provider.
- **Risk and compliance requirement.** Define any relevant risk management and regulatory compliance criteria for service and data security/privacy.
- **Network requirement.** Define any specific network connectivity requirements/restrictions.

The ODCA's online Proposal Engine Assistant Tool (PEAT)[8] tool may serve as a useful reference for cloud consumers and cloud subscribers to identify some of the more detailed requirements that an organization should consider when preparing an RFI or RFP for cloud services. PEAT helps organizations issuing RFPs based on ODCA requirements to quickly identify the ODCA usage models that match hardware, software, and services requirements outlined in an RFP and to easily connect with vendors and providers offering products and solutions.

Summary of Required Industry Actions

From the individual perspectives of cloud brokers, cloud providers, and cloud consumers, we recommend these actions to further the adoption of cloud service brokerages:

- **Brokers**: Provide catalog templates that guide the consumer more accurately in defining their original demand statements.
- **Providers**: Identify and integrate standards and common definitions for service elements and parameters, which brokers can more easily parse and triage for comparison.
- **Consumers:** Demand standards-based services and product definitions, to reduce lock-in and improve portability.

[8] ODCA Proposal Engine Assistant Tool (PEAT). www.opendatacenteralliance.org/ourwork/proposalengineassistant

RESOURCES

For more information, refer to the following resources.

ODCA Usage Models

Find these resources on the ODCA website at www.opendatacenteralliance.org/library

- Open Data Center Alliance[SM] Usage Model: Cloud Maturity Model Rev. 2.0, 2013.
- Open Data Center Alliance[SM] Master Usage Models: Commercial Framework Rev 1.0, 2013.
- Open Data Center Alliance[SM]: Service Catalog Rev. 1.1, 2013.
- Open Data Center Alliance[SM]: Master Usage Model: Service Orchestration Rev 2.0, 2014.

Other Sources

- Barry, D. K., *Web Services, Service-Oriented Architectures, and Cloud Computing*, 2nd ed. Ch. 13, Morgan Kaufmann (2012).
- Clancy, H., "Cloud Integration Brokerage Services Mature" (2014). ZDNet. www.zdnet.com/cloud-integration-brokerage-services-mature-7000028421
- D. C. Plummer and L. F. Kenney, "Three Types of Cloud Brokerage Will Enhance Cloud Services" (2009). Gartner. www.gartner.com/doc/973412
- Moore, J., "Cloud Service Brokerages Emerge As New Integrators" (2012). CIO. www.cio.com/article/2389837/value-added-resellers/cloud-service-brokerages-emerge-as-new-integrators.html
- Plummer, D., "Cloud Services Brokerage: A Must-Have for Most Organizations" (2012). Forbes. www.forbes.com/sites/gartnergroup/2012/03/22/cloud-services-brokerage-a-must-have-for-most-organizations
- Sarbazo-Azad, H., and A. Y. Zomaya (editors), *Large Scale Network-Centric Distributed Systems.* Chapter 15: A Cloud Broker Architecture for MultiCloud Environments, Wiley-IEEE Press (2013).