

NIST Cloud Computing Reference Architecture

Version 1

March 28, 2011

Summary of Major Changes

- Add cloud broker
- Add cloud auditor
- Change “cloud service distributor” to “cloud carrier”
- Change “cloud service consumer” to “cloud consumer”
- Remove cloud service developer
- Cloud consumer: Change the subgroups to be “XaaS consumer”, add a table to show example users
- Cloud provider: Change the service orchestration diagram (with a new three-layer cloud infrastructure model: physical resource layer /resource abstraction and control layer /service Layer); combine business support and operational support to be cloud service management; move security and privacy to be at the same level with cloud service management
- Cloud carrier: Add transport agent
- Update the combined conceptual model diagram

Objective

- The objective is to define a neutral reference architecture consistent with NIST Definition of Cloud Computing that:
 - Represents the three service models (*Software as a Service (SaaS)/Platform as a service (PaaS)/Infrastructure as a Service(IaaS)*), four deployment models (*private cloud/community cloud/public cloud/hybrid cloud*), and five essential characteristics (*on-demand self-service/broad network access/resource pooling/rapid elasticity/measured service*)
 - Relates different cloud services and maps them to the overall model
 - Serves as a roadmap for IT to understand, select, design and/or deploy cloud infrastructures
- This report presents the first version of the NIST Cloud Computing Reference Architecture.

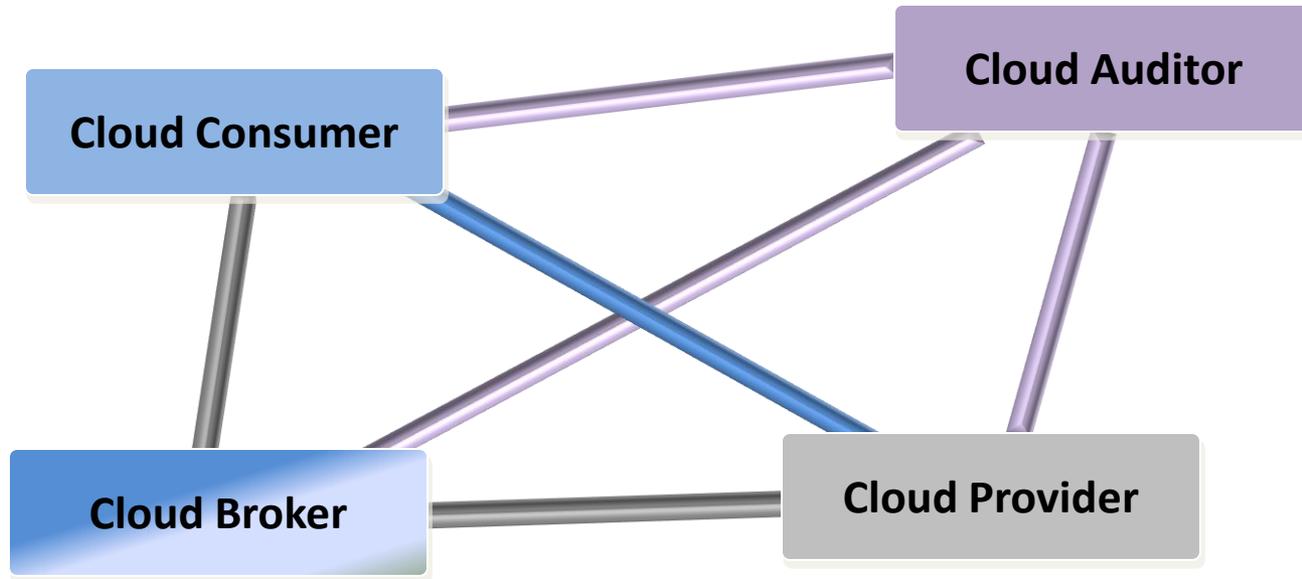
NIST Cloud Computing Reference Architecture

- Top-Level View

- The NIST Cloud Computing Reference Architecture consists of five major **actors**. Each actor plays a **role** and performs a set of **activities** and **functions**. The reference architecture is presented as successive diagrams in increasing level of detail.
- Among the five actors, cloud brokers are optional, as cloud consumers may obtain service directly from a cloud provider.

Actor	Definition
Cloud Consumer	Person or organization that maintains a business relationship with, and uses service from, <i>Cloud Providers</i> .
Cloud Provider	Person, organization or entity responsible for making a service available to <i>Cloud Consumers</i> .
Cloud Auditor	A party that can conduct independent assessment of cloud services, information system operations, performance and security of the cloud implementation.
Cloud Broker	An entity manages the use, performance and delivery of cloud services, and negotiates relationships between <i>Cloud Providers</i> and <i>Cloud Consumers</i> .
Cloud Carrier	The intermediary that provides connectivity and transport of cloud services from <i>Cloud Providers</i> to <i>Cloud Consumers</i> .

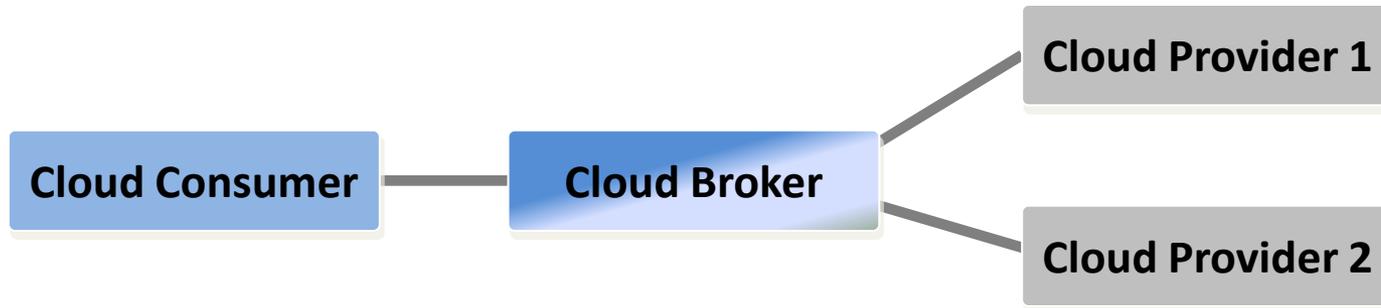
Interactions between the Actors in Cloud Computing



-  The communication path between a cloud provider and a cloud consumer
-  The communication paths for a cloud auditor to collect auditing information
-  The communication paths for a cloud broker to provide service to a cloud consumer

Example Usage Scenarios

- Scenario 1: A cloud consumer may request service from a cloud broker instead of contacting a cloud provider directly. The cloud broker may create a new service by combining multiple services or enhance an existing service. In this example, the cloud providers are invisible to the cloud consumer.



Example Usage Scenarios

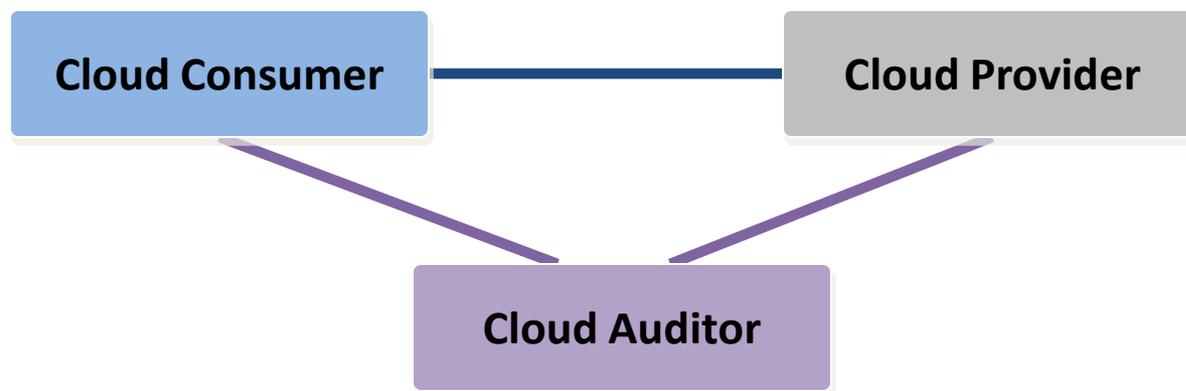
- Scenario 2: Cloud carriers provide connectivity and transport of cloud services from cloud providers to cloud consumers. A cloud provider will set up SLAs with a cloud carrier and may request dedicated and encrypted connections.



- SLA between cloud consumer and cloud provider
- SLA between cloud provider and cloud carrier

Example Usage Scenarios

- Scenario 3: For a cloud service, a cloud auditor conducts independent assessments of the operation and security of the cloud service implementation.



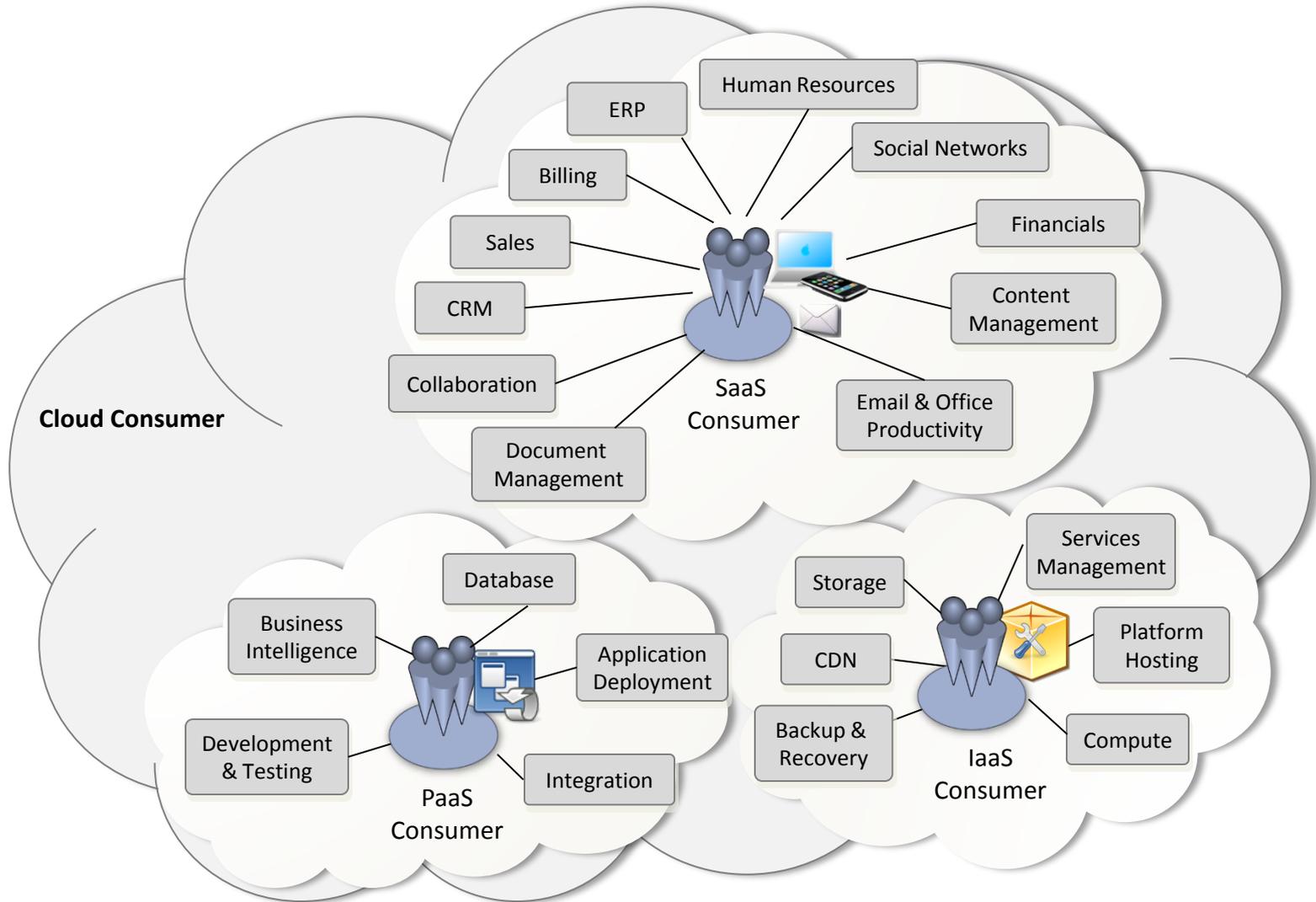
Cloud Consumer

- **Cloud Consumer:** Person or organization that maintains a business relationship with, and uses services from, *Cloud Providers*.
- Cloud consumers are categorized into three groups based on their different application/usage scenarios.

Consumer Type	Major Activities	Example Users
SaaS	Uses application/service for business process operations	Business users, software application administrators
PaaS	Develops, tests, deploys and manages applications hosted in a cloud environment	Application developers, testers and administrators
IaaS	Creates/installs, manages and monitors services for IT infrastructure operations	System developers, administrators, IT managers

- Some example cloud services available to a cloud consumer are listed in the following diagram.

Example Services Available to a Cloud Consumer



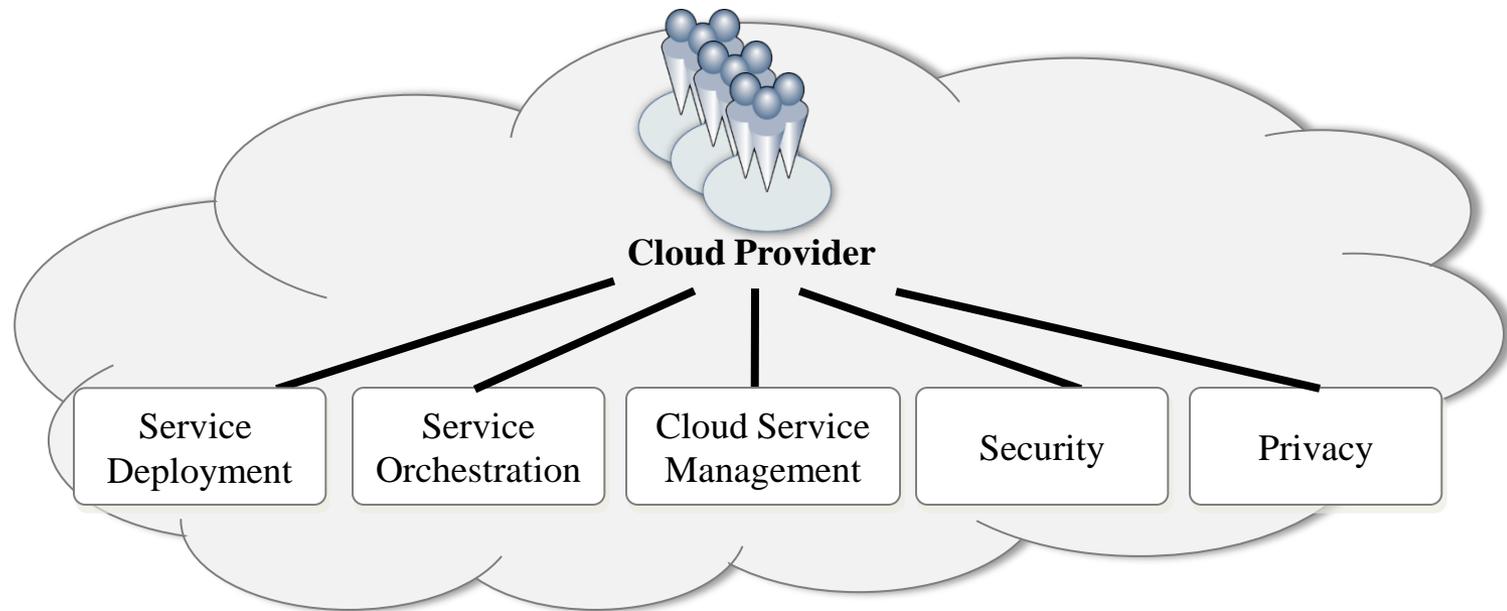
Cloud Provider

- **Cloud Provider:** Person, organization or entity responsible for making a service available to *Cloud Consumers*.
- Cloud providers perform different tasks for different service models.

Provider Type	Major Activities
SaaS	Installs, manages, maintains and supports the software application on a cloud infrastructure.
PaaS	Provisions and manages cloud infrastructure and middleware for the platform consumers; provides development, deployment and administration tools to platform consumers.
IaaS	Provisions and manages the physical processing, storage, networking and the hosting environment and cloud infrastructure for IaaS consumers.

- The activities of cloud providers are discussed in greater detail from the perspectives of *Service Deployment, Service Orchestration, Cloud Service Management, Security and Privacy*.

Cloud Provider - Top-level View



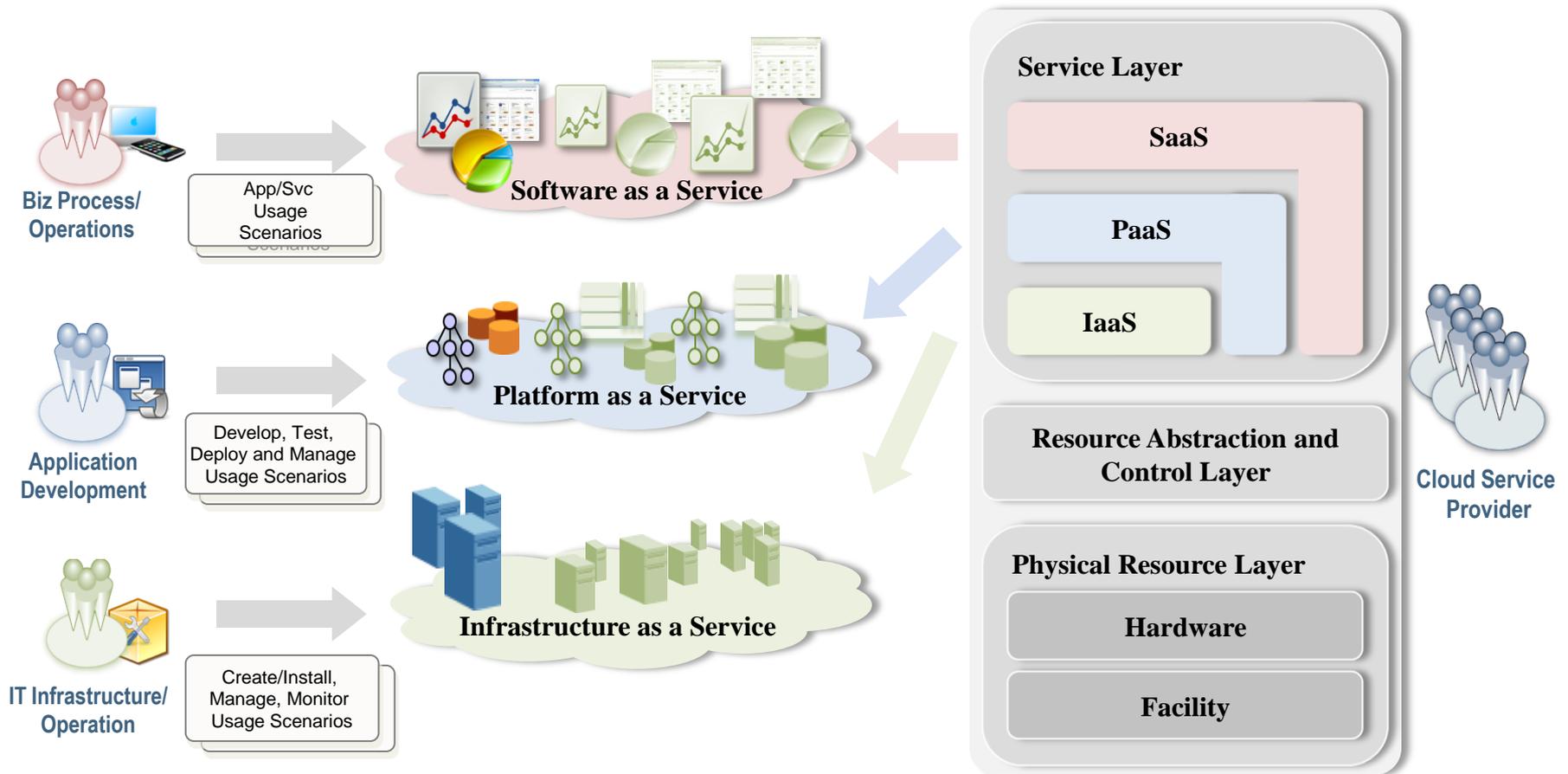
Cloud Provider – Service Deployment

- A cloud system can be operated in one of the following four deployment models:
 - **Private cloud:** The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise.
 - **Community cloud:** The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on premise or off premise.
 - **Public cloud:** The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.
 - **Hybrid cloud:** The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

Cloud Provider – Service Orchestration

- **Service Orchestration** refers to the arrangement, coordination and management of cloud infrastructure to provide different cloud services to meet IT and business requirements.
- The three conceptual layers of a generalized cloud environment:
 - **Service Layer:** Defines the basic services provided by cloud providers
 - **SaaS** : Deployed applications targeted towards end-user software clients or other programs, and made available via the cloud.
 - **PaaS:** Services for consumers to develop and deploy applications onto the cloud infrastructure, including application containers, application development tools, database management systems, etc.
 - **IaaS:** The provisioning of processing, storage, networks, and other fundamental computing resources upon which cloud consumers can deploy and run applications on the cloud infrastructure.
 - **Resource Abstraction and Control Layer**
 - Entails software elements, such as hypervisor, virtual machines, virtual data storage, and supporting software components, used to realize the infrastructure upon which a cloud service can be established, and the associated function modules that manage the abstracted resources to ensure efficient, secure and reliable usage.
 - While virtual machine technology is commonly used at this layer, other means of providing the necessary software abstractions are not precluded.
 - **Physical Resource Layer:** Includes all the physical resources, such as:
 - **Hardware:** Computers (CPU, memory), network (router, firewall, switch, network link and interface), storage components (hard disk), and other physical computing infrastructure elements.
 - **Facility** : HVAC, power, communications, and other aspects of the physical plant.

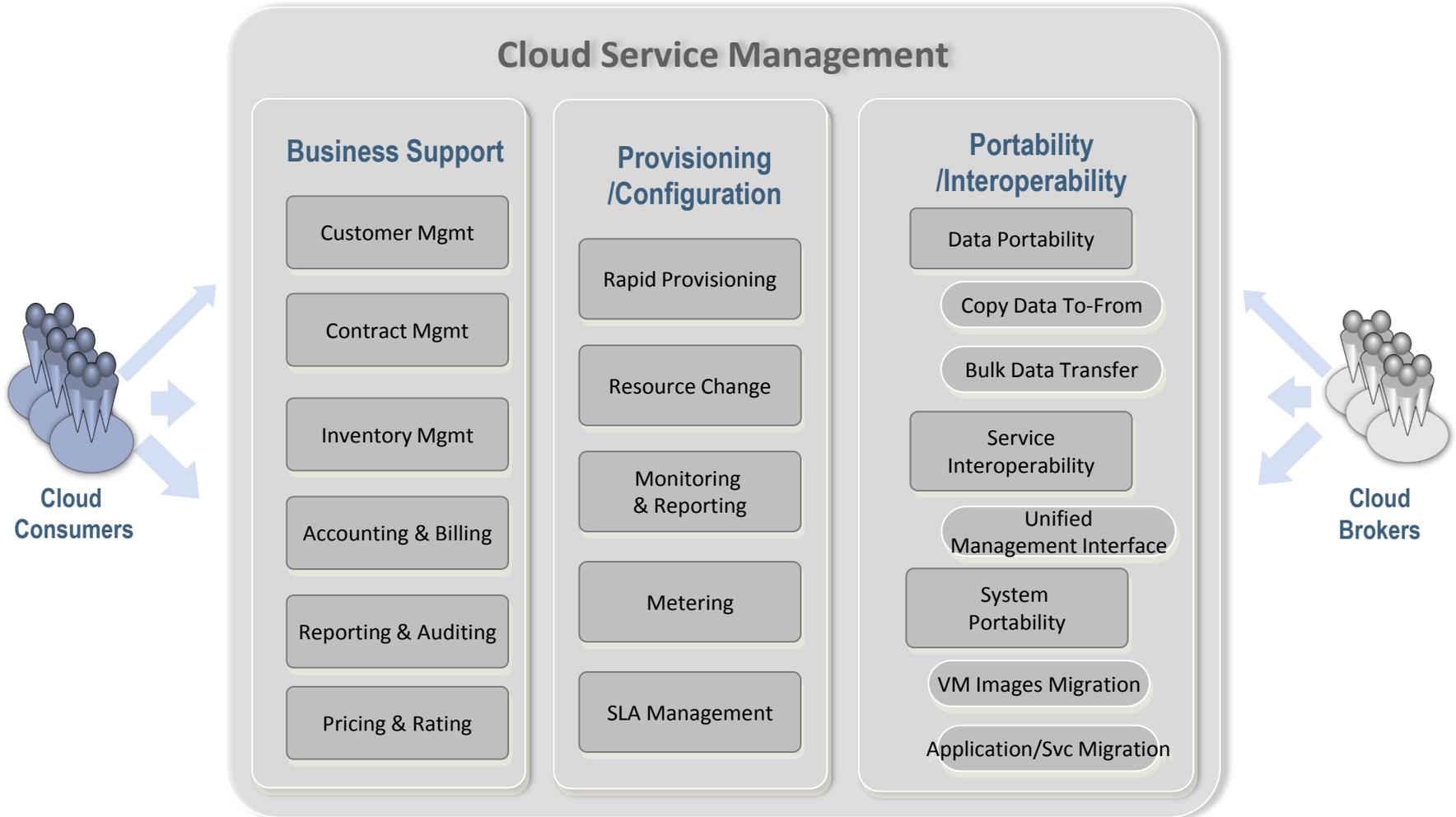
Cloud Provider – Service Orchestration



Cloud Provider – Cloud Service Management (1)

- **Cloud Service Management** includes all the service-related functions that are necessary for the management and operations of those services required by or proposed to cloud consumers.
- A cloud provider performs the following functions to support cloud service management: *Business Support, Provisioning/Configuration, and Portability/Interoperability.*

Cloud Provider – Cloud Service Management (2)



Cloud Provider – Cloud Service Management (3)

- **Business Support:** Entails the set of business-related services dealing with clients and supporting processes such as taking orders, processing bills, and collecting payments. It includes the components used to run business operations that are client-facing.
 - *Customer management:* Manage customer accounts, open/close/terminate accounts, manage user profiles, manage customer relationships by providing point-of-contact and resolution for customer issues and problems, etc.
 - *Contract management:* Manage service contract, setup/close/terminate contract, etc.
 - *Inventory Management:* Set up and manage service catalogs, etc.
 - *Accounting and Billing:* Manage customer billing information, send billing statements, process received payments, track invoices, etc.
 - *Reporting and Auditing :* Monitor user operations, generate reports, etc.
 - *Pricing and Rating:* Evaluate cloud services and determine prices, handle promotions and pricing rules that depend on a user's profile, etc.

Cloud Provider – Cloud Service Management (4)

- *Provisioning/Configuration*
 - *Rapid provisioning*: Automatically deploying cloud systems based on the requested service/resources/capabilities.
 - *Resource changing*: Adjusting configuration/resource assignment for repairs, upgrades and joining new nodes into the cloud.
 - *Monitoring and Reporting*: Discovering and monitoring virtual resources, monitoring cloud operations and events and generating performance reports.
 - *Metering*: Providing a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts).
 - *SLA management*: Encompassing the SLA contract definition (basic schema with the QoS parameters), SLA monitoring and SLA enforcement according to defined policies.

Cloud Provider – Cloud Service Management (5)

- *Portability/Interoperability:*
 - **Portability:** 1. The ability to transfer data from one system to another without being required to recreate or reenter data descriptions or to modify significantly the application being transported. 2. The ability of software or of a system to run on more than one type or size of computer under more than one operating system. [Federal Standard 1037C]
 - **Interoperability:** The capability to communicate, execute programs, or transfer data among various functional units under specified conditions. [ANS/DIT]
 - Cloud Providers should provide mechanisms to support:
 - *Data Portability*
 - *Copy data to-from:* Copy data objects into/out of a cloud.
 - *Bulk data transfer:* Use a disk for bulk transfer.
 - *Service Interoperability*
 - Allow cloud consumers to use their data and services across multiple cloud providers with a unified and enhanced management interface.
 - *System portability*
 - *VM images migration:* Migrate a fully-stopped VM instance or machine image from one provider to another provider.
 - *Application/Service migration:* Migrate application/service and current contents from one service provider to another provider.

Cloud Providers – Security & Privacy

- Security

- *Authentication and Authorization*: Authenticate and authorize cloud consumers using credentials that have been established previously.
- *Availability*: Ensure timely and reliable access to and use of information.
- *Confidentiality*: Protect the confidentiality of the data objects written into clouds by preserving authorized restrictions on access and disclosure.
- *Identity management*: Enforce identity and access control policies on users accessing cloud.
- *Integrity*: Guard against improper information modification or destruction, and include ensuring information non-repudiation and authenticity.
- *Security monitoring & Incident Response*: Conduct ongoing automated monitoring of the cloud provider infrastructure to demonstrate compliance with cloud-consumer security policies and auditing requirements.
- *Security policy management*: Configure/generate/enforce/audit/update security policies on users accessing clouds.

- Privacy

- Protect the assured, proper, and consistent collection, processing, communication, use and disposition of personal and personally identifiable information (PII) information on the cloud.

Cloud Auditor

- **Cloud Auditor:** A party that can conduct independent assessment of cloud services, information system operations, performance and security of the cloud implementation.
- A cloud auditor can evaluate the services provided by a cloud provider in terms of *security controls, privacy impact, performance, etc.*
 - For security auditing, a cloud auditor can make an assessment of the security controls in the information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.
- Auditing is especially important for federal agencies and “agencies should include a contractual clause enabling third parties to assess security controls of cloud providers” (by Vivek Kundra, *Federal Cloud Computing Strategy, Feb. 2011.*).

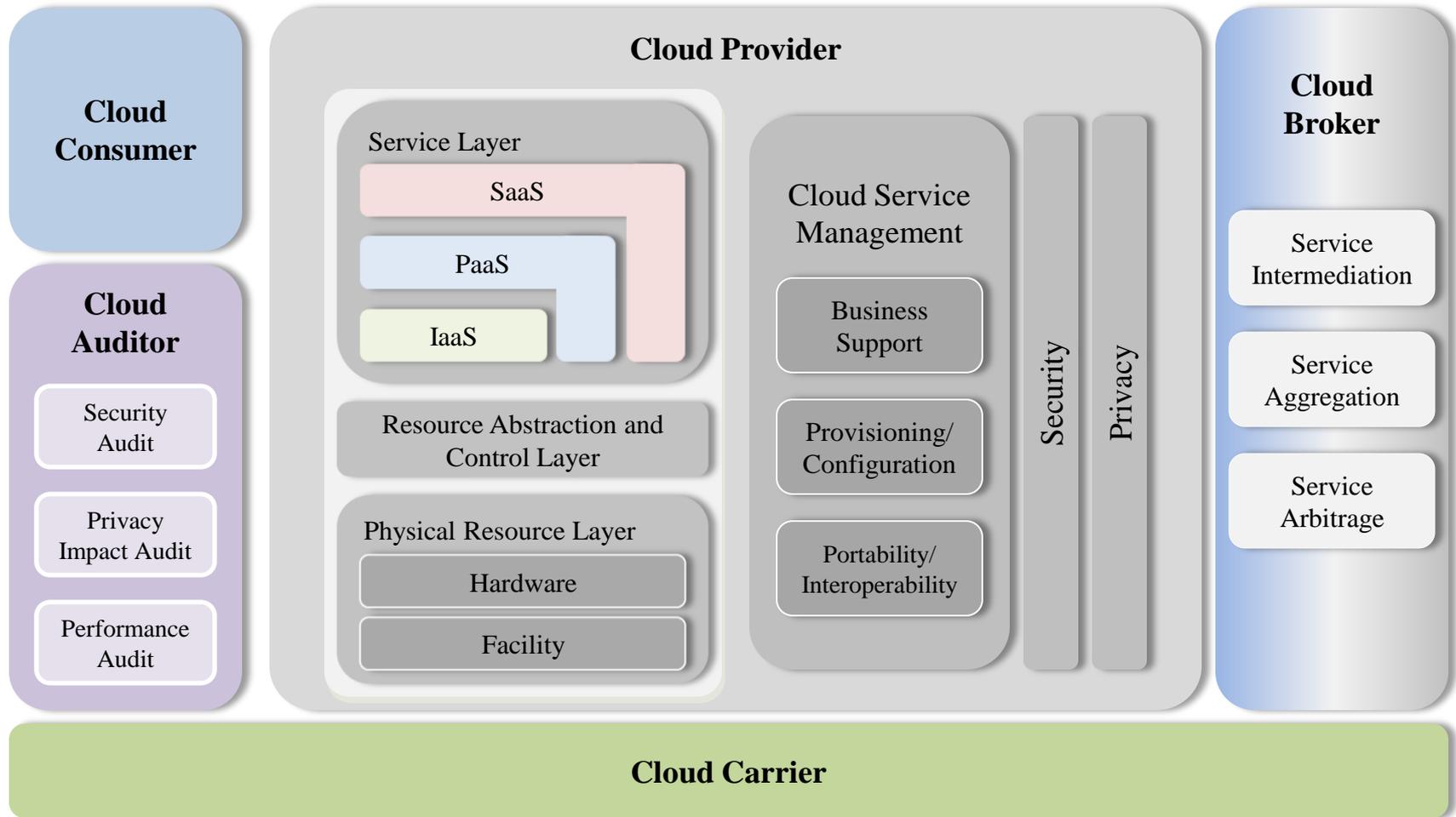
Cloud Broker

- **Cloud Broker:** An entity that manages the use, performance and delivery of cloud services and negotiates relationships between *Cloud Providers* and *Cloud Consumers*.
- As cloud computing evolves, the integration of cloud services can be too complex for cloud consumers to manage.
- The major services provided by a cloud broker include:
 - **Service Intermediation:** An intermediation broker provides a service that directly enhances a given service delivered to one or more service consumers, essentially adding value on top of a given service to enhance some specific capability. Examples of the added services include:
 - **Service Aggregation:** An aggregation brokerage service combines and integrates multiple services into one or more new services. It will ensure that data are modeled across all component services and integrated as well as ensuring the movement and security of data between the service consumer and multiple providers.
 - **Service Arbitrage:** Cloud service arbitrage is similar to cloud service aggregation. The difference between them is that the services being aggregated aren't fixed. Indeed, the goal of arbitrage is to provide flexibility and opportunistic choices for the service aggregator, e.g., providing multiple e-mail services through one service provider or providing a credit-scoring service that checks multiple scoring agencies and selects the best score.

Cloud Carrier

- **Cloud Carrier:** The intermediary that provides connectivity and transport of cloud services between *Cloud Providers* and *Cloud Consumers*.
 - Provide access to cloud consumers through network, telecommunication and other access devices.
 - Example: Network access devices include computers, laptops, mobile phones, mobile internet devices (MIDs), etc.
 - Distribution can be provided by network and telecomm carriers or a transport agent.
 - **Transport agent:** A business organization that provides physical transport of storage media such as high-capacity hard drives.
 - A cloud provider shall set up SLAs with a cloud carrier to provide a consistent level of service. In general, the cloud carrier may be required to provide dedicated and encrypted connections.

The Combined Conceptual Reference Diagram



Reference

- NIST SP 800-145, “A NIST definition of cloud computing”, http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145_cloud-definition.pdf
- NIST SP 800-144, “Guidelines on Security and Privacy Issues in Public Cloud Computing”, http://csrc.nist.gov/publications/drafts/800-144/Draft-SP-800-144_cloud-computing.pdf
- NIST SP 800-146, “NIST Cloud Computing Synopsis and Recommendations”, *manuscript*.
- Federal Cloud Computing Strategy, <http://www.cio.gov/documents/Federal-Cloud-Computing-Strategy.pdf>
- NIST cloud computing use cases, <http://collaborate.nist.gov/twiki-cloud-computing/bin/view/CloudComputing/UseCaseCopyFromCloud>
- IETF internet-draft, “Cloud Reference Framework”, <http://www.ietf.org/id/draft-khasnabish-cloud-reference-framework-00.txt>
- IBM, “Cloud Computing Reference Architecture v2.0”, <http://www.opengroup.org/cloudcomputing/doc.tpl?CALLER=documents.tpl&dcat=15&gdid=23840>
- GSA, “Cloud Computing Initiative Vision and Strategy Document (DRAFT)”, http://info.apps.gov/sites/default/files/Cloud_Computing_Strategy_0.ppt
- Gartner, “Gartner Says Cloud Consumers Need Brokerages to Unlock the Potential of Cloud Services”, <http://www.gartner.com/it/page.jsp?id=1064712>.
- Cloud Taxonomy, <http://cloudtaxonomy.opencrowd.com/>
- OASIS, the charter for the OASIS Privacy Management Reference Model Technical Committee, <http://www.oasis-open.org/committees/pmrm/charter.php>
- Open Security Architecture (OSA), “Cloud Computing Patterns”, <http://www.opensecurityarchitecture.org/cms/library/patternlandscape/251-pattern-cloud-computing>
- Juniper Networks, “Cloud-ready Data Center Reference Architecture”, www.juniper.net/us/en/local/pdf/reference-architectures/8030001-en.pdf