A Strawman Model v2

NIST Cloud Computing Reference Architecture and Taxonomy Working Group

February 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
- Present the actors with two-tier diagram
- Cloud consumer: Change the subgroups to be “XaaS consumer”, add a table to show example users
- Cloud provider: Update service orchestration diagram (the five cloud infrastructure layers); Add interfaces to support interoperability
- Cloud carrier: Add transport agent
- Add a combined conceptual model diagram

Objective

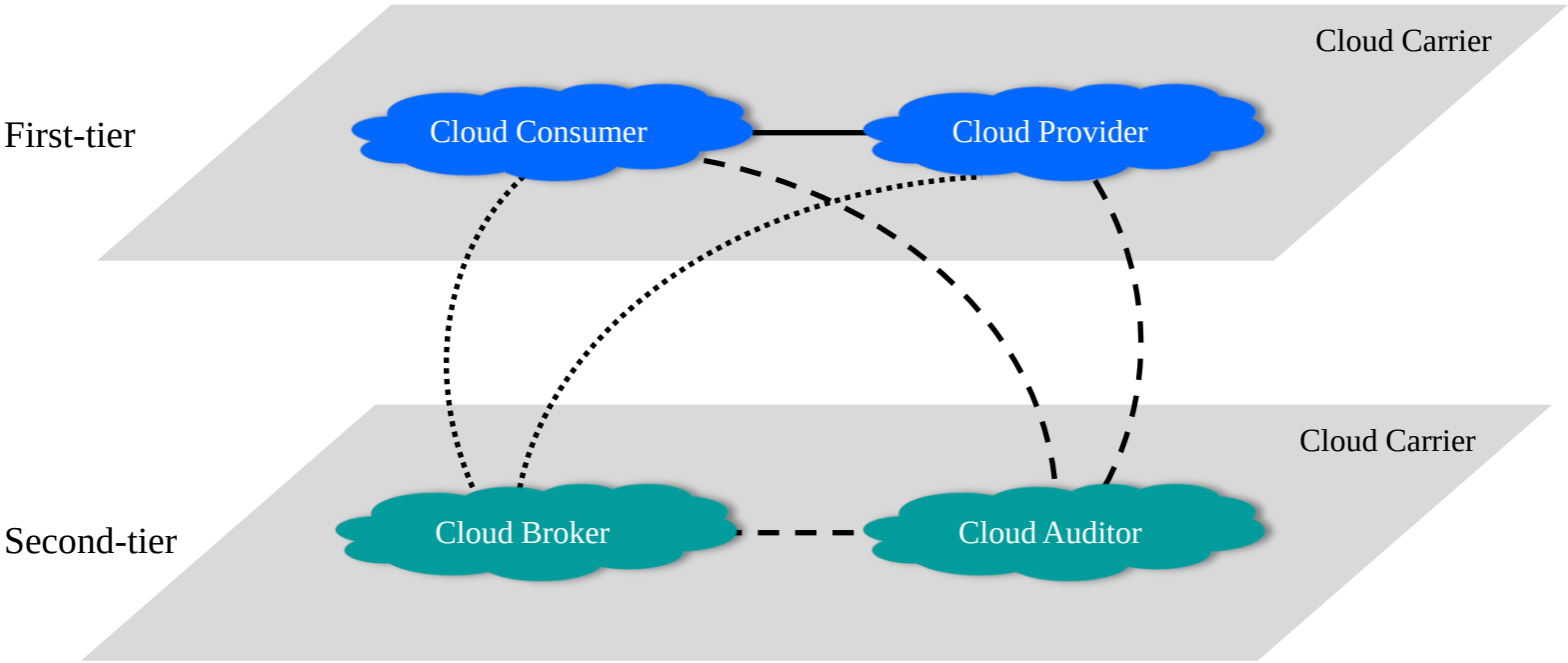
- Our objective is to define a neutral reference architecture consistent with NIST definition of cloud computing that:
  - Represents the three service models (*Software as a Service (SaaS)/Platform as a service (PaaS)/Infrastructure as a Service(IaaS)*), four deployment models (*private cloud/community 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 map them to the overall model
  - Serves as a roadmap for IT to understand, select, design and/or deploy cloud infrastructures

- In this report, we present our second version of a neutral cloud computing reference architecture.

Cloud Computing Conceptual Model - Top-Level View

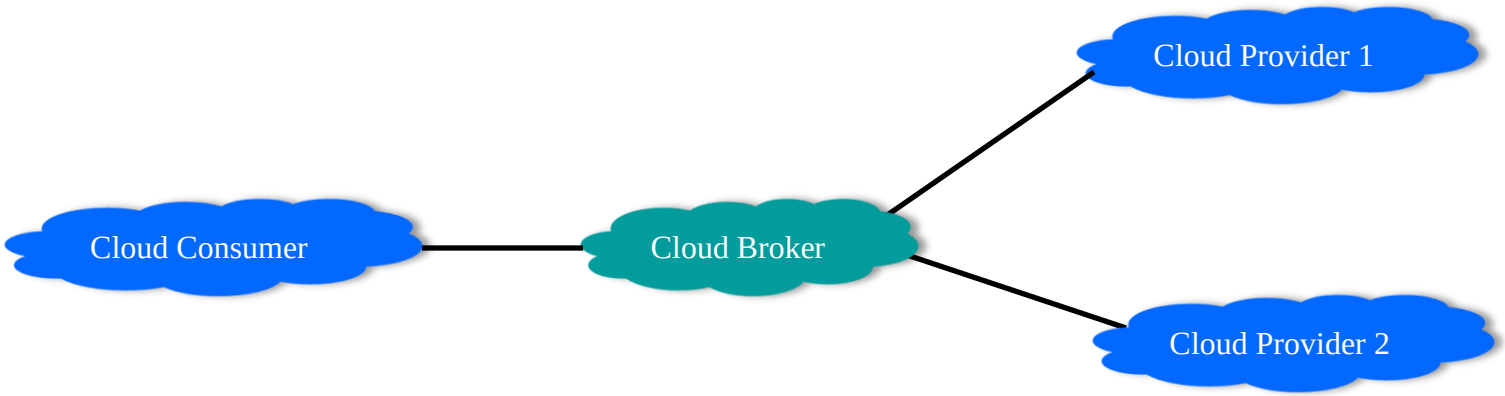
- The cloud computing conceptual model is presented as successive diagrams of increasing level of detail. The conceptual model consists of five major actors in two tiers.
- ***First-tier actors:*** The core actors in all usage scenarios
  - ***Cloud Consumer***: Person or organization that maintains a business relationship with, and uses service from, *Cloud Providers*.
  - ***Cloud Provider*****:** Person, organization or higher-level system responsible for making a service available to *Cloud Consumers*.
- ***Second-tier actors:*** The supporting actors that assist in implementing cloud services. Actors in this tier are not required or not that critical for every cloud application.
  - ***Cloud Broker:*** An entity that manages the use, performance and delivery of cloud services, and negotiates relationships between *Cloud Providers* and *Cloud Consumers*.
  - ***Cloud Auditor:*** A third-party that can conduct independent auditing of the cloud services, information system operation and determine the security of the cloud implementation.
- ***Intermediary actor:***
  - ***Cloud Carrier:*** The intermediary that provides connectivity and transport of cloud services.

Cloud Computing Conceptual Model - Top-Level View



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 combine multiple services into one new service, and/or enhance the service by adding value. In this example, the cloud providers are invisible to the cloud consumer.

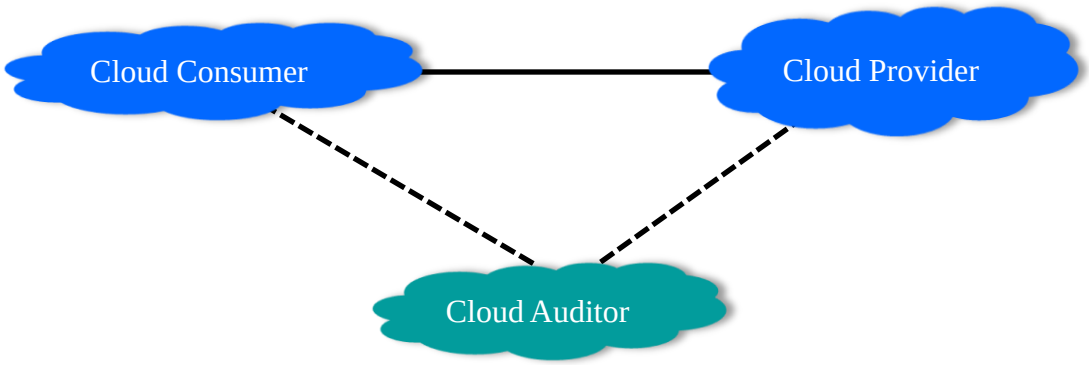


Example Usage Scenarios

- 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, but may request value-added dedicated and encrypted connections.

Example Usage Scenarios

- Scenario 3: For an application deployed in the cloud, a third-party cloud auditor may be required to determine the security of the cloud implementation and conduct independent audits of the operations.



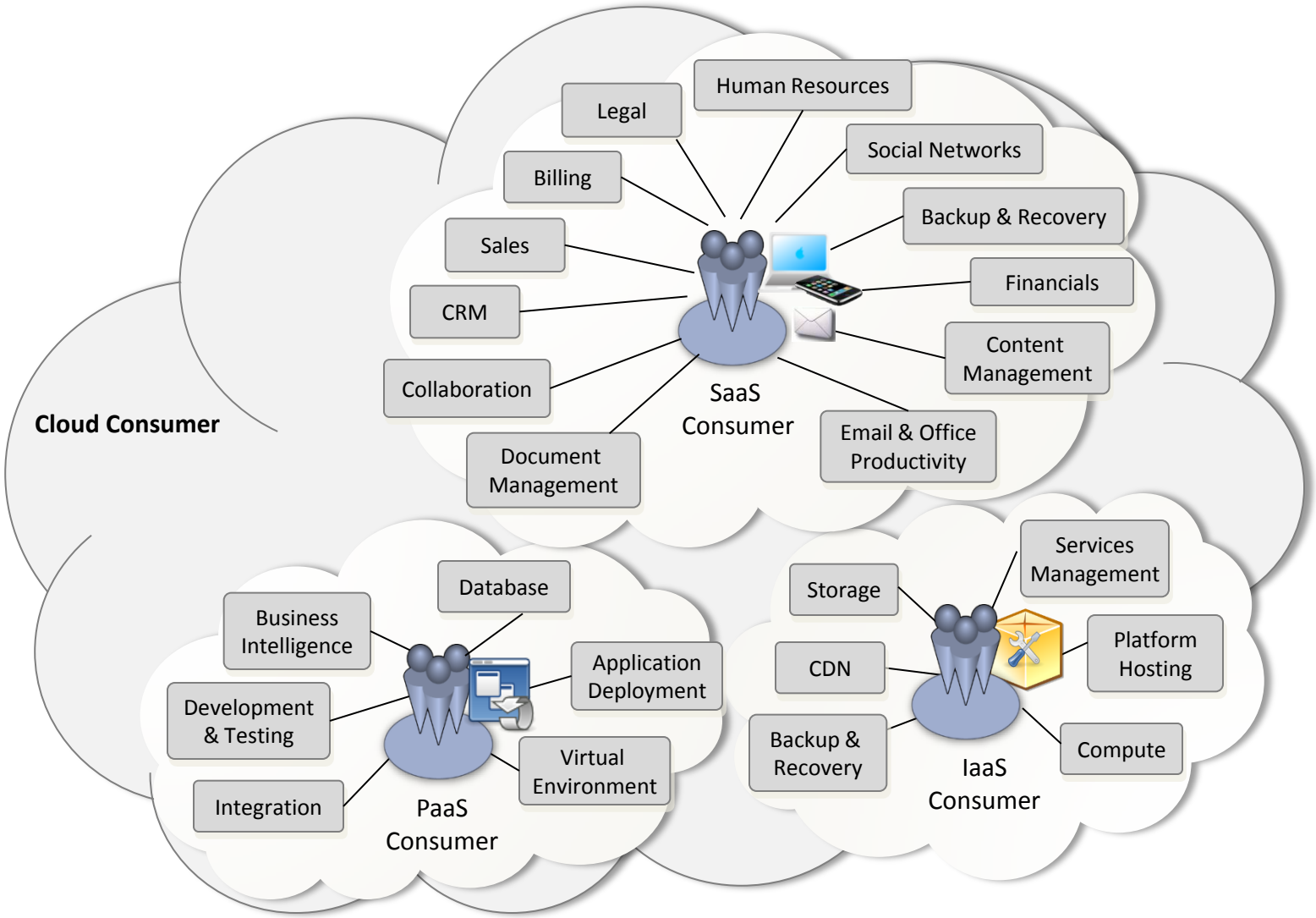
Cloud Consumer

- ***Cloud Consumer***: Person or organization that maintains a business relationship with, and uses service 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 biz process operations	Biz users
PaaS	Develops, tests, deploys and manages services for application development.	Software developers, system developers, CIOs, IT managers
IaaS	Creates/installs, manages and monitors services for IT infrastructure operations.	System developers, IT managers

- Some example usage scenarios are listed in the following diagram.
- Ref:
  - Cloud Taxonomy, http://cloudtaxonomy.opencrowd.com/
  - GSA, "Cloud Computing Initiative Vision and Strategy Document (DRAFT)", http://info.apps.gov/sites/default/files/Cloud_Computing_Strategy_0.ppt

Typical Services Available to a Cloud Consumer



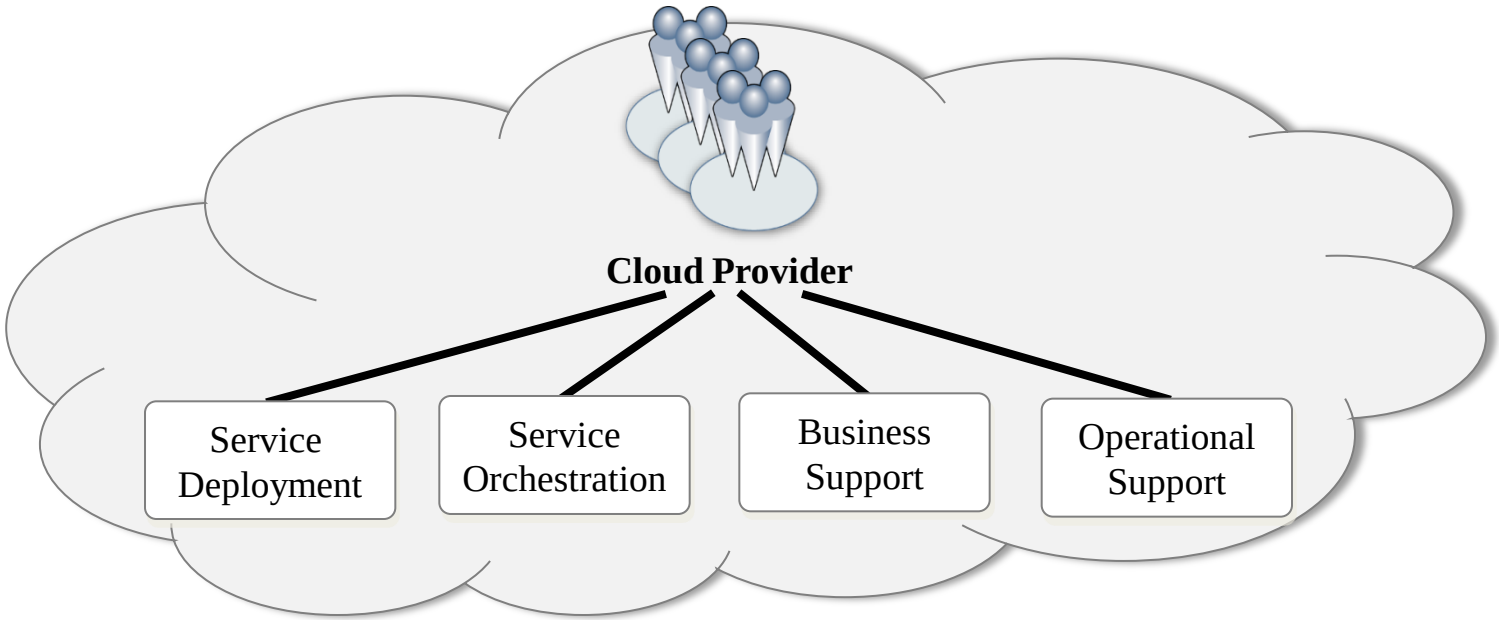
Cloud Provider

- ***Cloud Provider*:** Person, organization or higher-level system responsible for making a service available to *Cloud Consumers*
- The providers perform different tasks for different service types.

Provider Type	Major Activities
SaaS	Installs, manages, maintains and supports the software
PaaS	Manages cloud infrastructure and other middleware the for the platform
IaaS	Maintains the storage, networking and the hosting environment for virtual machines

- The operations of service providers are discussed in further details from the following perspectives: *Service Deployment*, Service Orchestration, *Business Support* and *Operational Support*.

Cloud Provider - Top-level View



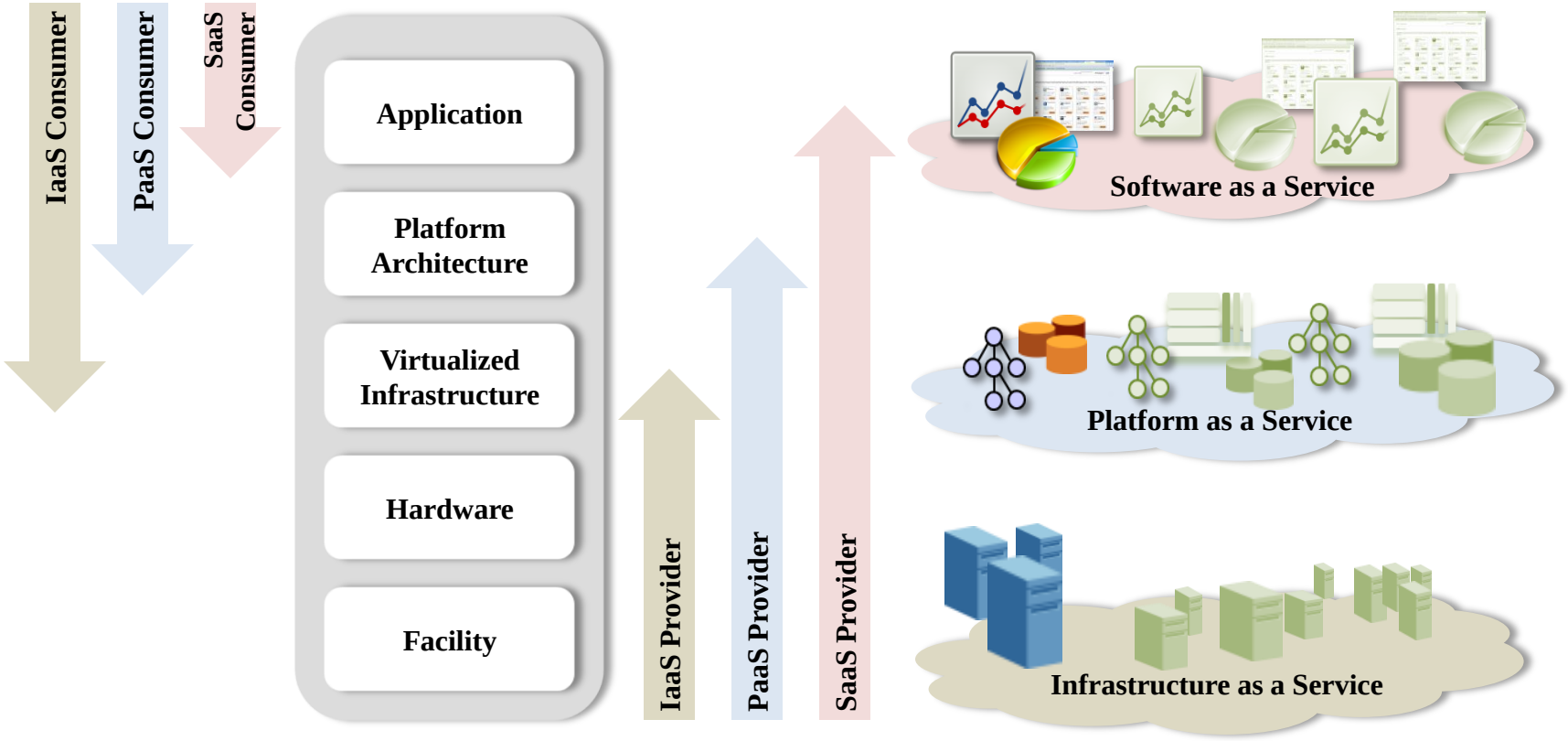
Cloud Provider – Service Deployment

- Cloud infrastructure is operated in 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).
- Ref:
  - NIST definition of cloud computing v15, *www.nist.gov/itl/cloud/upload/cloud-def-v15.pdf*.

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 five conceptual layers of a generalized cloud environment:
  - ***Facility Layer:*** Heating, ventilation, air conditioning (HVAC), power, communications, and other aspects of the physical plant comprise the lowest layer, the facility layer.
  - ***Hardware Layer:*** Includes computers (CPU, memory), network (router, firewall, switch, network link and interface) and storage components (hard disk), and other physical computing infrastructure elements.
  - ***Virtualized Infrastructure Layer:*** Entails software elements, such as hypervisors, virtual machines, virtual data storage, and supporting middleware components used to realize the infrastructure upon which a computing platform can be established. While virtual machine technology is commonly used at this layer, other means of providing the necessary software abstractions are not precluded.
  - ***Platform Architecture Layer:*** Entails compilers, libraries, utilities, and other software tools and development environments needed to implement applications.
  - ***Application Layer***: Represents deployed software applications targeted towards end-user software clients or other programs, and made available via the cloud.

Cloud Provider – Service Orchestration



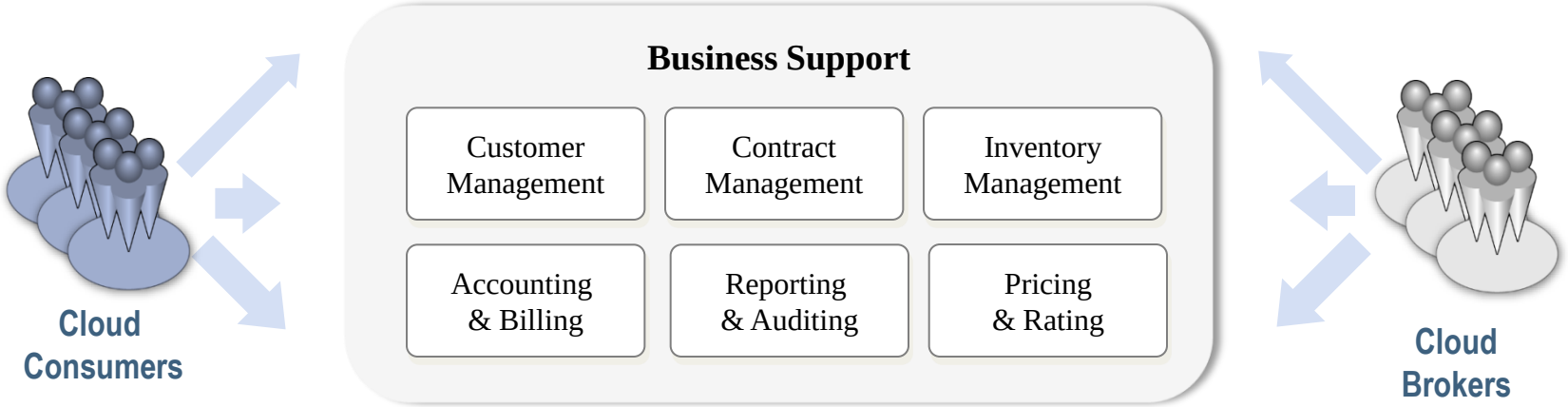
Cloud Provider – Service Orchestration (cont'd)

- The differences in scope and control between the cloud consumers and cloud providers, for each of the service models:
  - SaaS: The cloud consumer does not manage or control the underlying cloud infrastructure or individual applications, except for preference selections and limited administrative application settings. Security provisions are carried out mainly by the cloud provider.
  - PaaS: The cloud consumer has control over applications and application environment settings of the platform. Security provisions are split between the cloud provider and the cloud consumer.
  - IaaS: The cloud consumer generally has broad freedom to choose the operating system and development environment to be hosted. Security provisions beyond the basic infrastructure are carried out mainly by the cloud consumer.
- Ref:
  - NIST SP-800-144, "Guidelines on Security and Privacy Issues in Public Cloud Computing", Draft, http://collaborate.nist.gov/twiki-cloud-computing/pub/CloudComputing/Documents/Draft-SP-800-144_cloud-computing.pdf.

Cloud Provider – Business Support

- Business Support: Entails the set of business-related services dealing with clients, 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.
  - *Accounting and Billing*: Manage customer billing information, send billing statements, process received payments, track invoices, etc.
  - *Reporting and Auditing :* Monitor user operations, generate reports.
  - *Pricing and Rating:* Evaluate cloud services and determine prices, handle promotions and pricing rules that depend on a user's profile, etc.
- Ref:
  - IBM, "Cloud Computing: Save Time, Money, and Resources with a Private Test Cloud", *www.redbooks.ibm.com/redpapers/pdfs/redp4553.pdf*.
  - GSA, "Cloud Computing Initiative Vision and Strategy Document (DRAFT)", http://info.apps.gov/sites/default/files/Cloud_Computing_Strategy_0.ppt

Cloud Provider – Business Support



Cloud Provider – Operational Support (1)

- ***Operational Support***: represents the set of operational management and technical-related services
- *Provisioning/Configuration*
  - *Rapid provisioning*: Automatically deploying cloud system based on the requested service/resources/capabilities
  - *Resource change*: Adjust configuration/resource assignment for repairs, upgrades, and joining new nodes into the cloud
  - *Monitoring and Reporting*: Discover and monitor the virtual resources, monitor cloud operations and events, and generate performance reports.
  - *Metering:* Provide 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:* Encompasses the SLA contract definition (basic schema with the QoS parameters), SLA monitoring, and SLA enforcement, according to defined policies.

Cloud Service Providers – Operational Support (2)

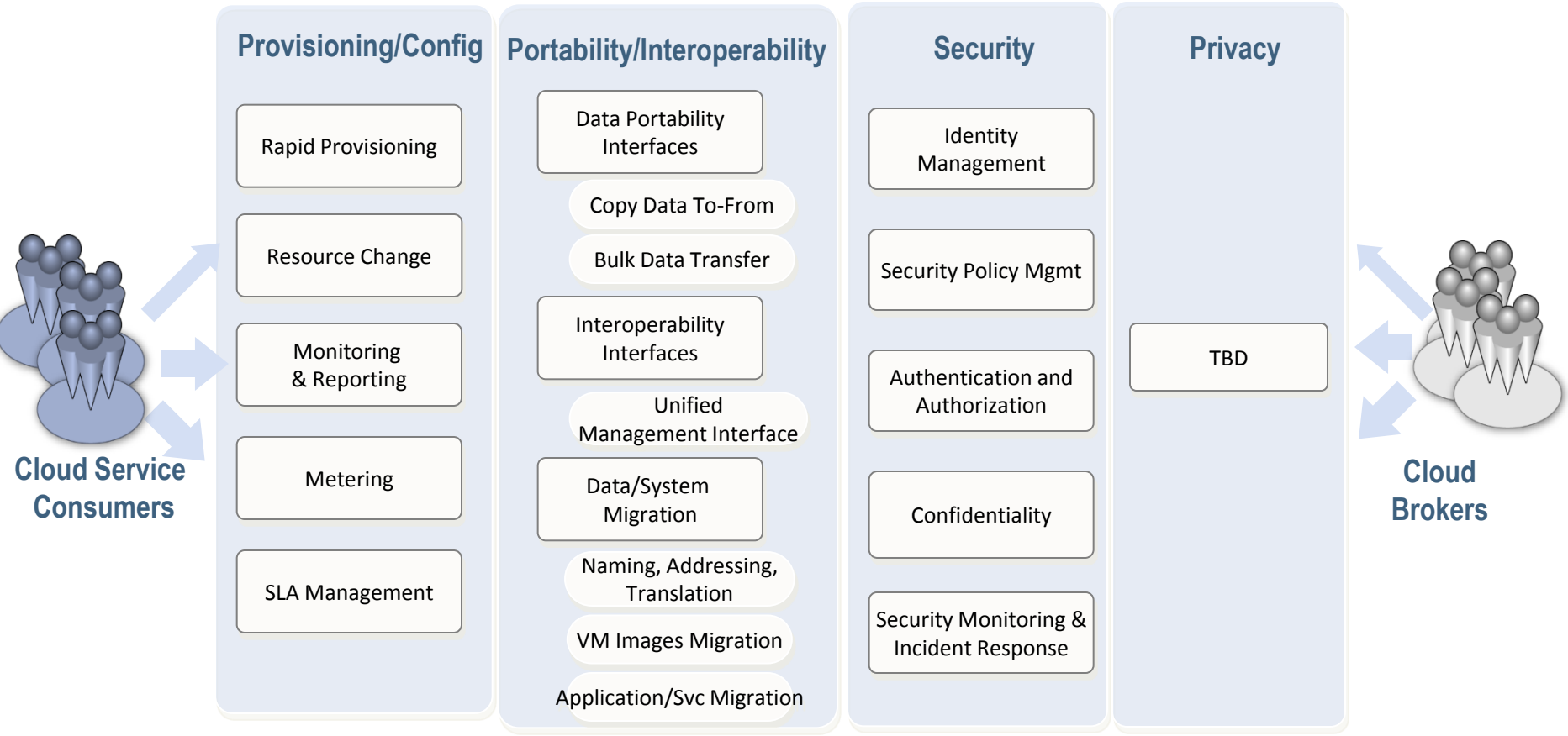
Portability/Interoperability - The Cloud Service Provider should provide

- *Interfaces that allow Data Portability*
  - *Copy data to-from*: Copy data objects into/out of a cloud.
  - *Bulk data transfer*: Use a disk for bulk transfer.
- *Interfaces to support interoperability*
  - *Cloud brokers should provide cloud service consumers a unified and enhanced management interface*
- *Access to user data that would allow Data format transform and management*
  - *Naming, Addressing and Translation*
- *System migration*
  - *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 Service Providers – Operational Support (3)

- *Security*
  - *Identity management:* Enforce identity and access control policies on users accessing cloud.
  - *Security policy management:* Configure/generate/enforce/audit/update security policies on users accessing clouds.
  - *Authentication and Authorization:* Authenticate and authorize cloud service consumers using credentials that have been established previously.
  - *Confidentiality and Privacy:* Protect the confidentiality and privacy of the data objects written into clouds
  - *Security monitoring:* Conduct ongoing automated monitoring of the cloud-provider infrastructure to demonstrate compliance with cloud-consumer security policies and auditing requirements
- Privacy
  - TBD
- Ref
  - IBM, "Cloud Computing: Save Time, Money, and Resources with a Private Test Cloud", *www.redbooks.ibm.com/redpapers/pdfs/redp4553.pdf*.
  - GSA, "Cloud Computing Initiative Vision and Strategy Document (DRAFT)", http://info.apps.gov/sites/default/files/Cloud_Computing_Strategy_0.ppt

Cloud Service Providers – Operational Support (4)



Cloud Carrier

- ***Cloud Carrier:*** The intermediary that provides connectivity and transport of cloud services between *Cloud Providers* and *Cloud Consumers*.
  - Provide access to consumers through network, telecommunication and other access devices
    - Examples: 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 carrier with consistent SLA shall be required. In general, the cloud carrier may be required to provide dedicated and encrypted connections.
- Ref:
  - Juniper Networks, "Cloud-ready Data Center Reference Architecture", www.juniper.net/us/en/local/pdf/reference-architectures/8030001-en.pdf
  - NIST definition of cloud computing v15, *www.nist.gov/itl/cloud/upload/cloud-def-v15.pdf*.
  - NIST cloud computing use cases, http://collaborate.nist.gov/twiki-cloud-computing/bin/view/CloudComputing/UseCaseCopyFromCloud

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 combination of cloud services can be too complex for cloud service consumers to manage their integration.
- Three major services provided by Cloud Brokers:
  - ***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. The added services can be categorized into:
    - Management services: identity management, access management, performance reporting, etc.
    - Deployment services - work by running on the raw infrastructure to provide the higher order functions.
  - ***Service Aggregation***: An aggregation brokerage service combines and integrates multiple services into one or more new services. It will ensure that data is 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.
- Ref:
  - Gartner, "Gartner Says Cloud Consumers Need Brokerages to Unlock the Potential of Cloud Services", http://www.gartner.com/it/page.jsp?id=1064712.

Cloud Auditor

- ***Cloud Auditor:*** A third-party that can conduct independent auditing of the cloud services, information system operation and determine the security of the cloud implementation.
- 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.
  - ***Security Assessment:*** Assess the management, operational, and technical controls of the cloud system with a frequency depending on risk.
  - ***Security Certification:*** A security certification is conducted for accrediting the cloud system. The security certification is a key factor in all security accreditation (i.e., authorization) decisions and is integrated into and spans the system development life cycle.
  - ***Security Accreditation:*** The organization authorizes (i.e., accredits) the cloud system for processing before operations and updates the authorization or when there is a significant change to the system.
- Ref:
  - Open Security Architecture (OSA), "Cloud Computing Patterns", http://www.opensecurityarchitecture.org/cms/library/patternlandscape/251-pattern-cloud-computing

The Combined Conceptual Reference Diagram