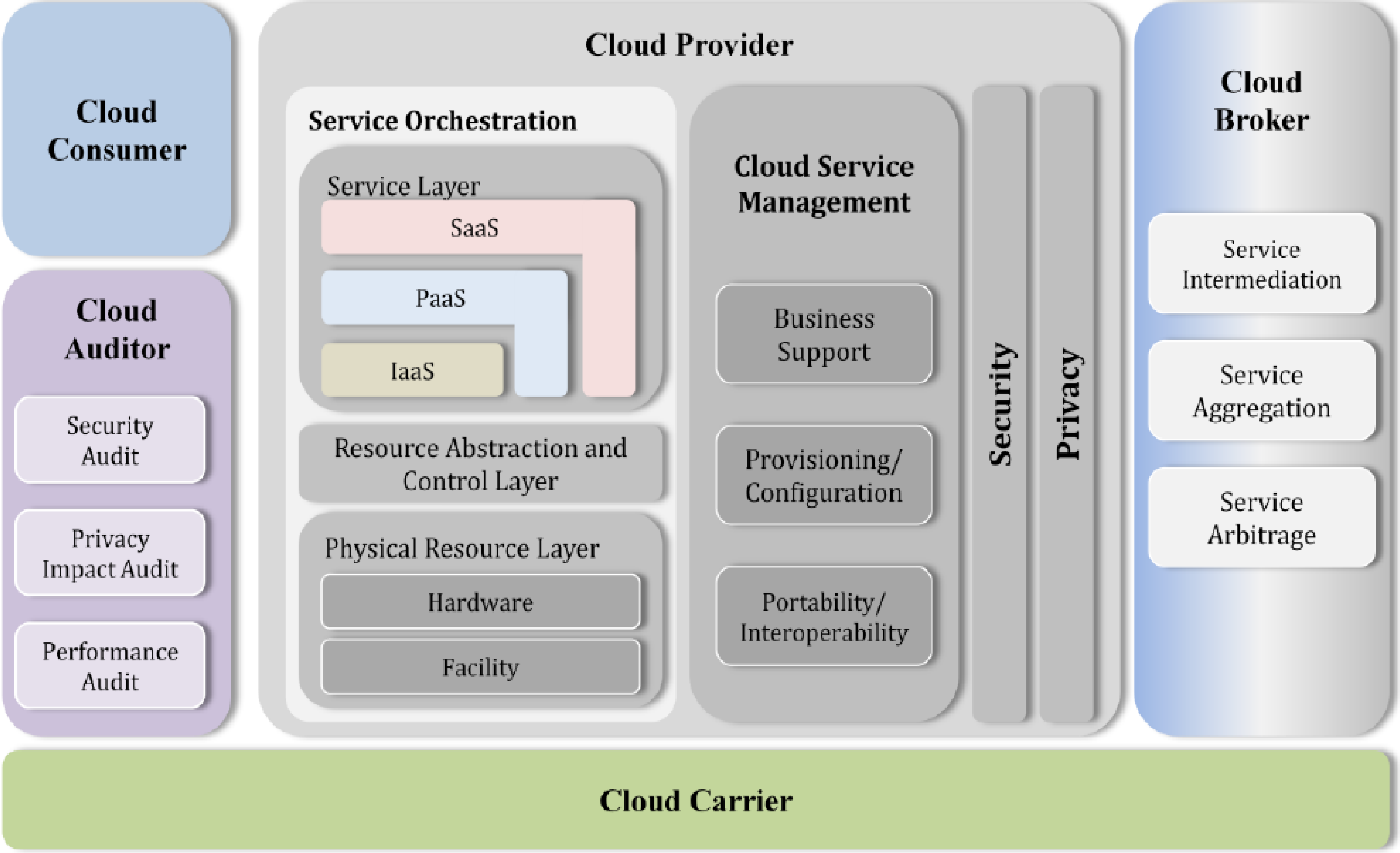
CAP470: Cloud Computing

Dr. Sophiya Sheikh
Assistant Professor
School of Computer Applications
Lovely Professional University

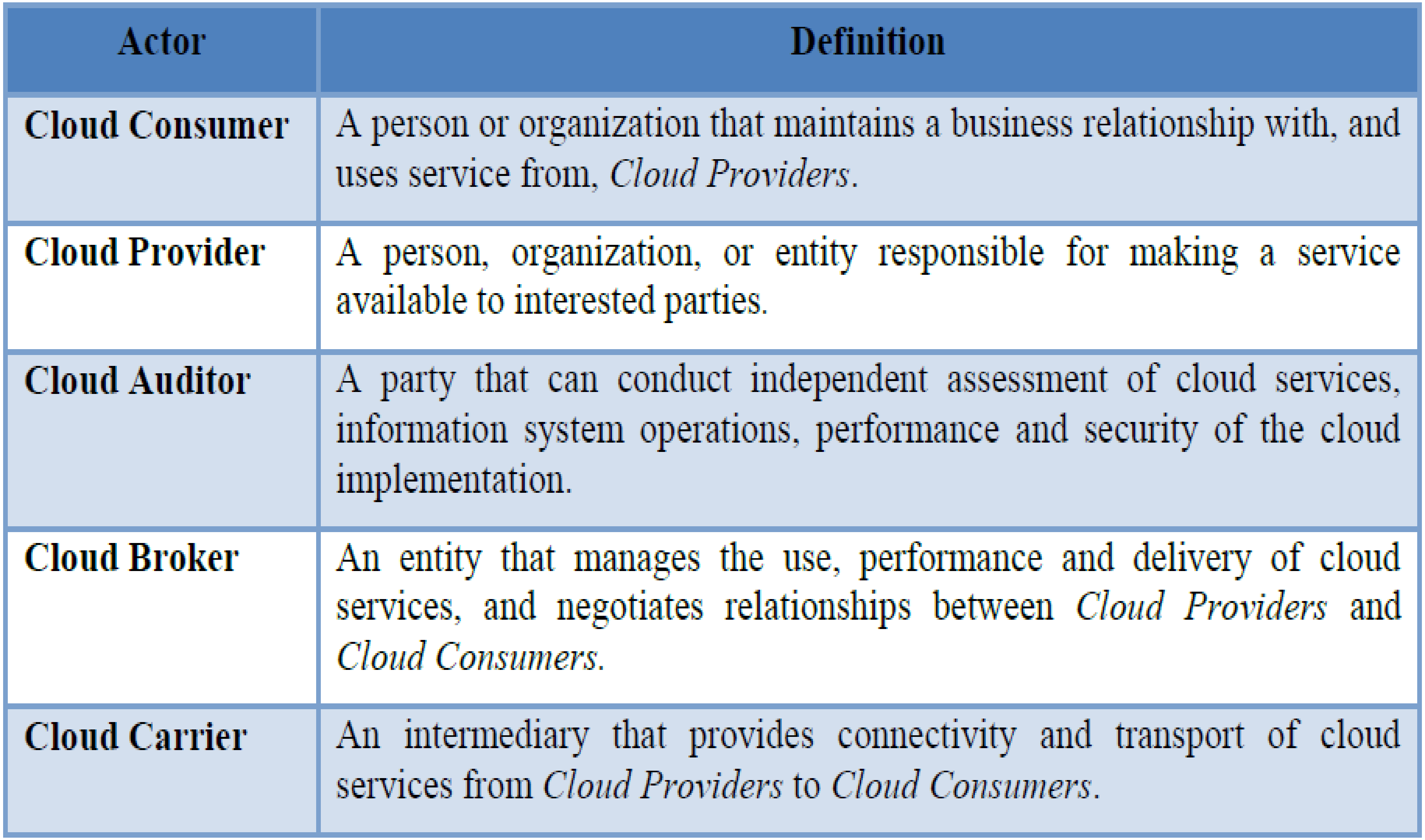
Business Models

- NIST Cloud Computing Reference Model
- Cloud Cube Model

NIST Cloud Computing Reference Model



Actors in Cloud Computing



Actor	Definition
Cloud Consumer	A person or organization that maintains a business relationship with, and uses service from, *Cloud Providers*.
Cloud Provider	A person, organization, or entity responsible for making a service available to interested parties.
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 that manages the use, performance and delivery of cloud services, and negotiates relationships between *Cloud Providers* and *Cloud Consumers*.
Cloud Carrier	An intermediary that provides connectivity and transport of cloud services from *Cloud Providers* to *Cloud Consumers*.

Question

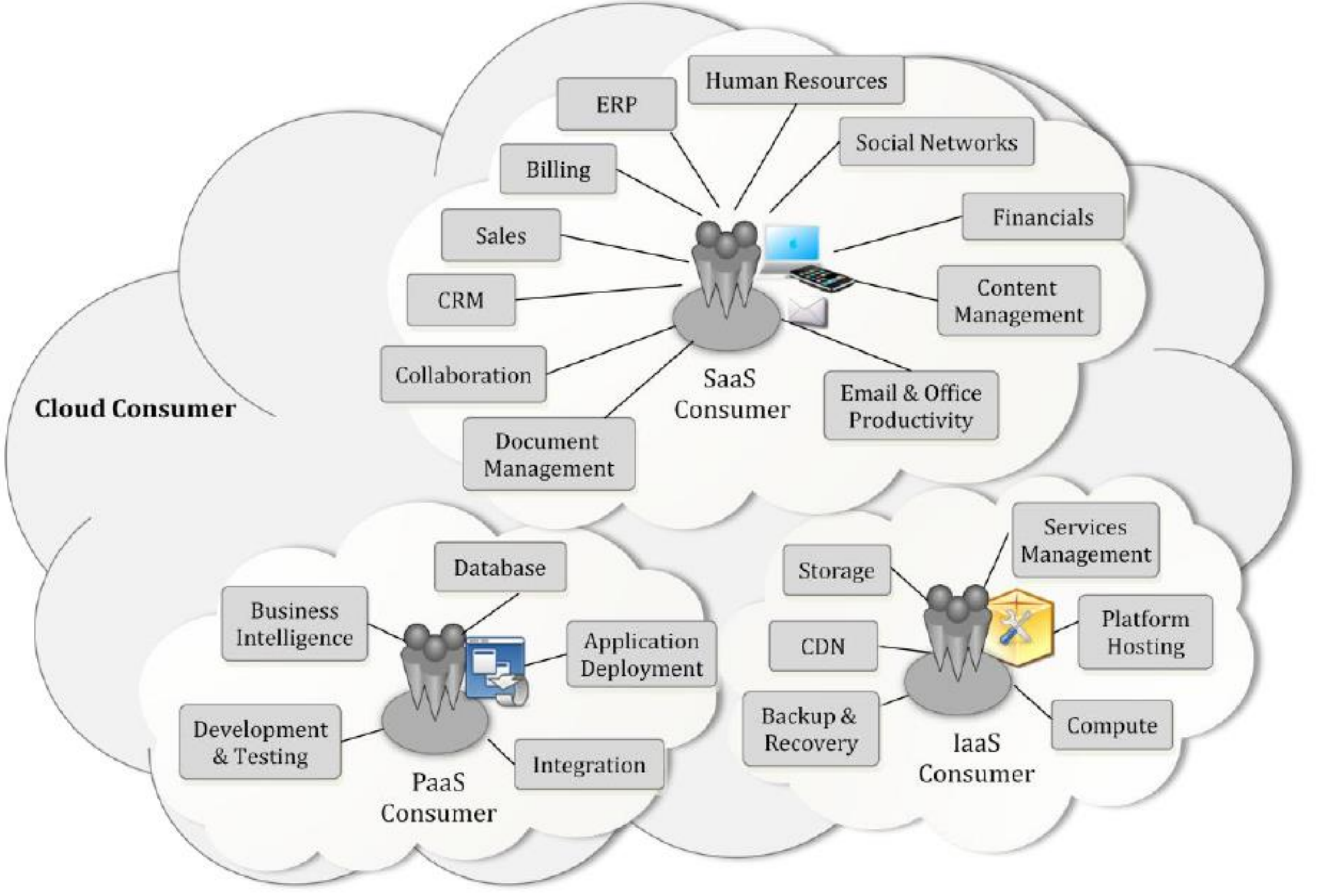
In the Planning Phase, Which of the following is the correct step for performing the analysis?

- Cloud Computing Value Proposition
- Cloud Computing Strategy Planning
- Both A and B
- Business Architecture Development

1. Cloud Consumer

The cloud consumer is the principal stakeholder for the cloud computing service.

- A cloud consumer represents a person or organization that maintains a business relationship with, and uses the service from a cloud provider.
- A cloud consumer browses the service catalogue from a cloud provider, requests the appropriate service, sets up service contracts with the cloud provider, and uses the service.
- The cloud consumer may be billed for the service provisioned, and needs to arrange payments accordingly.



Example Services Available to a Cloud Consumer

2. Cloud Provider

A cloud provider is a person, an organization; it is the entity responsible for making a service available to interested parties. A Cloud Provider:

- acquires and manages the computing infrastructure required for providing the services,
- runs the cloud software that provides the services, and
- makes arrangement to deliver the cloud services to the Cloud Consumers through network access.

A Cloud Provider's activities can be described in five major areas:

- *service deployment*,
- *service orchestration*,
- *cloud service management*,
- *security*, and
- *privacy*.

3. Cloud Auditor

A cloud auditor is a party that can perform an independent examination of cloud service controls with the intent to express an opinion thereon.

- Audits are performed to verify conformance to standards through review of objective evidence.
- A cloud auditor can evaluate the services provided by a cloud provider in terms of security controls, privacy impact, performance, etc.
- The auditor may ensure that fixed content has not been modified and that the legal and business data archival requirements have been satisfied.

4. Cloud Broker

As cloud computing evolves, the integration of cloud services can be too complex for cloud consumers to manage.

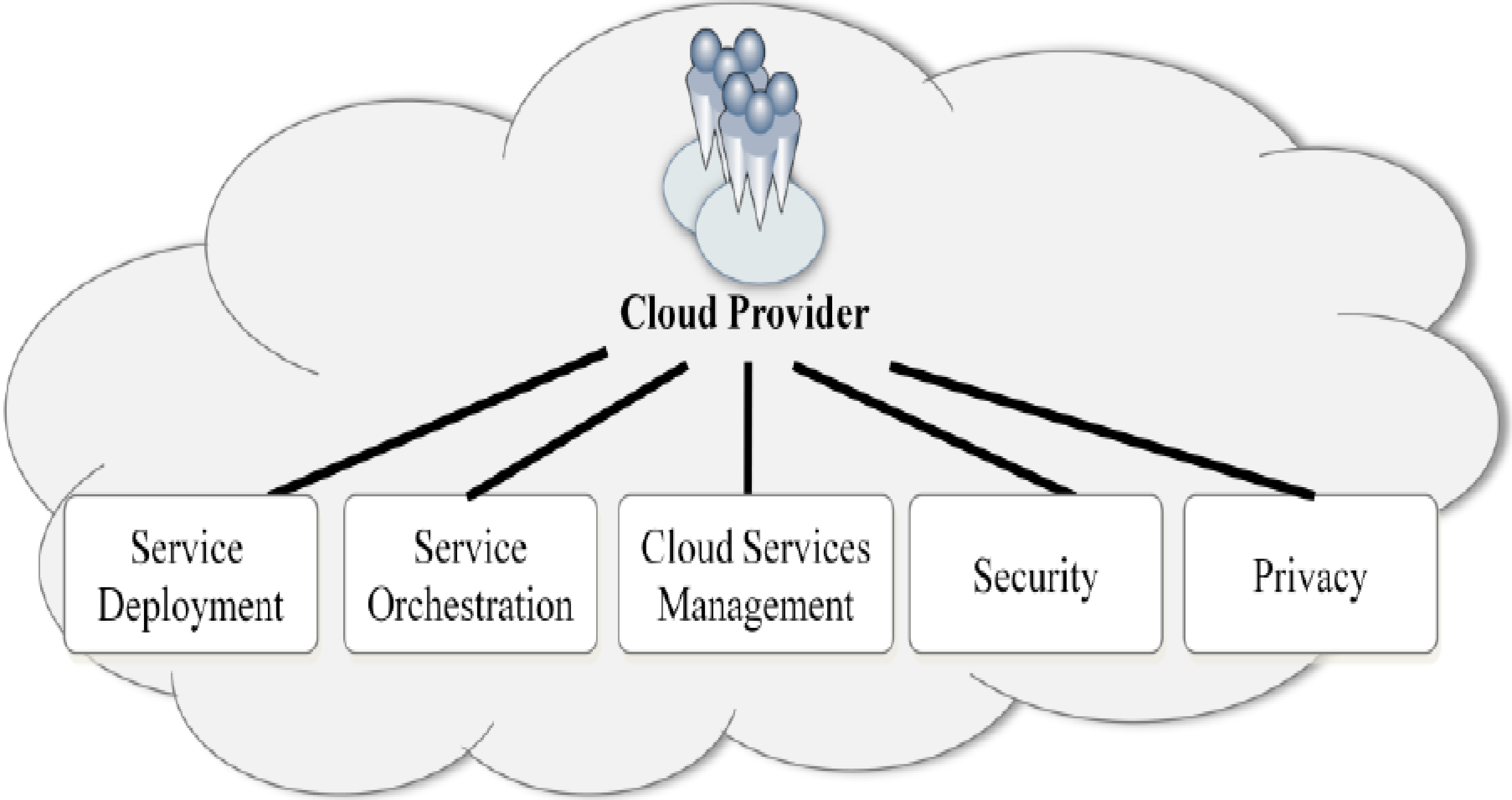
- A cloud consumer may request cloud services from a cloud broker, instead of contacting a cloud provider directly.
- A cloud broker is an entity that manages the use, performance and delivery of cloud services and negotiates relationships between cloud providers and cloud consumers.

5. Cloud Carrier

A cloud carrier acts as an intermediary that provides connectivity and transport of cloud services between cloud consumers and cloud providers.

- Cloud carriers provide access to consumers through network, telecommunication and other access devices.
  - For example, cloud consumers can obtain cloud services through network access devices, such as computers, laptops, mobile phones, mobile Internet devices (MIDs), etc.
- The distribution of cloud services is normally provided by network and telecommunication carriers or a transport agent, where a transport agent refers to a business organization that provides physical transport of storage media such as high-capacity hard drives.
  - Note that a cloud provider will set up SLAs with a cloud carrier to provide services consistent with the level of SLAs offered to cloud consumers, and may require the cloud carrier to provide dedicated and secure connections between cloud consumers and cloud providers.

Major activities of Cloud Provider



Cloud Provider

Service Deployment

Service Orchestration

Cloud Services Management

Security

Privacy

A. Service Deployment

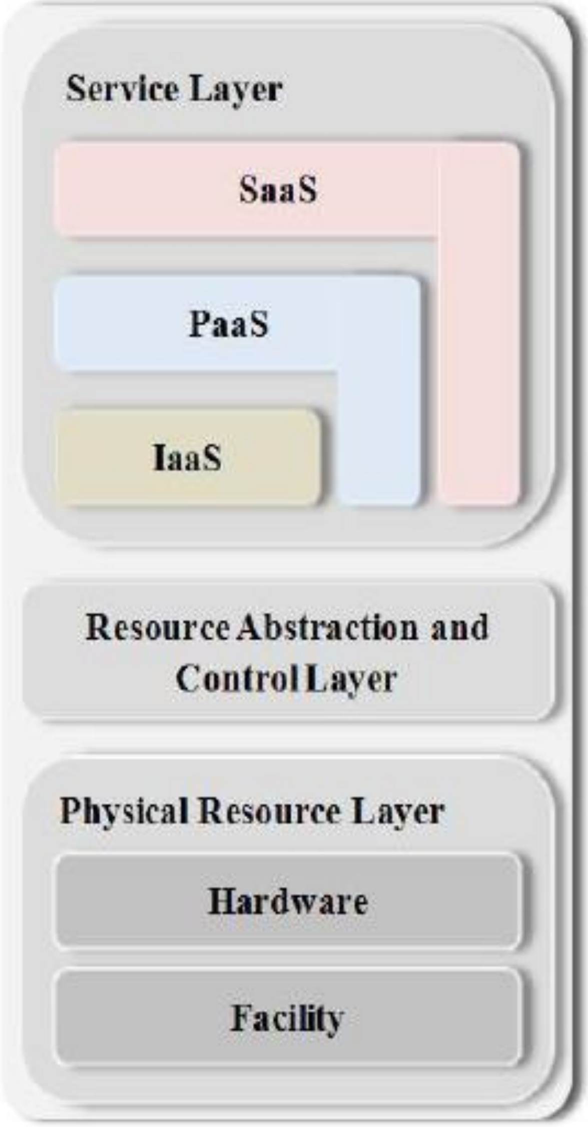
A cloud infrastructure may be operated in one of the following deployment models:

- public cloud,
- private cloud,
- community cloud, or
- hybrid cloud.

The differences are based on how exclusive the computing resources are made to a Cloud Consumer.

B. Cloud Service Orchestration

Service Orchestration refers to the composition of system components to support the Cloud Providers activities in arrangement, coordination and management of computing resources in order to provide cloud services to Cloud Consumers. Figure shows a generic stack diagram of this composition that underlies the provisioning of cloud services. A three-layered model is used in this representation, representing the grouping of three types of system components Cloud Providers need to compose to deliver their services.



Question

This phase involves selecting a cloud provider based on the Service Level Agreement (SLA), which defines the level of service the provider receives.

- Maintenance and Technical Service
- Selecting Cloud Computing Provider
- Both A and B
- None of the above

1. Service layer

This is where Cloud Providers define interfaces for Cloud Consumers to access the computing services.

- Access interfaces of each of the three service models are provided in this layer. It is possible, though not necessary, that SaaS applications can be built on top of PaaS components and PaaS components can be built on top of IaaS components.
- The optional dependency relationships among SaaS, PaaS, and IaaS components are represented graphically as components stacking on each other; while the angling of the components represents that each of the service component can stand by itself.

2. Resource Abstraction and Control Layer

This layer contains the system components that Cloud Providers use to provide and manage access to the physical computing resources through software abstraction.

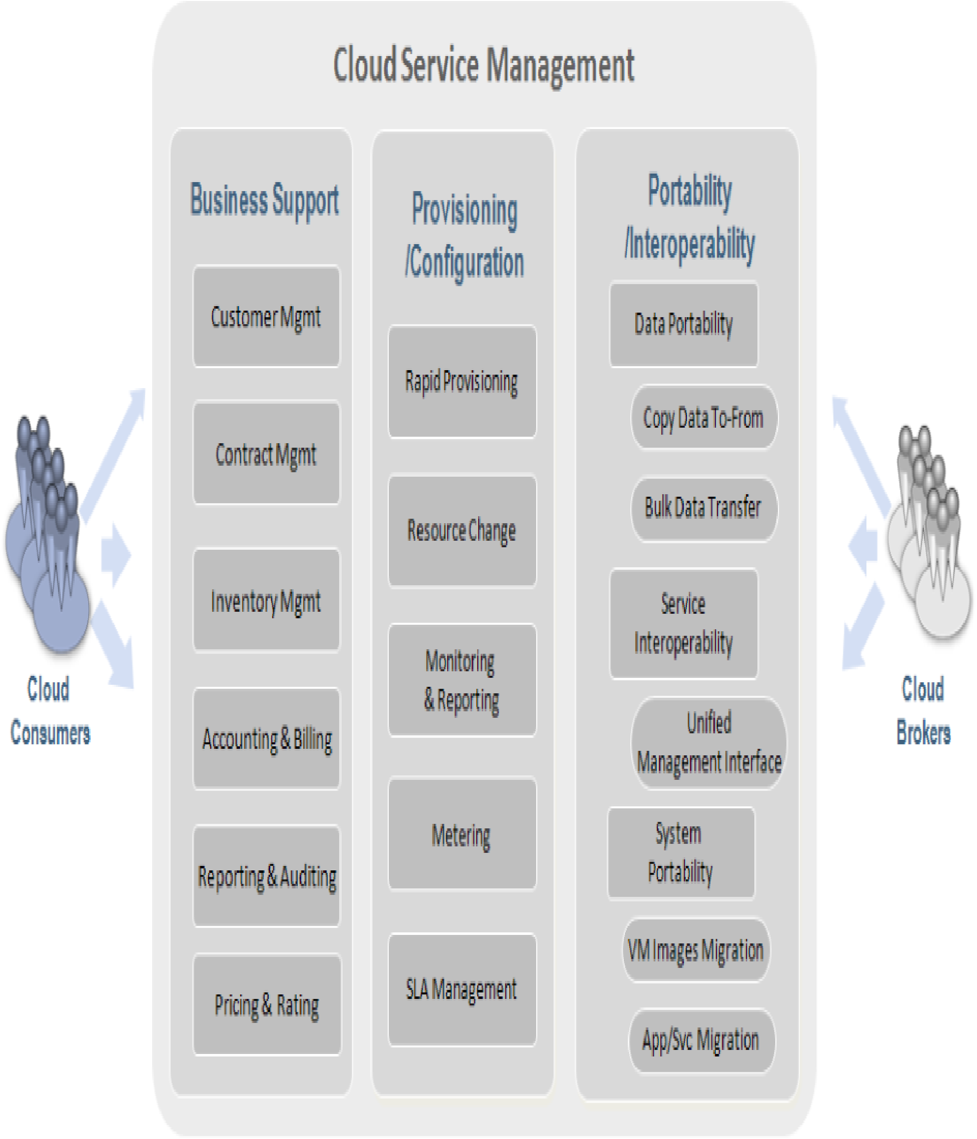
- The **resource abstraction** needs to ensure efficient, secure, and reliable usage of the underlying physical resources. While virtual machine technology is commonly used at this layer, other means of providing the necessary software abstractions are also possible.
    - Examples of resource abstraction components include software elements such as hypervisors, virtual machines, virtual data storage, and other computing resource abstractions.
- The **control** aspect of this layer refers to the software components that are responsible for resource allocation, access control, and usage monitoring.
    - This is the software fabric that ties together the numerous underlying physical resources and their software abstractions to enable resource pooling, dynamic allocation, and measured service.
    - Various open source and proprietary cloud software are examples of this type of middleware.

3. Physical Resource Layer

- This layer includes **hardware resources**, such as computers (CPU and memory), networks (routers, firewalls, switches, network links and interfaces), storage components (hard disks) and other physical computing infrastructure elements.
- It also includes **facility resources**, such as heating, ventilation and air conditioning (HVAC), power, communications, and other aspects of the physical plant.

C. Cloud Service Management

Cloud Service Management includes all of the service-related functions that are necessary for the management and operation of those services required by or proposed to cloud consumers. As illustrated in Figure, cloud service management can be described from the perspective of *business support, provisioning and configuration*, and from the perspective of *portability and interoperability* requirements.



Business Support

- *Business Support* entails the set of business-related services dealing with clients and supporting processes. 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 points-of-contact and resolving customer issues and problems, etc.
- *Contract management:* Manage service contracts, setup/negotiate/close/ terminate contract, etc.
- *Inventory Management:* Set up and manage service catalogues, 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 based on a user's profile, etc.

Provisioning and 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.

Portability and Interoperability

The proliferation of cloud computing promises cost savings in technology infrastructure and faster software upgrades. The US government, along with other potential cloud computing customers, has a strong interest in moving to the cloud. However, the adoption of cloud computing depends greatly on how the cloud can address users concerns on security, portability and interoperability.

- For portability, prospective customers are interested to know whether they can move their data or applications across multiple cloud environments at low cost and minimal disruption.
- From an interoperability perspective, users are concerned about the capability to communicate between or among multiple clouds.

Cloud providers should provide mechanisms to support *data portability, service interoperability*, and *system portability*.

- **Data portability** is the ability of cloud consumers to copy data objects into or out of a cloud or to use a disk for bulk data transfer.
- **Service interoperability** is the ability of cloud consumers to use their data and services across multiple cloud providers with a unified management interface.
- **System portability** allows the migration of a fully-stopped virtual machine instance or a machine image from one provider to another provider, or migrate applications and services and their contents from one service provider to another.

It should be noted that various cloud service models may have different requirements in related with portability and interoperability.

For example,

- IaaS requires the ability to migrate the data and run the applications on a new cloud. Thus, it is necessary to capture virtual machine images and migrate to new cloud providers which may use different virtualization technologies. Any provider-specific extensions to the VM images need to be removed or recorded upon being ported.
- While for SaaS, the focus is on data portability, and thus it is essential to perform data extractions and backups in a standard format.

D. Security

- It is critical to recognize that security is a cross-cutting aspect of the architecture that spans across all layers of the reference model, ranging from physical security to application security.
- Therefore, security in cloud computing architecture concerns is not solely under the purview of the Cloud Providers, but also Cloud Consumers and other relevant actors.
- Cloud-based systems still need to address security requirements such as authentication, authorization, availability, confidentiality, identity management, integrity, audit, security monitoring, incident response, and security policy management.

While these security requirements are not new, we discuss cloud specific perspectives to help discuss, analyse and implement security in a cloud system.

- **Cloud Service Model Perspectives**
- **Implications of Cloud Deployment Models**
- **Shared Security Responsibilities**

E. Privacy

Cloud providers should protect the assured, proper, and consistent collection, processing, communication, use and disposition of personal information (PI) and personally identifiable information (PII) in the cloud.

- PII is the information that can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.
- Though cloud computing provides a flexible solution for shared resources, software and information, it also poses additional privacy challenges to consumers using the clouds.

Question

What is Business Architecture Development?

- We recognize the risks that might be caused by cloud computing application from a business perspective.
- We identify the applications that support the business processes and the technologies required to support enterprise applications and data systems.
- We formulate all kinds of plans that are required to transform the current business to cloud computing modes.
- None of the above

Cloud Cube Model

- According to cloud cube model, there are several “cloud formations” - or forms of cloud computing. Each offers
  - different characteristics,
  - varying degrees of flexibility,
  - different collaborative opportunities, and
  - different risks.
- One of the key challenges that businesses face when considering cloud computing as an option is to determine how to choose the cloud formation best suited to their various types of business operations.
- The Jericho Forum’s developed Cloud Cube Model with objectives related to cloud computing to distinctive enabling secure collaboration in the appropriate cloud formations best suited to the business needs.

The Jericho Forum

The Jericho Forum is actively encouraging solution providers and vendors to develop the missing capabilities and services to ensure customers are protected from the stormier implications of clouds.

In Feb 2009, they delivered a practical framework geared to showing how to create the right **Collaboration Oriented Architecture (COA)** to assure secure business collaboration in de-perimeterised environments. For the Jericho Forum, the natural evolution from this is to address how to follow a well-structured path towards enabling secure business collaboration without becoming vulnerable to issues which may put at risk your data, or your ability to work with your chosen business parties, or your regulatory compliance.

Recommendation

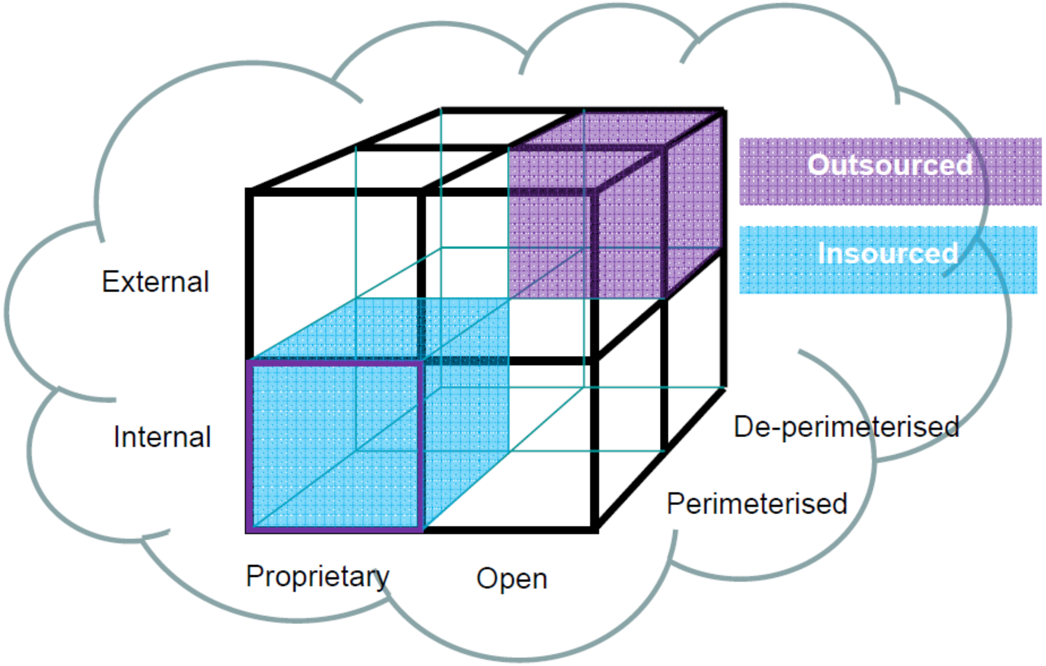
- First you need to classify your data so as to know what rules must apply to protecting it:
  - it's sensitivity
  - what regulatory/compliance restrictions apply on it.
- We can only meet this requirement if we have universally adopted standards for:
  - a data classification model
  - an associated standard for managing trust levels
  - standardised metadata that signals to "cloud security" what security needs be applied to each item of data.

With an understanding on what security you need to apply to your data, you're in a position to decide:

- What data and processes to move to the Clouds
- At what level you want to operate in the Clouds? Cloud models separate layers of business service from each other, for example, Infrastructure / Platform / Software / Process.
- Which Cloud Formations are best suited to your needs.

The Cloud Cube Model

The Jericho Forum has identified 4 criteria to differentiate cloud formations from each other and the manner of their provision. These dimensions are as follows:



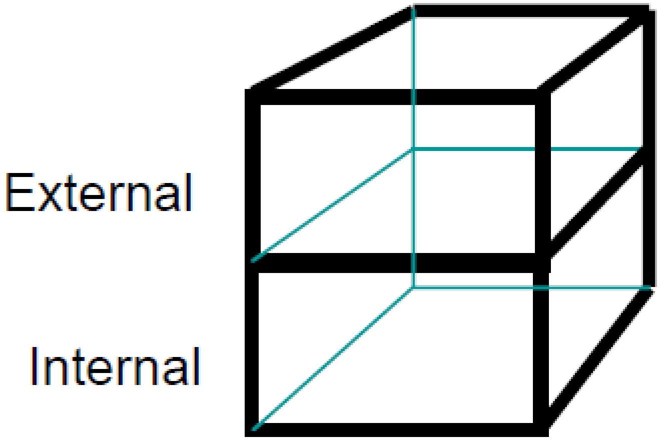
- **Internal (I) / External (E)**
- **Proprietary (P) / Open (O)**
- **Perimeterised (Per) / De-perimeterised (D-p) Architectures**
- **Insourced / Outsourced**

1. Dimension: Internal (I) / External (E)

This is the dimension that defines the physical location of the data: where does the cloud form you want to use exist inside or outside your organization's boundaries.

- If it is within your own physical boundary then it is Internal.
- If it is not within your own physical boundary then it is External.

For example, virtualised hard disks in an organisation's data centre would be internal, while Amazon SC33 would be external at some location "off-site".



Question

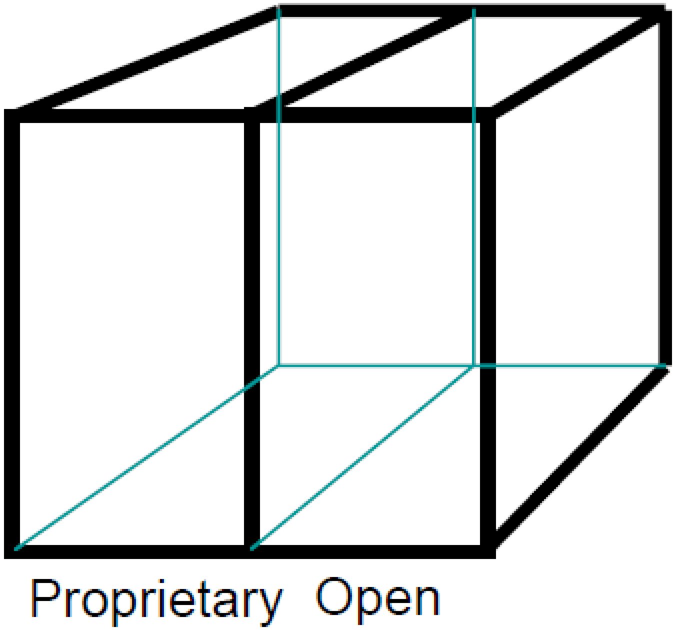
How many types of security boundary values exist in Cloud Cube model?

- a) 1
- b) 2
- c) 3
- d) None of the mentioned

2. Dimension: Proprietary (P) / Open (O)

This is the dimension that defines the state of ownership of the cloud technology, services, interfaces, etc.

- It indicates the degree of interoperability, as well as enabling “data/application transportability” between your own systems and other cloud forms.
- It indicates the ability to withdraw your data from a cloud form or to move it to another without constraint.
- It also indicates any constraints on being able to share applications.



Continue..

Proprietary means that the organization providing the service is keeping the means of the provision under their ownership.

- As a result, when operating in clouds that are proprietary, you may not be able to move to another cloud supplier without significant effort or investment.
- Often the more innovative technology advances occur in the proprietary domain. As such the proprietor may choose to enforce restrictions through patents and by keeping the technology involved a trade secret.

Continue..

Clouds that are **Open** are using technology that is not proprietary, meaning that there are likely to be more suppliers, and you are not as constrained in being able to share your data and collaborate with selected parties using the same open technology.

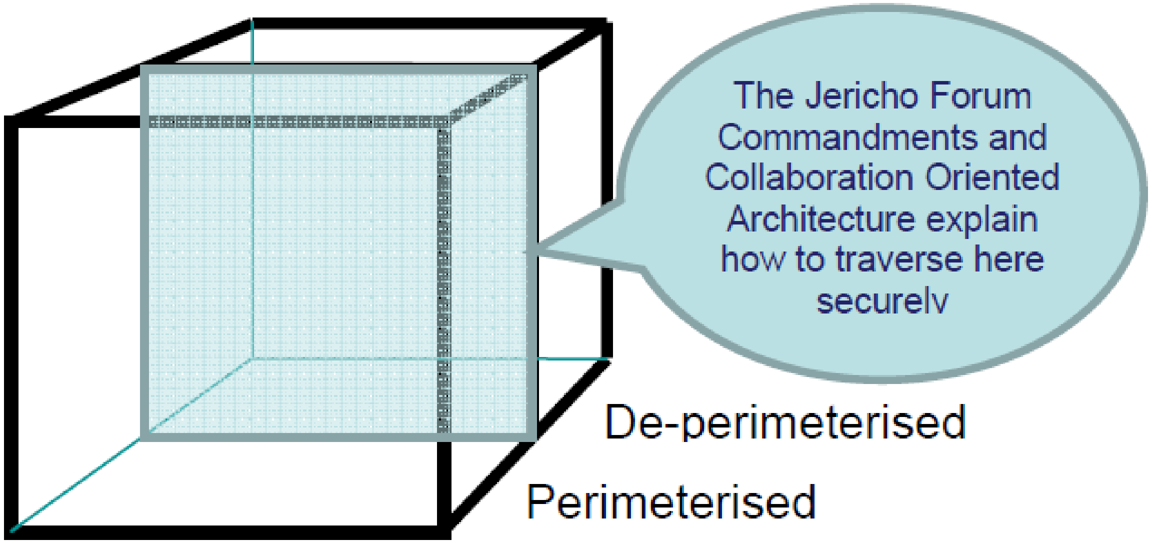
- Open services tend to be those that are widespread and consumerised, and most likely a published open standard, for example email (SMTP).
- An as yet unproven premise is that the clouds that most effectively enhance collaboration between multiple organisations will be Open.

3. Dimension: Perimeterised (Per) / De-perimeterised (D-p) Architectures

The third dimension represents the "architectural mindset" :

Are you operating inside your traditional IT perimeter or outside it?

De-perimeterisation has always related to the gradual failure / removal /shrinking / collapse of the traditional silo-based IT perimeter.


The Jericho Forum Commandments and Collaboration Oriented Architecture explain how to traverse here securelv
De-perimeterised
Perimeterised

Continue..

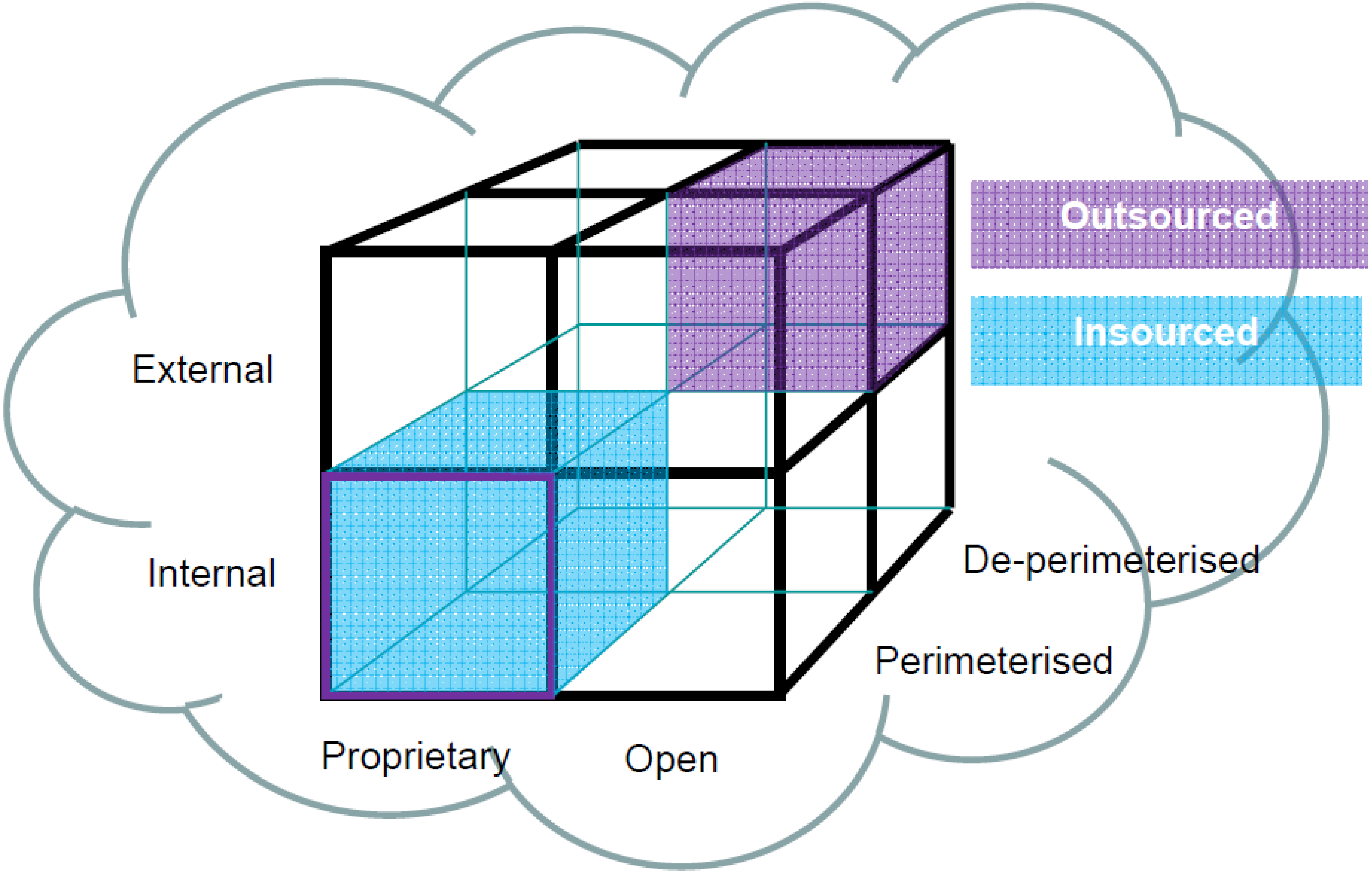
Perimeterised implies continuing to operate within the traditional IT perimeter, often signalled by “network firewalls”.

- When operating in the perimeterised areas, you may simply extend your own organisation’s perimeter into the external cloud computing domain using a VPN and operating the virtual server in your own IP domain, making use of your own directory services to control access.
- Then, when the computing task is completed you can withdraw your perimeter back to its original traditional position. We consider this type of system perimeter to be a traditional, though virtual, perimeter.

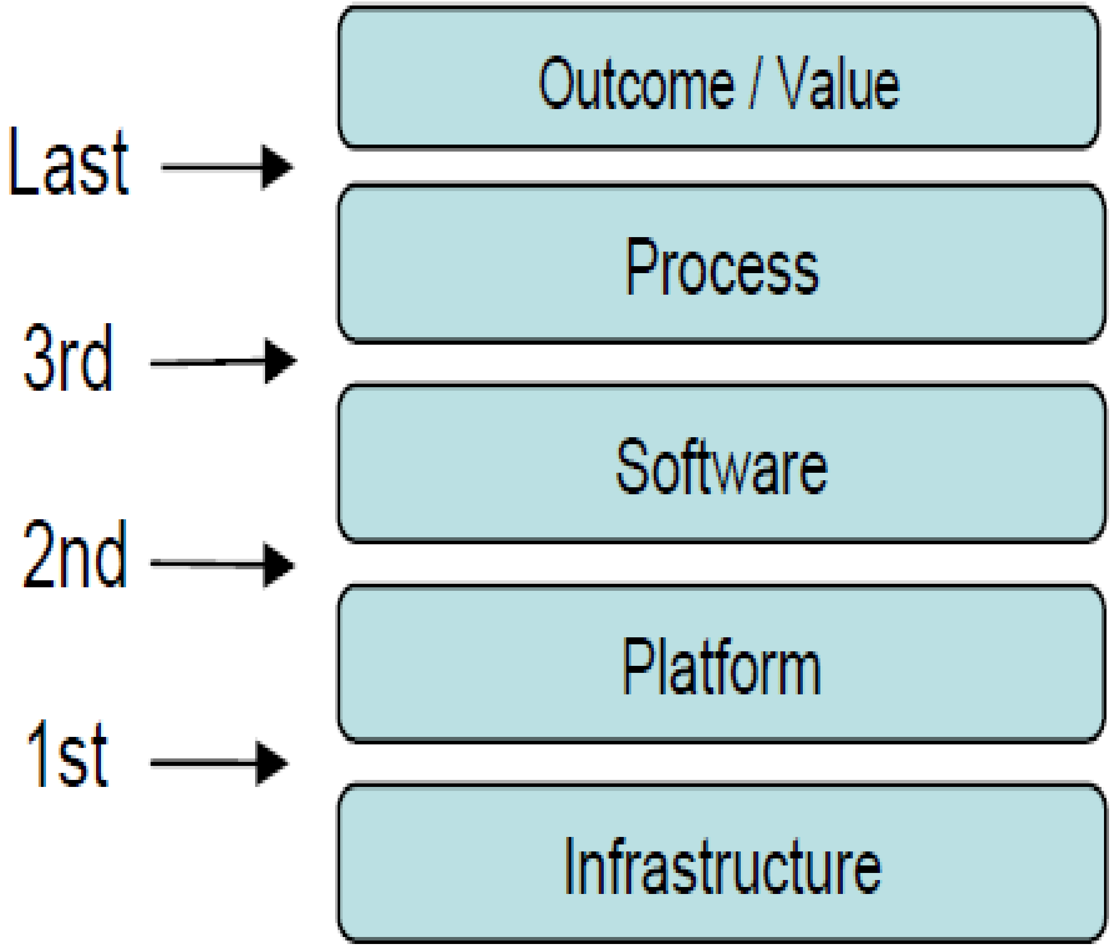
Continue..

De-perimeterised, assumes that the system perimeter is architected following the principles outlined in the Jericho Forum's Commandments and Collaboration Oriented Architectures Framework.

- In a de-perimeterised environment an organisation can collaborate securely with selected parties (business partner, customer, supplier, outworker) globally over any COA capable network.
- The terms **Micro-Perimeterisation** and **Macro-Perimeterisation** will likely be in active use here - for example in a de-perimeterised frame the data would be encapsulated with meta-data and mechanisms that would protect the data from inappropriate usage. COA-enabled systems allow secure collaboration.


Outsourced
Insourced
External
Internal
De-perimeterised
Perimeterised
Proprietary
Open

While the underlying intent remains the same, an added distinction in describing Deperimeterised cloud usage arises in that the detailed description changes based on the level of abstraction at which you choose to operate.



4. Dimension: Insourced / Outsourced

A 4th dimension that has 2 states in each of the 8 cloud forms: Per(IP,IO,EP,EO) and D-p(IP,IO,EP,EO), that responds to the question

"Who do you want running your Clouds?"

- **Outsourced**: the service is provided by a 3rd party
- **Insourced**: the service is provided by your own staff under your control

These 2 states describe who is managing delivery of the cloud service(s) that you use. This is primarily a policy issue (i.e. a business decision, not a technical or architectural decision) which must be embodied in a contract with the cloud provider.

In the Cloud Cube Model diagram this 4th dimension is shown by 2 colors; any of the 8 cloud forms can take either color.

Key questions customers need to ask their Cloud Computing suppliers

1. Where in our cloud cube model is my cloud supplier operating when providing each of their services?
2. How will my cloud supplier assure that when using their services I am operating in a cloud form that has and will maintain the features I expect?
3. How can I ensure that my data and the cloud services will continue to be available, in the event of the provider’s bankruptcy or change in business direction.

Question

Which of the following is provided by ownership dimension of Cloud Cube Model?

- a) Proprietary
- b) Owner
- c) P
- d) All of the mentioned