Cloud Cube Model:
Selecting Cloud Formations for Secure Collaboration

Problem

Cloud computing offers massive scalability - in virtual computing power, storage, and applications resources - all at almost immediate availability and low cost, and business managers are demanding their IT operations assess the benefits this new computing model can represent. As with all new technologies, there are new risks to be discovered and old risks to be re-evaluated. Many articles have already been published, and several new groups have formed to address cloud computing. In line with our continuing strategy for enabling secure business collaboration, the Jericho Forum members are addressing how to collaborate securely in the clouds.

There are several "cloud formations" - or forms of cloud computing. Each offers different characteristics, varying degrees of flexibility, different collaborative opportunities, and different risks. Thus 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 objectives related to cloud computing are distinctive – enabling secure collaboration in the appropriate cloud formations best suited to the business needs.

With this in mind, the aim of this paper is to:

- point out that not everything is best implemented in clouds; it may be best to operate some business functions using a traditional non-cloud approach
- explain the different cloud formations that the Jericho Forum has identified
- describe key characteristics, benefits and risks of each cloud formation
- provide a framework for exploring in more detail the nature of different cloud formations and the issues that need answering to make them safe and secure places to work in.

This is very much "work-in-progress", which we hope will enable all stakeholders, but particularly business decision-makers, to appreciate the key considerations that need to be taken into account when deciding which parts of their business could be operated in which of the available cloud formations.

Why should I care?

Cloud computing suppliers claim they are responding to customer demands for assurances on the security of the services they provide. Some even claim that, because they know that their customers place high priority on the security of the data they own, the security of the cloud services they offer is often significantly better than that of the customer's own IT systems.

While this may well be true, it is critical that cloud customers select the right cloud formations for their needs, to ensure they remain secure, able to collaborate safely with their selected parties as their evolving business needs require, and compliant to applicable regulatory requirements - including on the use and location of their data.

The joy of the cloud model is that it can deliver great advantages, but only if you know where in the different formations of cloud you need to be in order to achieve the right flexibility for your business needs. For example, if a cloud vendor were to cease providing a service, how effortlessly could you move to another provider or use your cloud-based capability to provide you with seamless disaster recovery and business continuity?

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, we delivered a practical framework geared to showing how to create the right Collaboration Oriented Architecture[1] (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 / response

Protecting your Data

First, it is necessary to classify your data so as to know what rules must apply to protecting it:

- it's sensitivity - must it only exist at specific trust levels? If so, which?
- What regulatory/compliance restrictions apply – e.g. Must it stay within your national boundary? Does it have to stay in Safe Harbours? etc.

We can only meet this requirement if we have universally adopted standards for:

- a data classification model that is sufficiently easy for all originators of data to use – for example the G8 Traffic Light Protocol[2].
- 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:

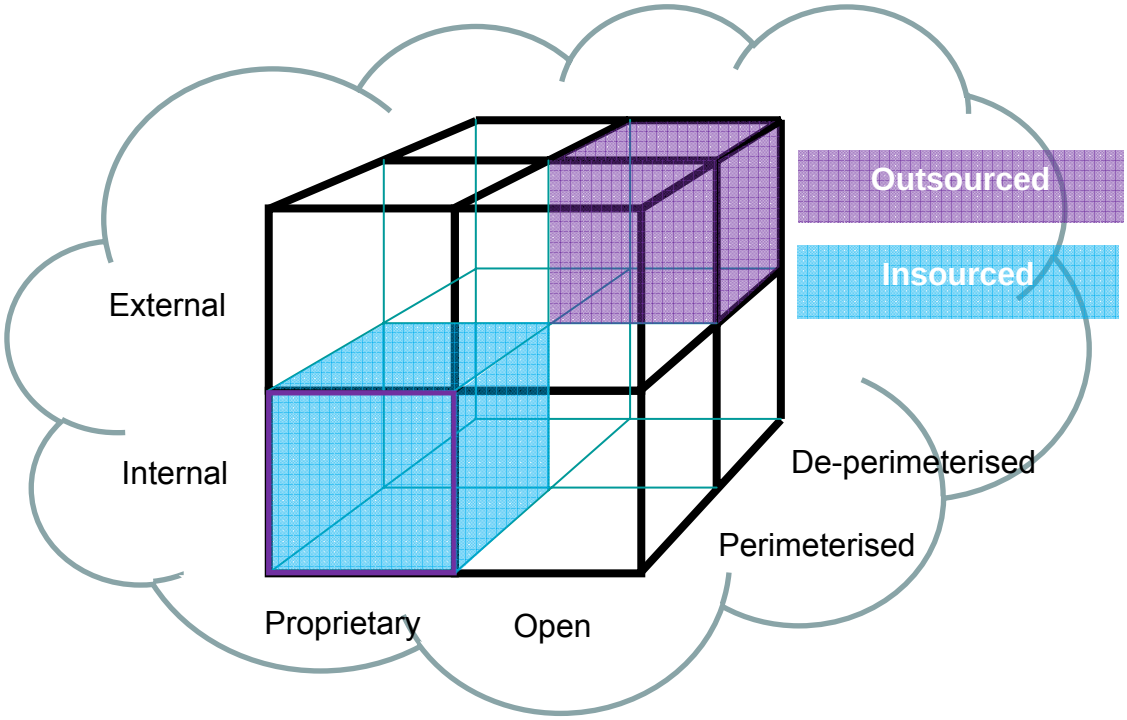
- what data and processes to move to the Clouds
- at what level you want to operate in the Clouds? Cloud models separate layers of business service from each other, for example, Infrastructure / Platform / Software / Process.
- which Cloud Formations are best suited to your needs.

[1] Collaboration Oriented Architectures (COA) Framework – see COA papers freely available from the Jericho Forum Web site at http://www.opengroup.org/jericho/publications.htm

[2] See COA paper on Trust Management – available as free download from http://www.opengroup.org/jericho/publications.htm

Cloud Formations – the Cloud Cube Model

The Jericho Forum has identified 4 criteria to differentiate cloud formations from each other and the manner of their provision. The Cloud Cube Model summarises these 4 dimensions, which are explained in turn in the rest of this paper.

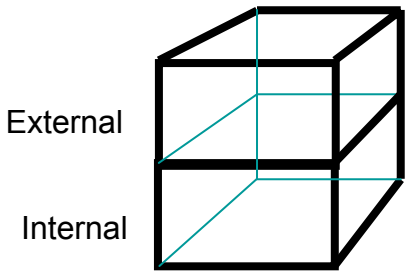


The Cloud Cube Model

Cloud Cube Model Dimensions

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.



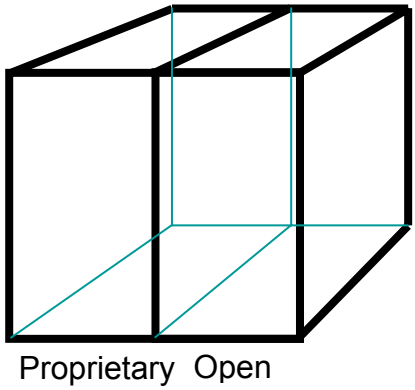
- If it is within your own physical boundary then it is Internal.
- If it is not within your own physical boundary then it is External.

For example, virtualised hard disks in an organisation's data centre would be internal, while Amazon SC3[3] would be external at some location "off-site".

Note: Be wary of making a false assumption that Internal is more secure than External. The effective use of both is likely to provide the most secure usage model.

[3] Amazon's SC3 - on-demand storage solution.

Dimension: Proprietary (P) / Open (O)

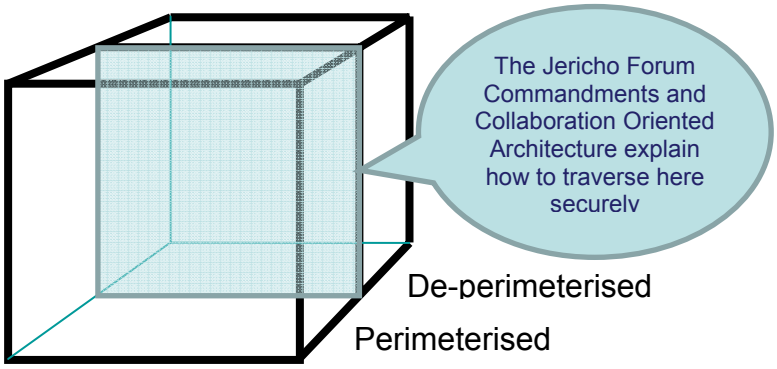


This is the dimension that defines the state of ownership of the cloud technology, services, interfaces[4], etc. It indicates the degree of interoperability, as well as enabling "data/application transportability" between your own systems and other cloud forms, and the ability to withdraw your data from a cloud form or to move it to another without constraint. It also indicates any constraints on being able to share applications.

- Proprietary means that the organisation providing the service is keeping the means of 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.
- 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.

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.

- Perimeterised implies continuing to operate within the traditional IT perimeter, often signalled by "network firewalls". As has been discussed in previous published Jericho Forum papers, this approach inhibits collaboration. In effect, 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.

[4] On the assumption that it is how you get your data in and out that is key to being able to move to another service, assuming the service does the same, it does not matter if internal code is the same.

- De-perimeterised, assumes that the system perimeter is architected following the principles outlined in the Jericho Forum's Commandments and Collaboration Oriented Architectures Framework. 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. In a de-perimeterised environment an organisation can collaborate securely with selected parties (business partner, customer, supplier, outworker) globally over any COA capable network

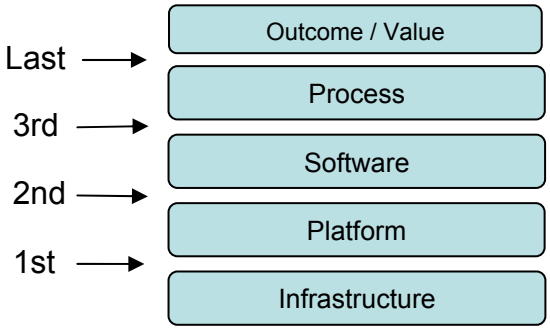
The de-perimeterised areas in our Cloud Cube Model use both internal and external domains but the collaboration or sharing of data should not be seen as internal or external – rather it is controlled by and limited to the parties that the using organisations select. For example, in the future frame, one organisation will not feel uncomfortable about allowing data into the internal COA-compliant domain of a collaborating organisation; rather, they will be confident that the data will be appropriately protected.

This means:

- You can operate in any of the four cloud formations so far described (I/P,I/O,E/P,E/O) with either of two architectural mindsets - Perimeterised or De-perimeterised.
- The top-right E/O/D-p cloud formation is likely to be the "sweet spot" where optimum flexibility and collaboration can be achieved.
- A Proprietary cloud provider will likely want to keep you in the left side of the cube, achieved by either continuous innovation that adds value, or by limiting the means of migrating from the proprietary domain. The ability to move from that top-left cloud form to the "sweet-spot" top-right cloud form will require a rare interface because facilitating you making this move is going to be rarely in the cloud supplier's best business interests.

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

At the heart of all cloud forms is the concept of abstraction. Cloud models separate one layer of business from another, e.g. process from software, platform from infrastructure, etc. We show an example model here with four levels of abstraction; we can expect other models identifying different layers and abstraction levels to emerge to suit different business needs. Most cloud computing activities today are occurring at the lower layers of the stack, so today we have more maturity at the lower level.



Example from one customer:
An early experience of using the external proprietary cloud form represented by Amazon SC3 has involved a combination of Perimeterised Amazon virtual servers and De-perimeterised public data sets to create private results that are then repatriated to the Internal non-cloud environment.

Dimension: Insourced / Outsourced

We define 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 we show this 4th dimension by 2 colors; any of the 8 cloud forms can take either color.

Note: Few organisations that are traditionally bandwidth, software or hardware providers will be able to easily make the move to becoming Cloud Service providers. It takes a new mindset - a new culture - to be a Cloud Service Provider, just as it takes a new mindset to be a Cloud Service User. We can expect early growing pains caused by both of these transitions. This leaves a market for traditional service providers to help organisations to make this cloud transition.

Given the ease with which a user within your business can procure cloud services – just by tendering a valid credit card - it is absolutely essential that your business develops the agility to rapidly set up legally binding collaboration agreements, and to close them equally rapidly as soon as they are no longer needed[5]. Will it be possible in the future to design a cloud data capsulation approach that means if the cloud provider accepts the data capsule then they automatically accept the terms that the data came with – for example "do not process outside the data owner's national boundary"?

Note: When closing down an agreement with a provider, care should be taken to ensure that the data is appropriately deleted from the cloud service provider's infrastructure (including backups), otherwise a data leak risk will remain. "Data Repatriation" is a key new capability.

Other attributes like Offshore and Onshore are also relevant to cloud computing, but in this paper we have focused on the 4 dimensions identified in our Cloud Cube Model.

Background / rationale

Key questions customers need to ask their Cloud Computing suppliers so as to be confident that they are securely collaboratively enabled and compliant with applicable regulations:

1. Where in our cloud cube model is my cloud supplier operating when providing each of their services?[6]
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.

[5] See COA paper: Trust Levels - Business Impact Level, available from the Jericho Forum publications page at http://www.opengroup.org/jericho/publications.htm . We expect this agility will require automated set-up and close-down of contractual agreements.

[6] This matters not just in terms of the characteristics of each cloud form, but also is driven by regulatory requirements that will need to be maintained up-to-date, not least to align with and account for the changes that cloud computing is bringing.

It's important for business managers in their decision-making:

- To understand how and why using any cloud form will return the value-add they want to achieve
- To set out their Cloud Computing requirements clearly, and know what to expect as a result, so they can achieve the great benefits that cloud computing can offer. Entering into any cloud form without establishing the actual business objectives – especially what collaborative flexibility and security they want - may well result in significant problems.
- Moving data, both sensitive and confidential, into the cloud also has legal and compliance issues. These too should be fully understood by all parties before the decision to move to a cloud service is made. It may be that while the cost associated with the cloud service is significantly lower, the business risk is too high.

Challenges to the industry

The major cloud services providers (including Google, Amazon, Salesforce.com, Yahoo) should work with the infrastructure suppliers (including Symantec, IBM, HP, Cisco, Juniper, Microsoft, SAP, TATA), and the Jericho Forum and other relevant consumer interest groups, to develop the services, solutions, and open standards-based interfaces, that customers need for secure open cloud computing (i.e. the right-hand side of the Cloud Cube Model).

These solutions should be based on the Jericho Forum's commandments (design principles) and COA Framework. Cloud computing has undoubted business capabilities and advantages for each cloud formation, and the Jericho Forum's COA Framework explains how to provide the business view. Cloud computing also has the potential to provide the right technical enabling and control capabilities for safe and secure business collaboration, and again the Jericho Forum's COA Framework describes the key technology components involved.

Working in common cause on these areas, the industry can build management of trust into cloud computing, so that everyone prospers – safely and securely - in all cloud formations.

The way forward

We need to provide examples of practical business uses of each cloud form, in use-cases which illustrate the exploitation of the distinguishing features of each of the cloud forms described in this paper. Use-case examples are the subject of another Jericho Forum paper.

Note that the dimensions used in this paper to define cloud forms are primarily business decisions, which may or may not be supported by technologies. Architectural and technology questions to support secure Cloud Computing lie at the next level down from defining these Cloud Cube dimensions. For example, we anticipate that you can't get to that sweet spot in the top right cloud formation – and probably all cloud formations - without appropriate cloud based identity, reputation, authentication, access & authorisation, and governance & compliance. These issues are among the many related topics requiring further study.