



# **Cloud's Illusions: Jericho Forum future direction**

Stephen T. Whitlock

Representing the

Board of Management of the Jericho Forum

# Briefest Introduction to the Jericho Forum

- In 2005 we began by alerting the industry to the effects of de-perimeterization
- In 2007 we started developing a "collaboration" framework (COA) to show how to architect effective solutions

**Today - we've gone a long way towards delivering these**

- The next natural step is to raise awareness and understanding on how to collaborate safely and securely in "the cloud".

## **Vision:**

To enable increased confidence and operational efficiencies in collaboration and commerce for all stakeholders in the context of emerging cloud models

## ▪ **Mission:**

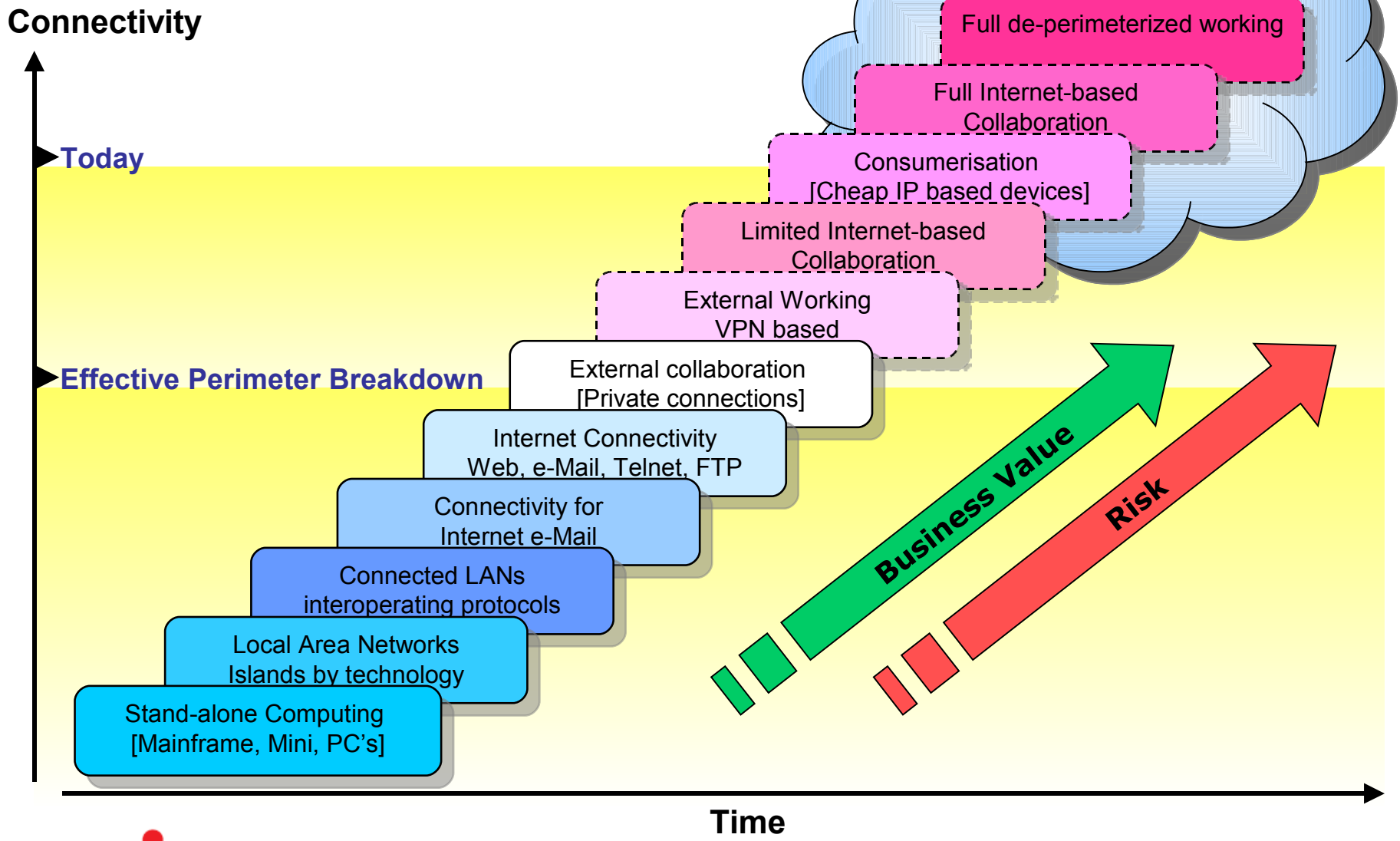
Act as a catalyst to accelerate the achievement of the collective vision

[www.jerichoforum.org](http://www.jerichoforum.org)

# Brief History

- In 2004, Jericho Forum thought leaders asked the IT industry the question:
  - *When corporate perimeters crumble due to business drivers demands for greater connectivity with collaborators over the Internet:*
    - How do you secure it?
    - How do you collaborate in it?"
- We called the crumbling perimeters problem ***deperimeterization***
- We analyzed the architectural space that needs to be secured
- We wrote "position papers" on many of these, and have delivered two key deliverables:
  - Design Principles (Jericho Forum Commandments)
    - Questions that evaluate how far IT architecture meets the criteria for secure operation in a deperimeterized environment
    - The implications are that that your IT systems should work the same way irrespective of whether you are inside or outside your corporate perimeter
  - Collaboration Oriented Architectures (COA) Framework
    - Identification of key components that need to be considered when designing a secure architecture
    - A practical blueprint showing an organization how to create the right architecture for secure business collaboration in their enterprise.

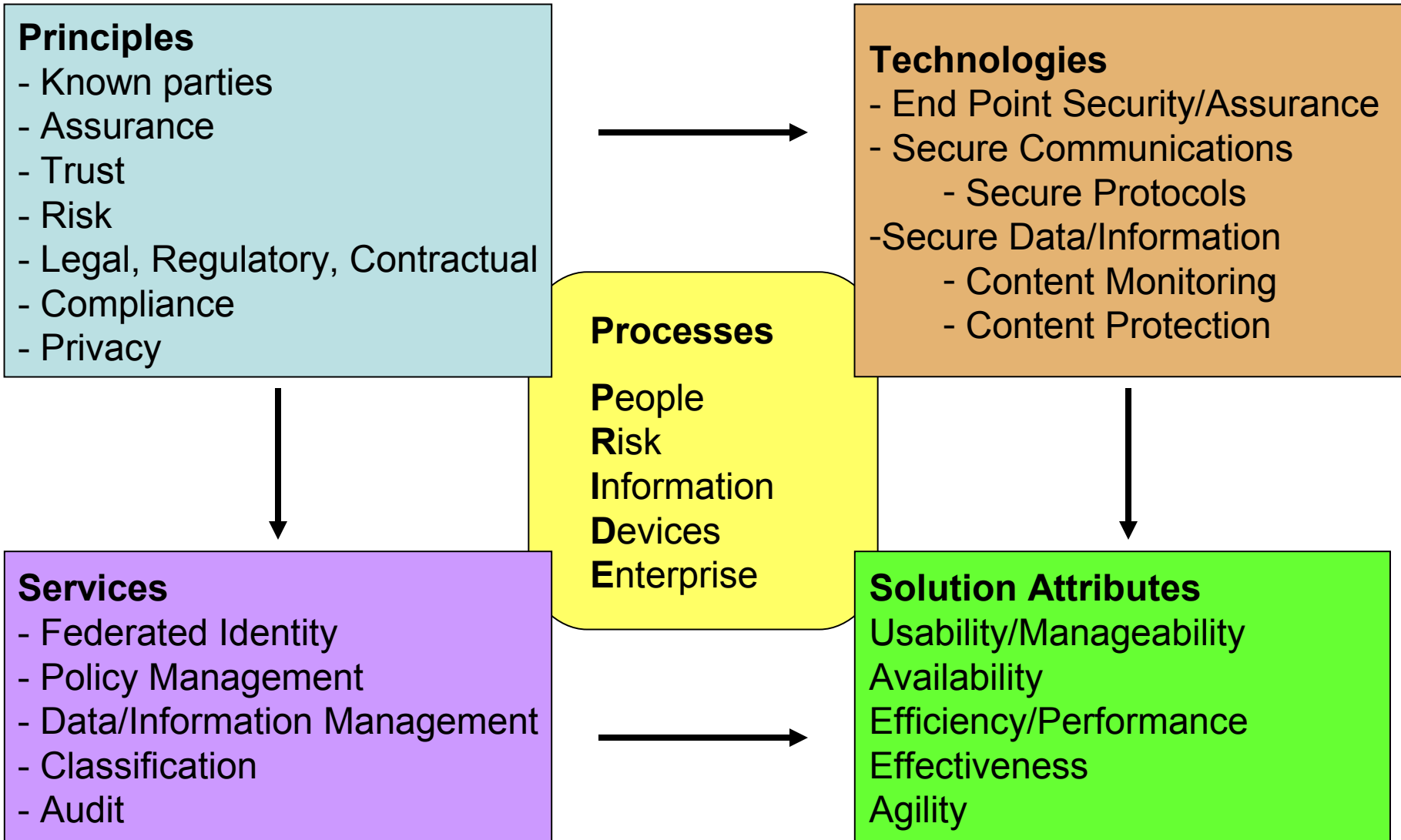
# From Connectivity to Collaboration



# Collaboration Oriented Architectures - COA

- The Collaboration Oriented Architectures framework lays out a set of design principles focusing on
  - Protection against security challenges caused by increased collaboration
  - Leveraging the business potential offered by Web 2.0 and other externalization technologies
- This practical blueprint is geared to showing each organization how to architect for safe business collaboration in a way that fits its individual needs
- Implementing COA builds upon existing standards and practices to enable effective and secure collaboration
- Developing a set of best practice principles addressing secure collaboration in the cloud is the obvious – and indeed important – next goal for us

# COA Components – Architect's View



## Types of Collaboration

- One size doesn't fit all - each organization needs
  - A clear vision of their business objectives
  - Necessary services – communication, conferencing, workflow, management, etc.
  - The collaboration oriented architecture they need to design to securely meet those objectives
- COA is a blueprint geared to showing an organisation how to create the right architecture for secure business collaboration.

# Collaboration Capability

## Collaboration Capability

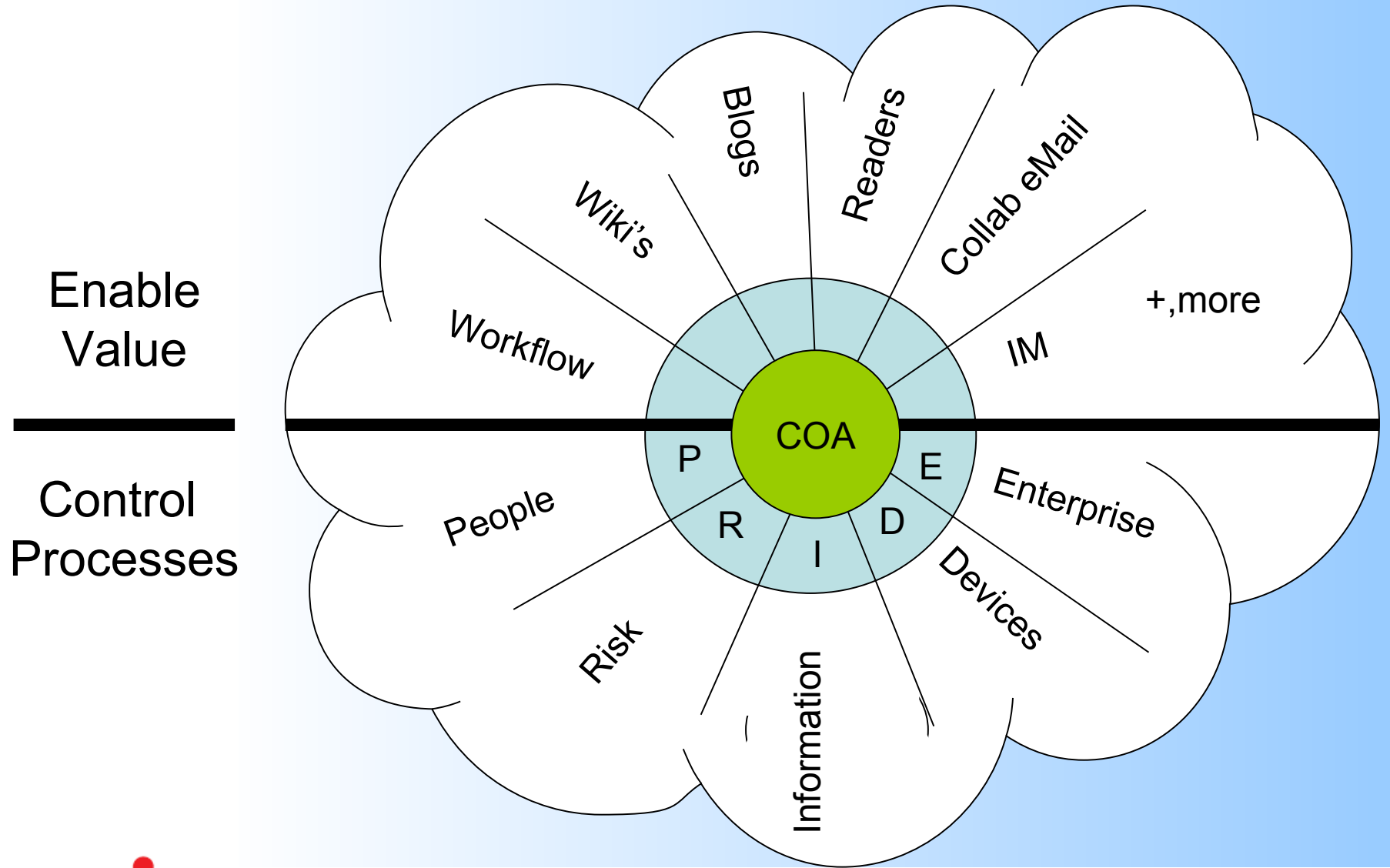
Integrated Development  
Shared Workspace  
Shared Workflow  
Shared Resources  
Web Access  
Information Exchange  
Direct Access  
Co-Location

## Enabling Technology

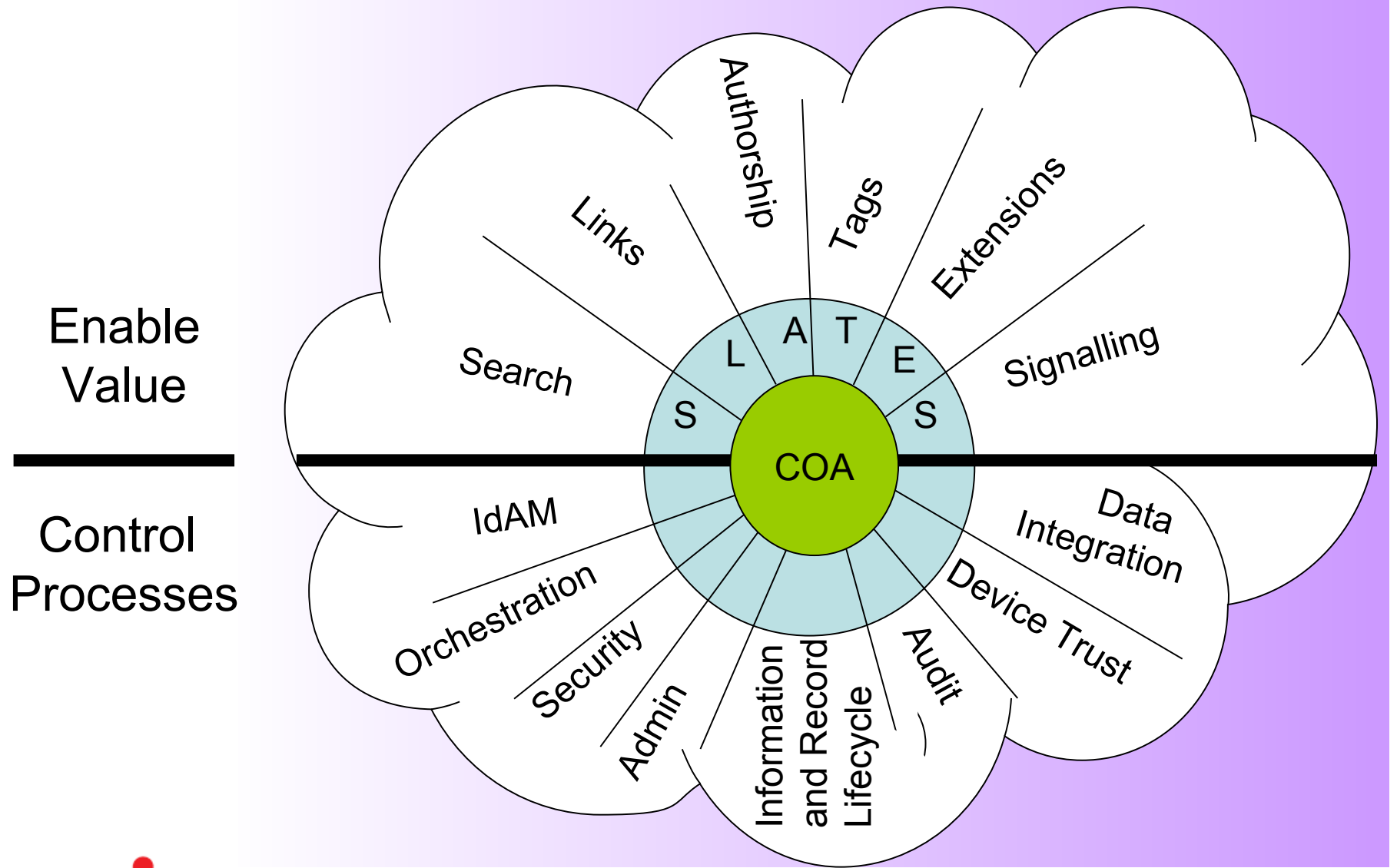
Cloud Computing  
Grid Computing  
Web 2.0  
Orchestration  
SOA / SAAS  
Publishing  
Messaging  
Remote Session  
Physical Access



# Cloud Computing: The Business View



# Cloud Computing: The Technical View



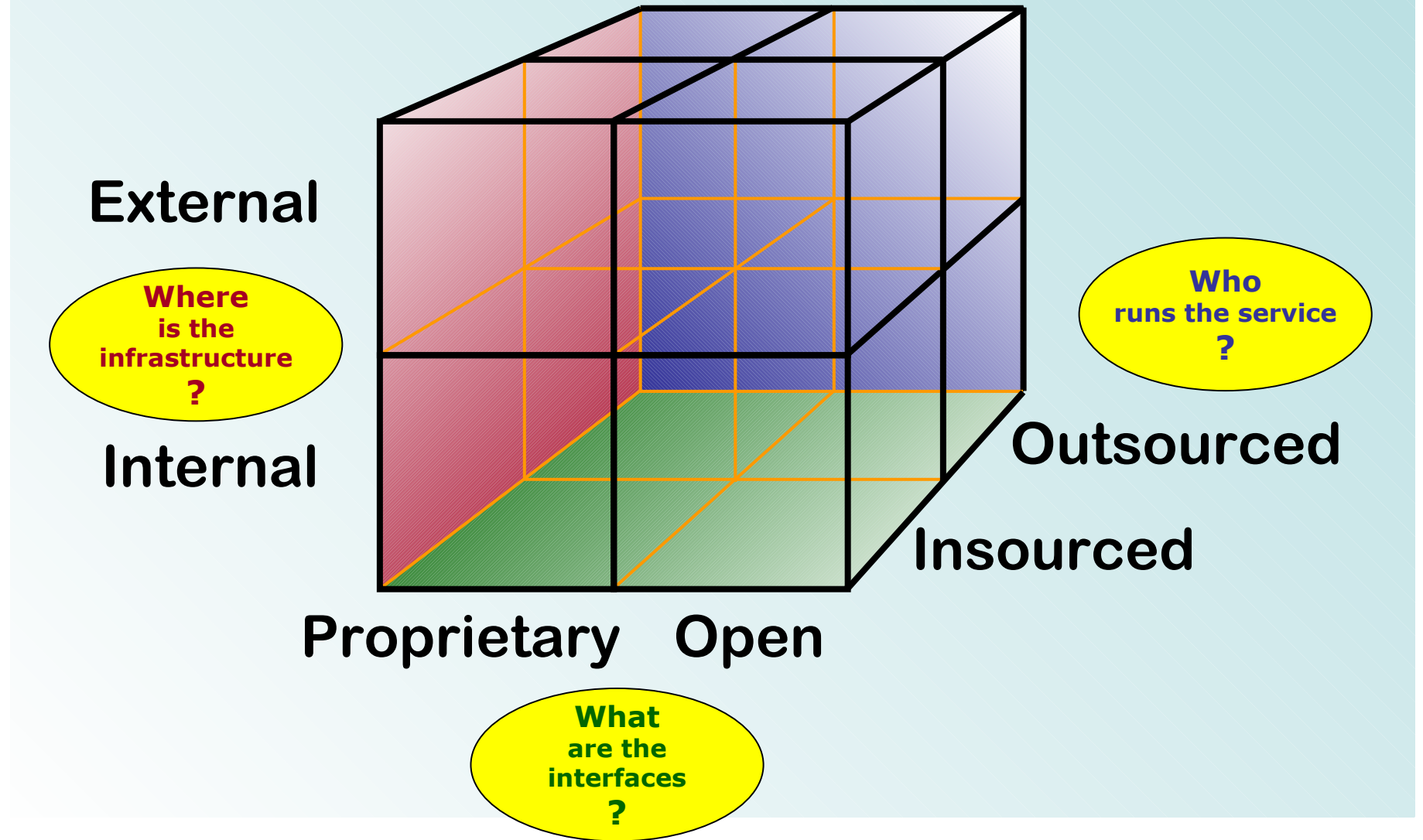
# Business Drivers for Cloud Computing

- **Cost**
  - Pay for what you actually use. No hardware or startup costs
- **Flexibility**
  - Use CC services when needed
  - Dynamically grow and shrink services
- **Simplicity**
  - Typically browser based user interfaces
- **Response**
  - Fast provisioning and de-provisioning
- **Availability**
  - Many cloud service providers have global, robust network, CPU and application capability

# Cloud Computing Services Summarized

- **Business Services** - Interoperable machine-to-machine interaction over a network accessed by other cloud computing components, or directly by end users
  - Identity (OAuth, OpenID)
  - Integration (Amazon Simple Queue Service)
  - Payments (Amazon Flexible Payments Service, Google Checkout, PayPal)
  - Mapping (Google Maps, Yahoo! Maps)
  - Search (Alexa, Google Custom Search, Yahoo! BOSS)
  - Others (Amazon Mechanical Turk)
- **Application** - Cloud based software, that often eliminates the need for local installation
  - Peer-to-peer / volunteer computing (Bittorrent, BOINC Projects, Skype)
  - Web application (Facebook)
  - Software as a service (Google Apps, Salesforce)
  - Software plus services (Microsoft Online Services)
- **Infrastructure** - Computing infrastructure, typically a platform virtualization environment, as a service
  - Full virtualization (GoGrid, Skytap)
  - Grid computing (Sun Grid)
  - Management (RightScale)
  - Compute (Amazon Elastic Compute Cloud)
- **Platform** - The delivery of a computing platform, and/or solution stack as a service
  - Web application frameworks
    - Ajax (Caspio)
    - Python Django (Google App Engine)
    - Ruby on Rails (Heroku)
  - Web hosting (Mosso)
  - Proprietary (Azure, Force.com)
- **Storage** - Data storage as a service, often billed on a utility basis, e.g., per gigabyte per month.
  - Database (Amazon SimpleDB, Google App Engine's BigTable datastore)
  - Network attached storage (MobileMe iDisk, CTERA Cloud Attached Storage, Nirvanix CloudNAS )
  - Synchronization (Live Mesh Live Desktop component, MobileMe push functions)
  - Web service (Amazon Simple Storage Service, Nirvanix SDN)

# Cloud Property Model



# Information Protection Challenges

Data becomes free  
of infrastructure

## Cloud Computing

Externalized SOA

**DATA** is trusted to third party services

Data location unknowable

## SOA

Client-server with relaxed protocols –

User defined to self describing protocols

Return of time share but **DATA** is everywhere

## Distributed Client-Server

Multiple computers

Move Computing to the **DATA**

Data location independence

## Time Share

Single computer - Time independence

Move **DATA** to the Computer

Data not only had value but lived in the care of others

## Stand Alone

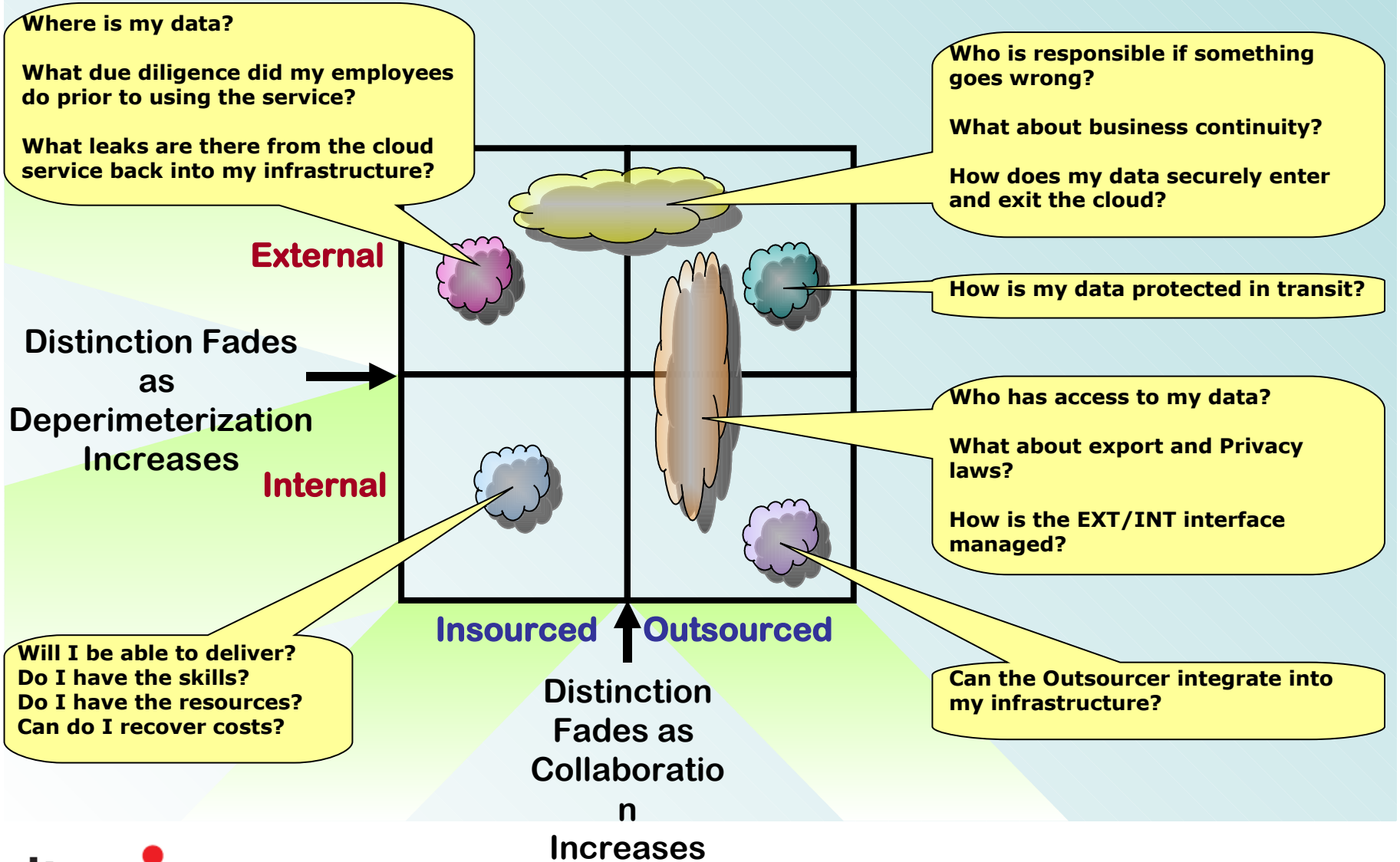
Single user

Minimal **DATA**

Creation of concept that data was a repository of value

Time

# Security Questions

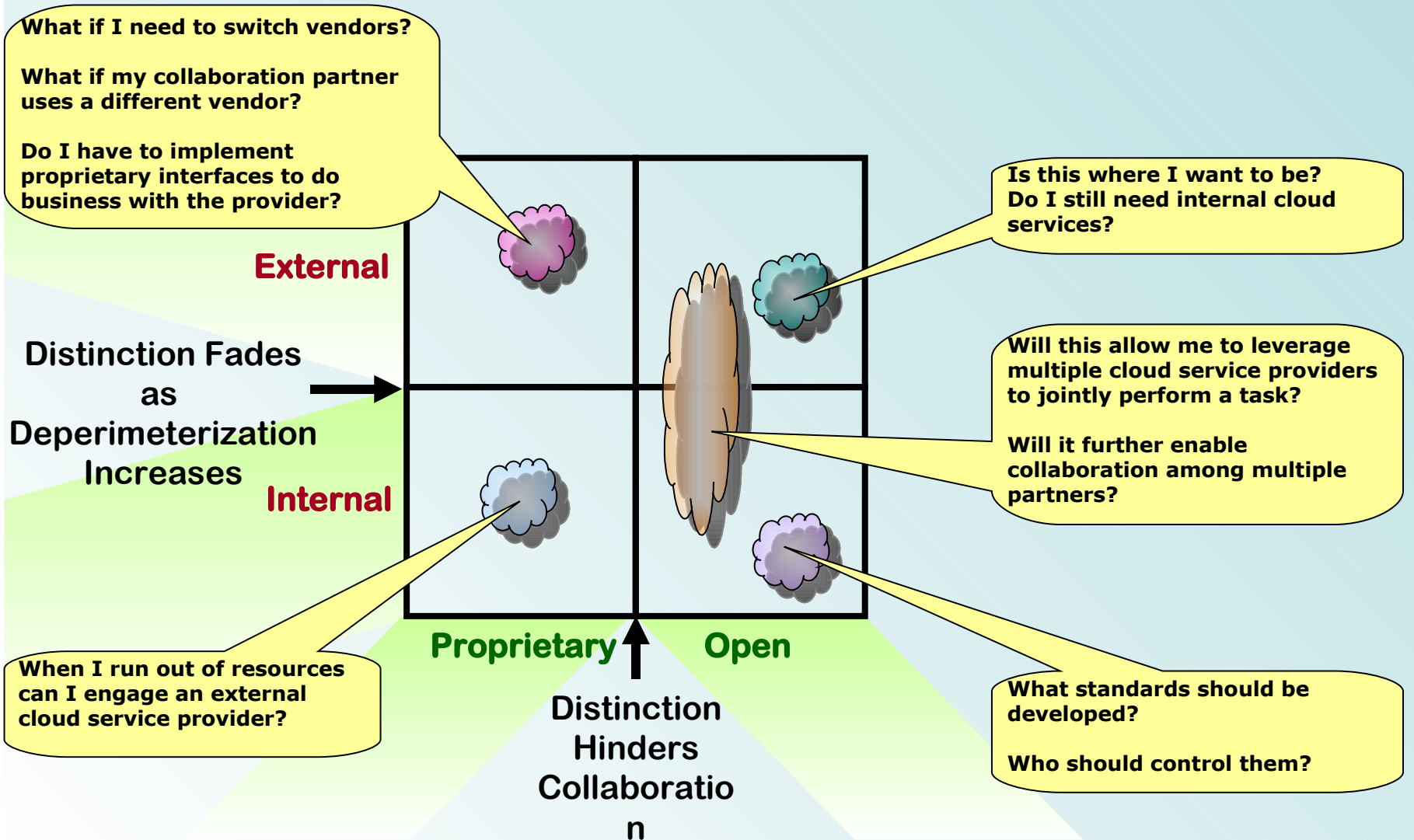


# Cloud Computing Risks (Gartner)

- **Privileged user access** - Sensitive data processed outside the enterprise brings with it an inherent level of risk, because outsourced services bypass the "physical, logical and personnel controls" IT shops exert over in-house programs.
- **Regulatory compliance** - Customers are ultimately responsible for the security and integrity of their own data, even when it is held by a service provider. Traditional service providers are subjected to external audits and security certifications. Cloud computing providers who refuse to undergo this scrutiny are "signaling that customers can only use them for the most trivial functions."
- **Data location** - When you use the cloud, you probably won't know exactly where your data is hosted. In fact, you might not even know what country it will be stored in.
- **Data segregation** - Data in the cloud is typically in a shared environment alongside data from other customers. Encryption is effective but isn't a cure-all. "Encryption accidents can make data totally unusable, and even normal encryption can complicate availability."
- **Recovery** - Even if you don't know where your data is, a cloud provider should tell you what will happen to your data and service in case of a disaster. "Any offering that does not replicate the data and application infrastructure is vulnerable to a total failure."
- **Investigative support** - Investigating inappropriate or illegal activity may be impossible in cloud computing, Gartner warns. "Cloud services are especially difficult to investigate, because logging and data for multiple customers may be co-located and may also be spread across an ever-changing set of hosts and data centers.
- **Long-term viability** - Ideally, your cloud computing provider will never go broke or get acquired and swallowed up by a larger company. But you must be sure your data will remain available even after such an event.



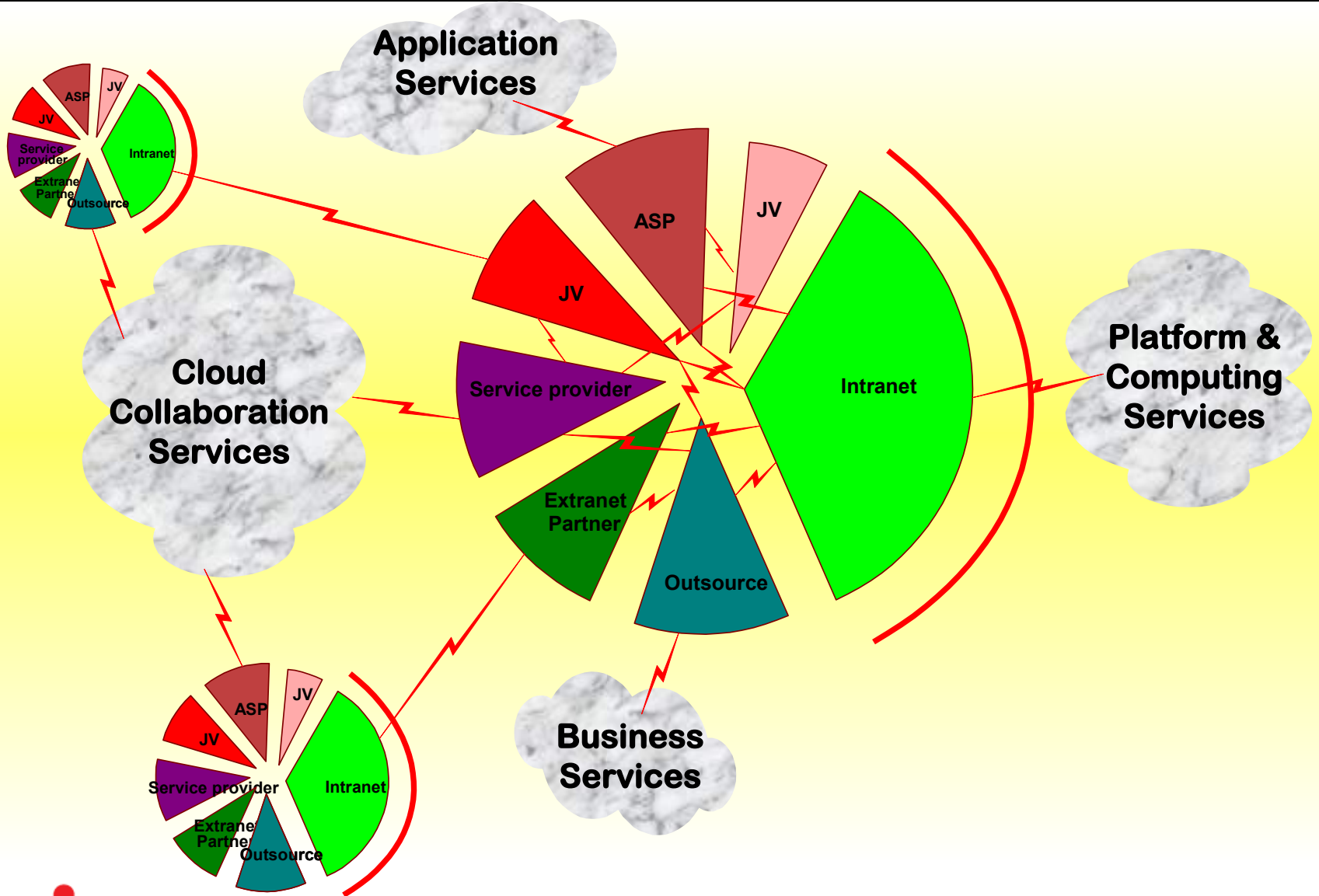
# Interoperability Questions



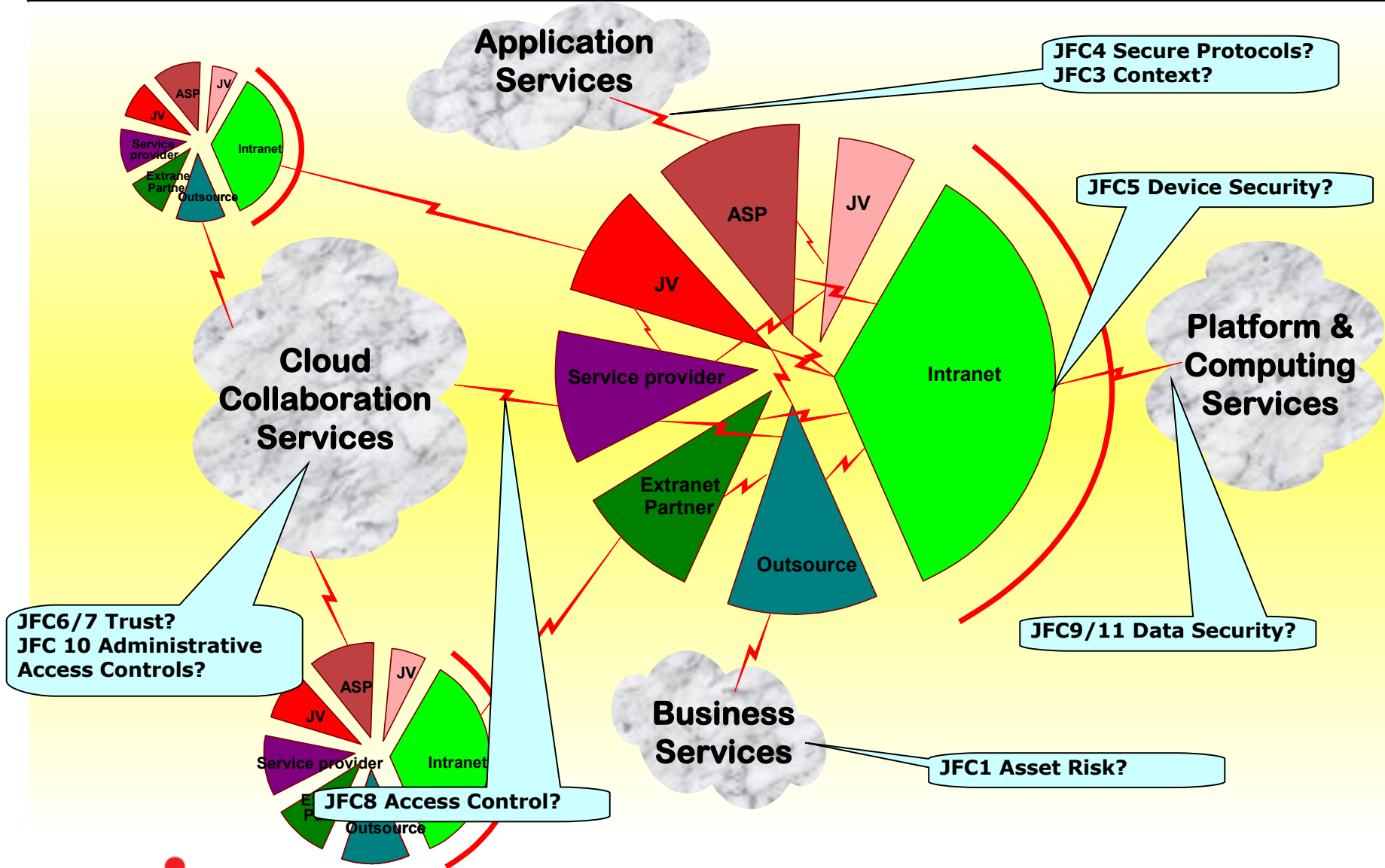
## Who Owns What?

- James Urquhart's Cloud Computing Bill of Rights
  - Article I: Customers Own Their Data
  - Article II: Vendors and Customers Jointly Own System Service Levels
  - Article III: Vendors Own Their Interfaces
- Lack of interface standardization will hinder flexibility, agility and expanded cloud service offerings such as collaboration

# Cloud Service Examples



# Jericho Forum Commandment Applicability



# Jericho Forum Activity

- Like many others, we see huge potential and benefits for moving into "the cloud"
- But we advise not leaping in their before understanding the:
  - Risks
  - Security issues
  - Interoperability issues
  - Business rationale
- The Jericho Forum is taking a lead on:
  - Analyzing the issues
  - Raising awareness
  - Establishing clear requirements
- Goal: Make the cloud a safe place to collaborate

# Summary

## ■ Security

- Cloud computing is the natural evolution of the deperimeterization environment and amplifies the associated risks
- To leverage cloud computing products and services for collaboration, they must be designed survive on the open Internet

## ■ Interoperability

- The long term business driver for cloud computing is collaboration
- Proprietary approaches will cause value of using the cloud to support collaboration to evaporate

# What Does This Mean to You?

- Remember – just like deperimeterization:
  - This is happening NOW
  - It is inevitable ... today's business drivers are taking us there
    - Large financial savings
    - Resource agility
    - Sophisticated collaboration
  - Will you prepare for it now, or wait and hope it's someone else's problem when it hits?
- Do you have a share in this challenge?
- Are you interested in finding out the new ideas and innovative thinking that will evolve from taking a serious analytical approach to addressing it?
  - If so, the Jericho Forum is the place to be

