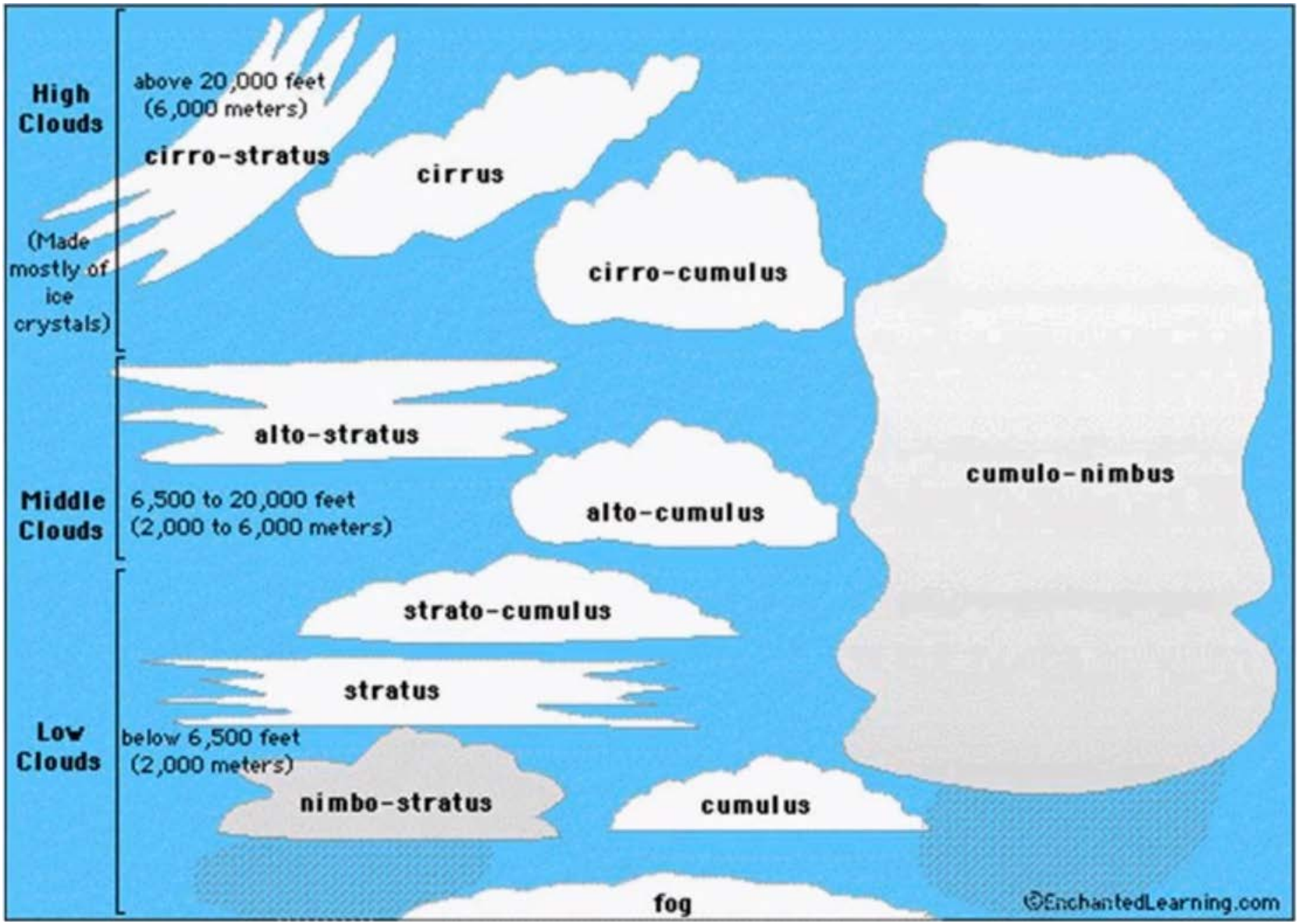
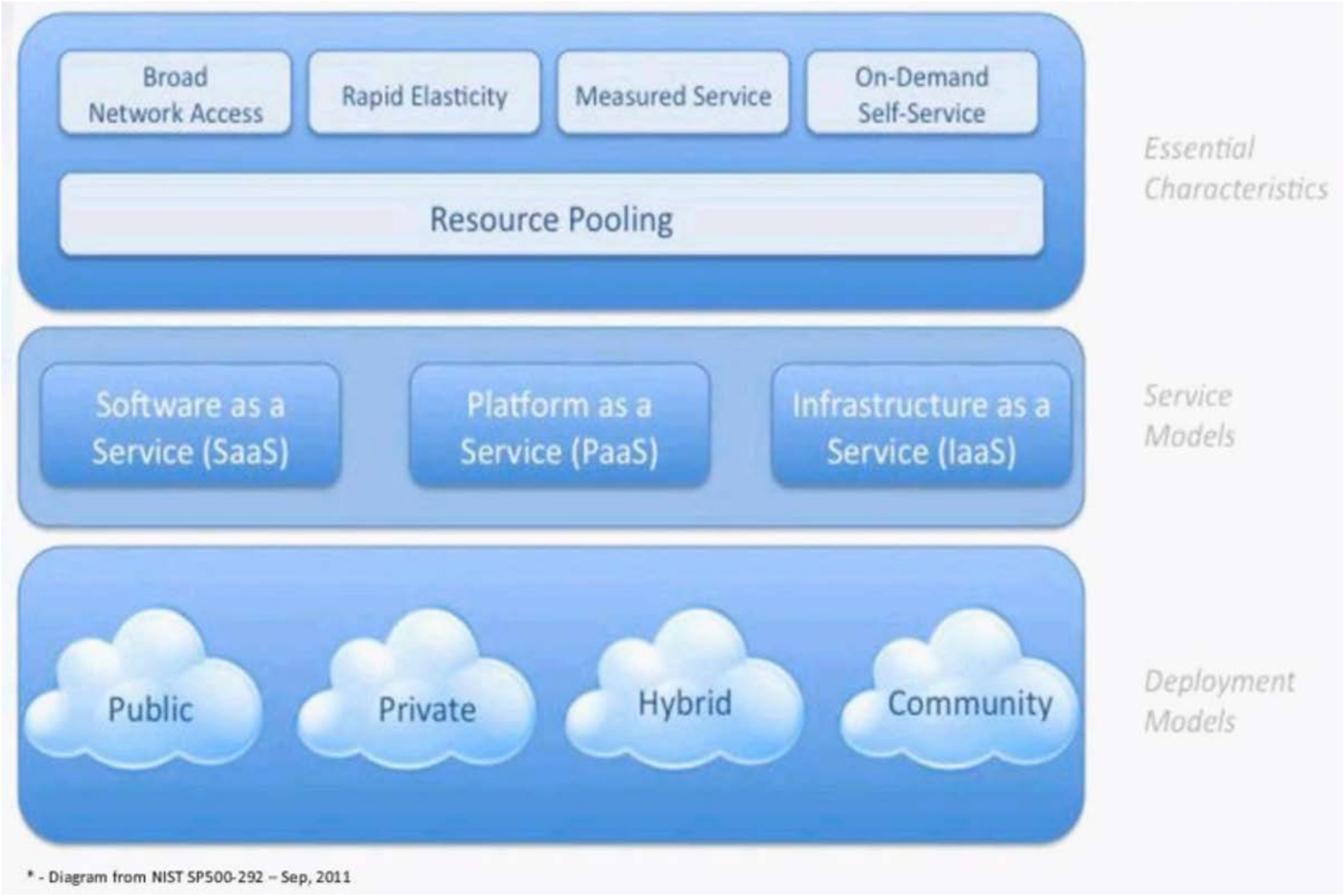
The Challenge of Cloud Security

Dr. Ray Klump
Chair, Mathematics & Computer Science
Director, MS in Information Security
Lewis University


High Clouds
above 20,000 feet
(6,000 meters)
cirro-stratus
cirrus
cirro-cumulus
(Made mostly of ice crystals)
alto-stratus
cumulo-nimbus
Middle Clouds
6,500 to 20,000 feet
(2,000 to 6,000 meters)
alto-cumulus
strato-cumulus
stratus
Low Clouds
below 6,500 feet
(2,000 meters)
nimbo-stratus
cumulus
fog
©EnchantedLearning.com


Broad Network Access
Rapid Elasticity
Measured Service
On-Demand Self-Service
Resource Pooling
Essential Characteristics
Software as a Service (SaaS)
Platform as a Service (PaaS)
Infrastructure as a Service (IaaS)
Service Models
Public
Private
Hybrid
Community
Deployment Models
* - Diagram from NIST SP500-292 – Sep, 2011

Poll Question #1:

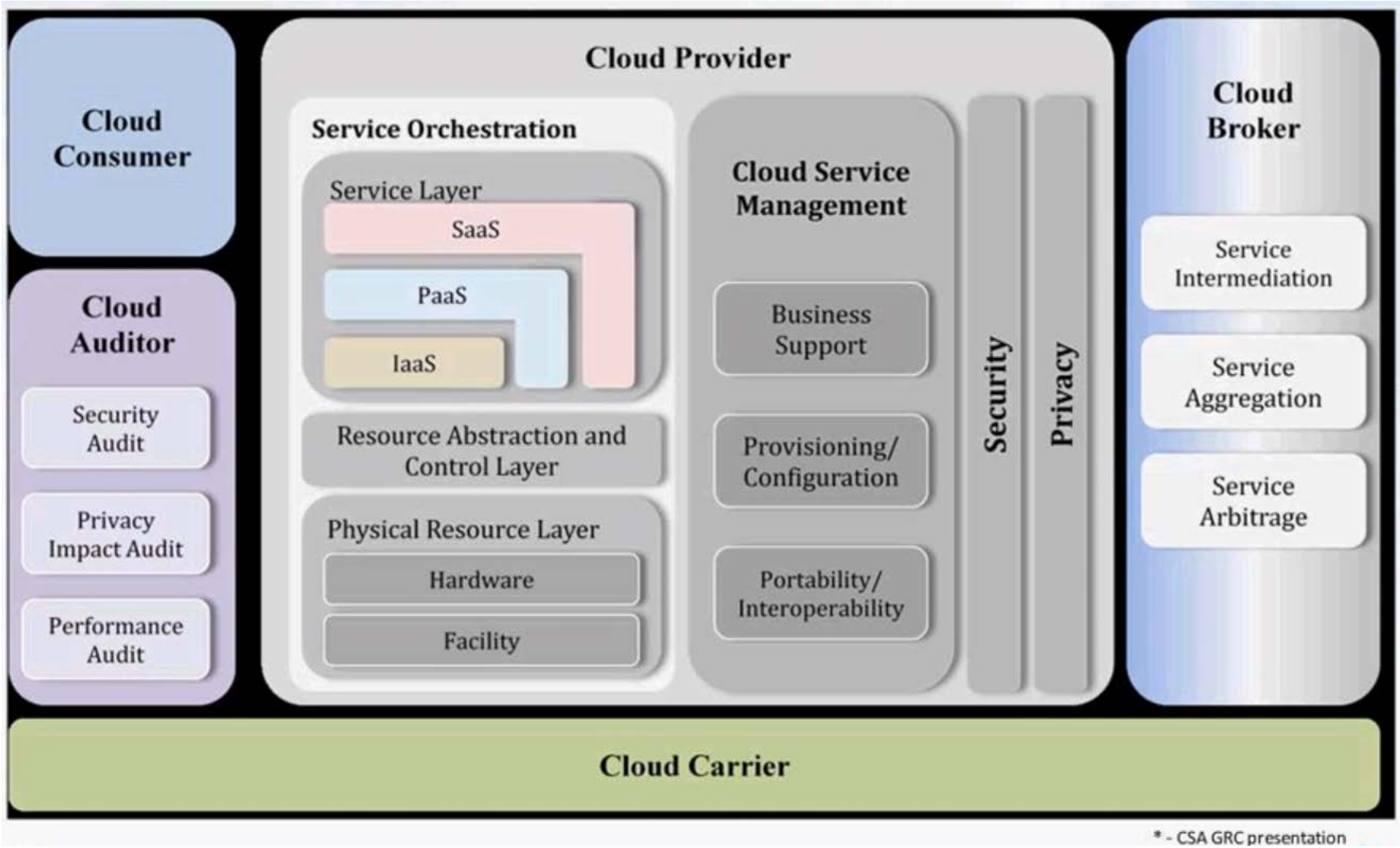
What type of cloud service are you currently using?

a) SaaS (Software as a service)

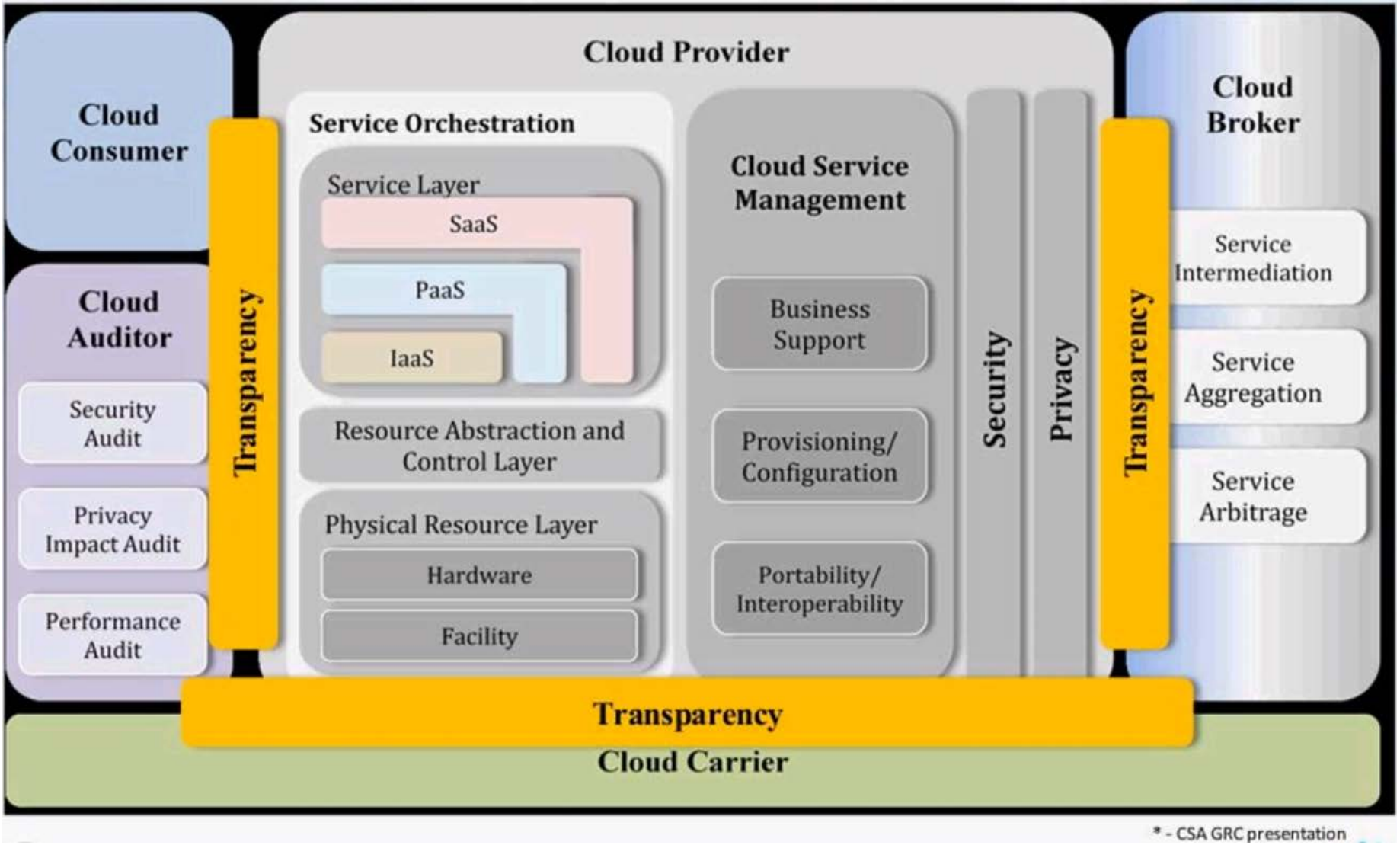
b) PaaS (Platform as a service)

c) IaaS (Infrastructure as a service)

d) None



* - CSA GRC presentation



* - CSA GRC presentation

Cloud consumers also have a responsibility to know what they want.

Understand your tolerance for risk.

Know your audience.

Migrate vs. Build New

Understand interdependencies

Governance

IT has to start thinking differently: new technologies and techniques for managing, securing, and monitoring data in the cloud.

Poll Question #2:

Why are you going to the cloud?

a) Cost savings
b) Service availability
c) Service scalability
d) Faster turn-up
e) Your boss told you to.

There are many obstacles to adopting the cloud.

Some are the traditional challenges for adopting any new technology.

Others are specific to the cloud.

Traditional considerations

Enterprise strategy
Business function / workload
Technical architecture
Network connectivity
Application standards
Interoperability
IT and IT Risk Governance
Security Policy
Compliance management
Maintenance
Challenge to operations

Cloud-Specific Concerns

Private, community, public, or hybrid?

Adjusting your security policy to include the cloud. How does it jive with the cloud provider?

Compliance and the cloud

Top Threats

Trust

Data leakage and unfriendly geography

Insecure cloud software

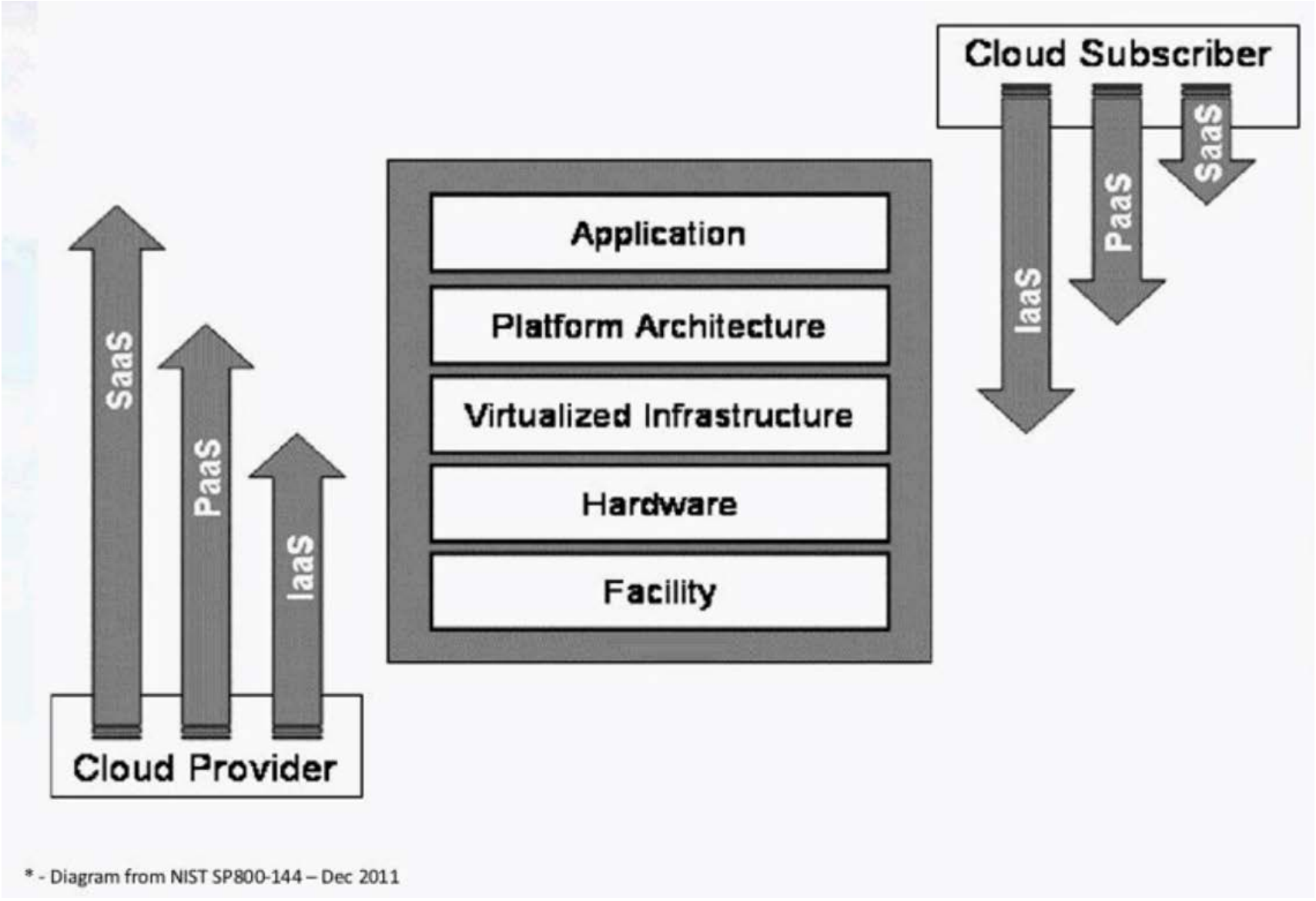
Who holds the keys?

Malicious use of cloud services

Account / service hijacking

Malicious insiders

Cloud-specific attacks



* - Diagram from NIST SP800-144 – Dec 2011

The top security issue for SaaS is password management.

Address this through a SSO option managed in-house.

The top security issue for PaaS is encryption. Data should be encrypted before it leaves your enterprise.

Use a solution that will automatically encrypt sensitive information using DLP classification technology.

The top security threat for IaaS is rogue users.

Address this through governance and usage monitoring, tracking who uses what.

Poll Question #3:

What are your top concerns with the Cloud?

a) Lack of trust
b) Loss of control
c) Data security
d) Availability
e) Regulation requirements

A key question is deployment: will you use a public cloud, a private cloud, or a hybrid?

With a public cloud, you need to recognize an important reality:

Your cloud provider has to become a transparent part of your IT.

In your search for a cloud provider, you need to find one that can answer the same kinds of questions your in-house IT people would answer.

In other words, you need to be able to do the following

Confirm chain of custody for information.

Conduct investigative forensics.

Detect attempts or occurrences of illegal disclosure

Discover and enforce configurations

Monitor and manage changes, patches, vulnerabilities

Questions to ask of a cloud provider

Third-party validation (SOC-2)

Security Policies

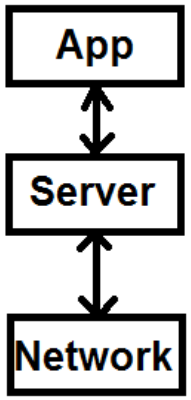
Disaster Recovery / Business Continuity

Access Controls – Physical and Virtual

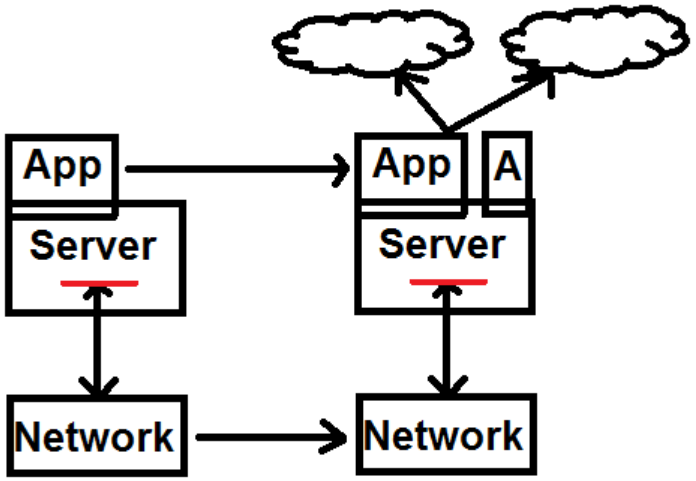
Data Protection

With a private cloud (i.e. one you manage yourself) you need to understand why things are different from traditional IT.

Traditional model



With virtualization



Poll Question #4:

In your company, the Cloud is …

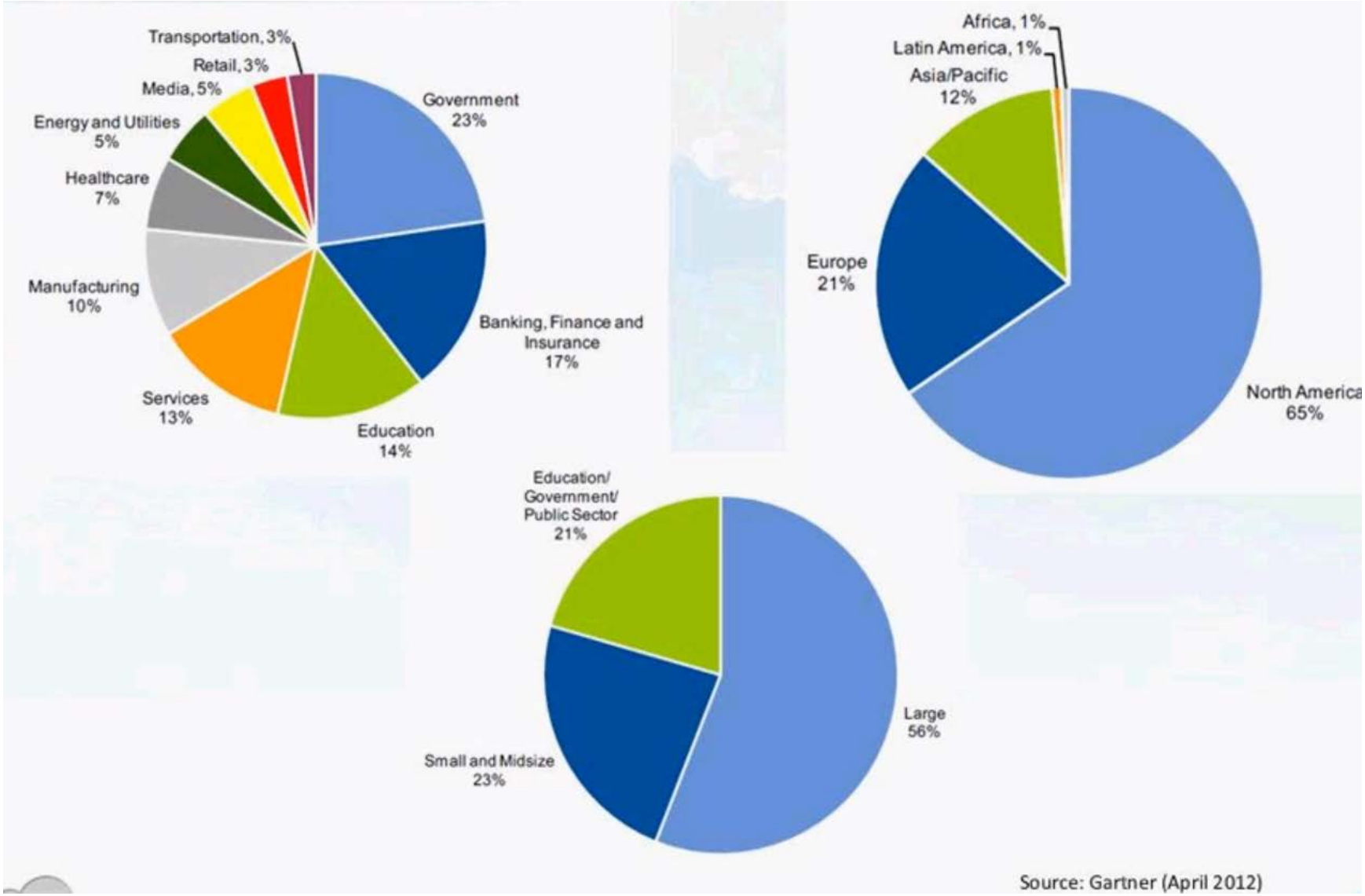
a) Mission critical

b) A playground for developers

c) Used for smaller / one-off projects

d) A mystery

Who is inquiring about cloud security?



What are some helpful resources?

NIST Publications

- SP800-144: Guidelines for Security and Privacy in Public Cloud Computing
- SP800-145: NIST Definition of Cloud
- SP500-291: Cloud Computing Standards Roadmap
- SP500-292: Cloud Computing Reference Architecture
- SP500-293: US Government Cloud Computing Technology Roadmap

Cloud Security Alliance

Security Guidance v3.0

Trusted Cloud Initiative (TCI)

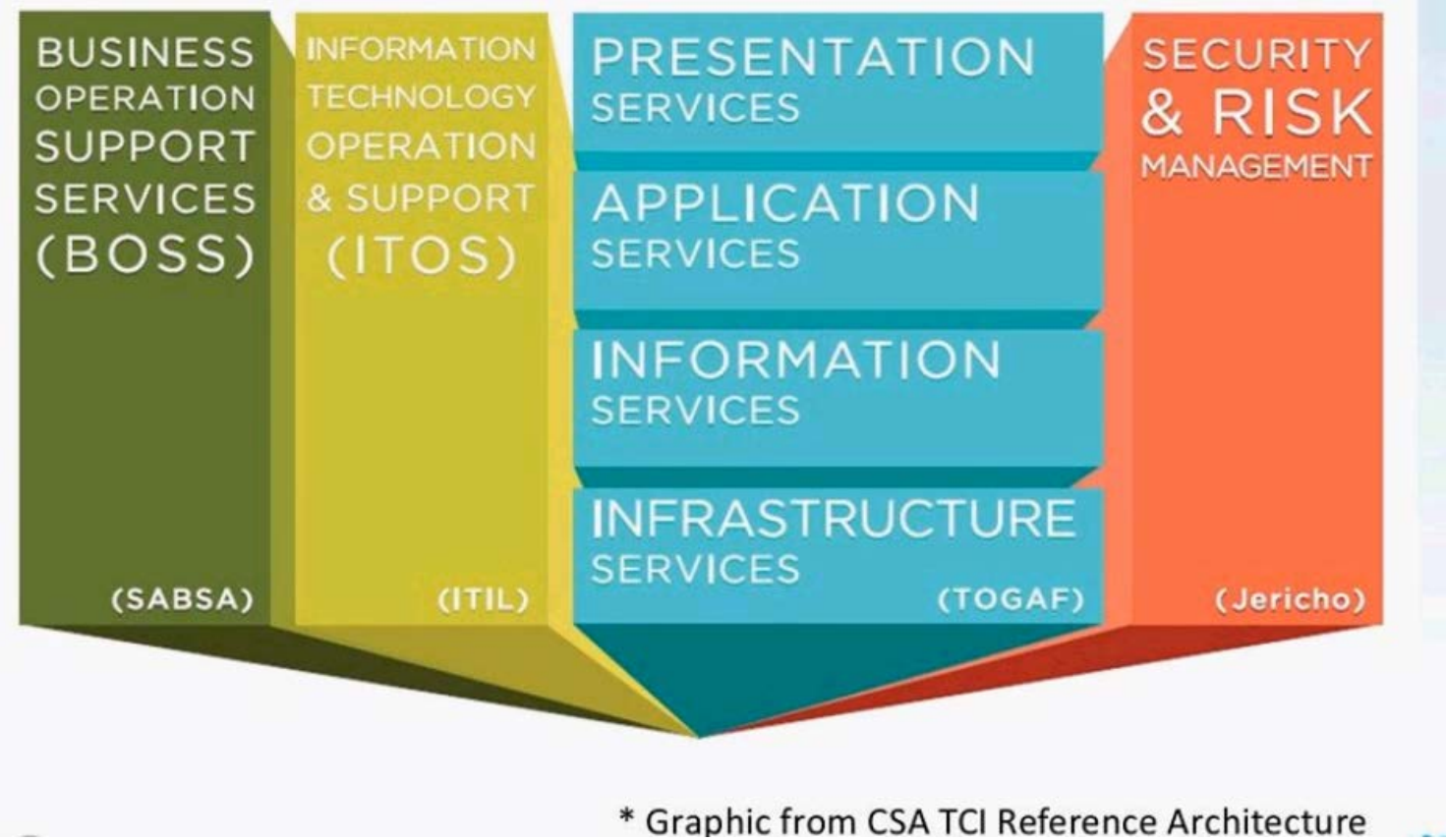
Cloud Control Matrix (CCM)

Cloud Trust Protocol (CTP)

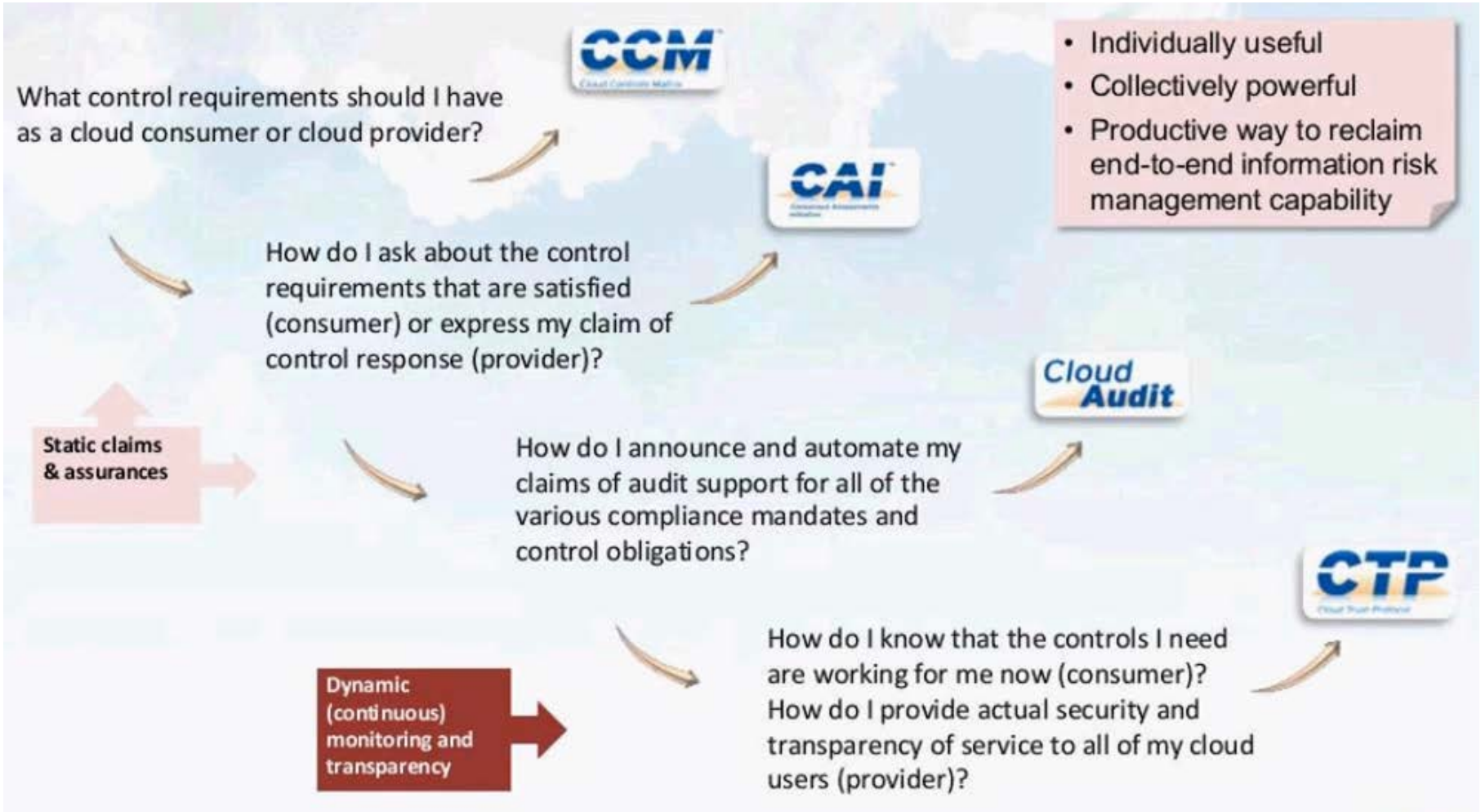
GRC Stack

Cloud Mobile

Trusted Cloud Initiative (TCI)



Governance, Risk Compliance (GRC) Framework



The cloud offers several promises, but it also presents unique and complex security challenges.

To make the most of the Cloud, you need to understand the challenges specific to your type of Cloud and how you deploy it.

The **Lewis Master of Science in Information Security program** is a unique graduate degree in Information Security.

The Lewis MSIS degree is unique in that it presents **both the managerial and technical aspects** of the problem.

This hybrid approach reflects the true nature of the information security challenge.

Students take a **shared core of courses and then specialize** in either the management track or the technical track.

Students complete their coursework by completing a **thesis or project** as well as **two CISSP review courses**.

Courses are **taught by industry professionals** as well as Ph.D.’s in Computer Science and Management Information Systems.

Most students complete the MSIS degree in **13 months to 2 years**.

For more information, contact

Dr. Ray Klump
Director, MSIS Program
Lewis University

klumpra@lewisu.edu

http://www.lewisu.edu/academics/msinfosec/index.htm