Cloud Security Alliance

Security Guidance for Critical Areas of Focus in Cloud Computing

genda

About the Cloud Security Alliance

Getting Involved

Guidance 1.0

Call to Action

out the Cloud Security Allia

Not-for-profit organization

nclusive membership, supporting broad spectrum
ubject matter expertise: cloud experts, security,
egal, compliance, virtualization, and on and on...

We believe in Cloud Computing, we want to make i
etter:

o promote the use of best practices for providing security assuran
within Cloud Computing, and provide education on the uses of Cl
Computing to help secure all other forms of computing."

etting Involved

ividual Membership (free)

- Subject matter experts for research
- Interested in learning about the topic
- Administrative & organizational help

rporate Sponsorship

- Help fund outreach, events

iliated Organizations (free)

- Joint projects in the community interest

Security Guidance for Critical Areas of Focus in Cloud Computing

Download at:

www.cloudsecurityalliance.org/guidance

Overview of Guidance

1. Architecture & Framework

verning in the Cloud

. Governance & Risk Mgt
. Legal
. Electronic Discovery
. Compliance & Audit
. Information Lifecycle Mgt
. Portability & Interoperability

Operating in the Cloud

8. Traditional, BCM, DR
9. Data Center Operati
10. Incident Response
11. Application Security
12. Encryption & Key Mg
13. Identity & Access Mg
14. Storage
15. Virtualization

ssumptions & Objectives

- rying to bridge gap between cloud adopters and ecurity practitioners
- road “security program” view of the problem
- elected domains based on both strategic and actical pain points
- ocused on differences caused by cloud models

rchitecture Framework

Not “One Cloud”: Nuanced definition critical to understanding risks & mitigation

5 principal characteristics (abstraction, democratization, services-oriented, elasticity, utility model)

3 delivery models

- Infrastructure as a Service (IaaS)
- Platform as a Service (PaaS)
- Software as a Service (SaaS)

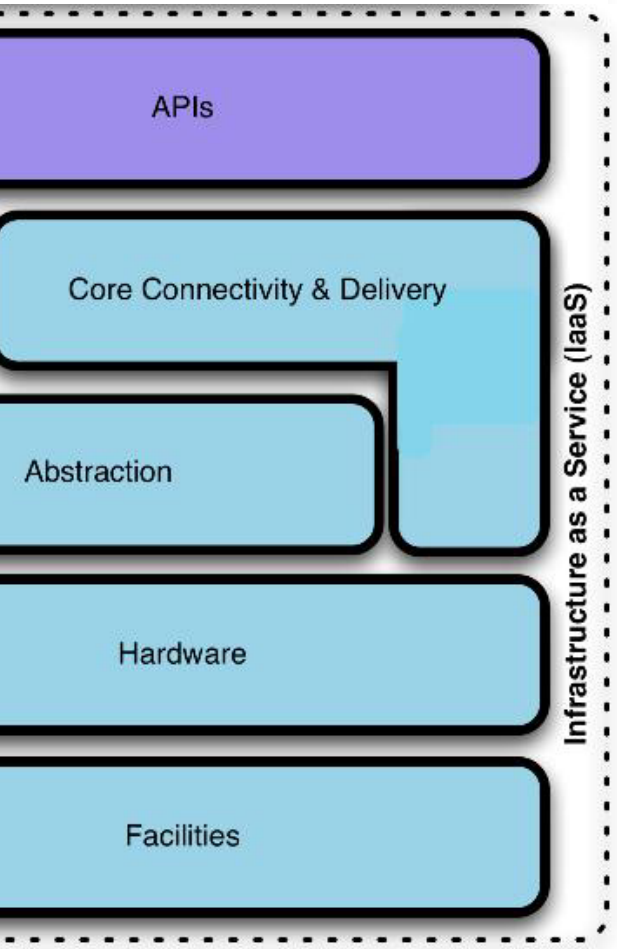
4 deployment models: Public, Private, ~~Managed~~, Hybrid

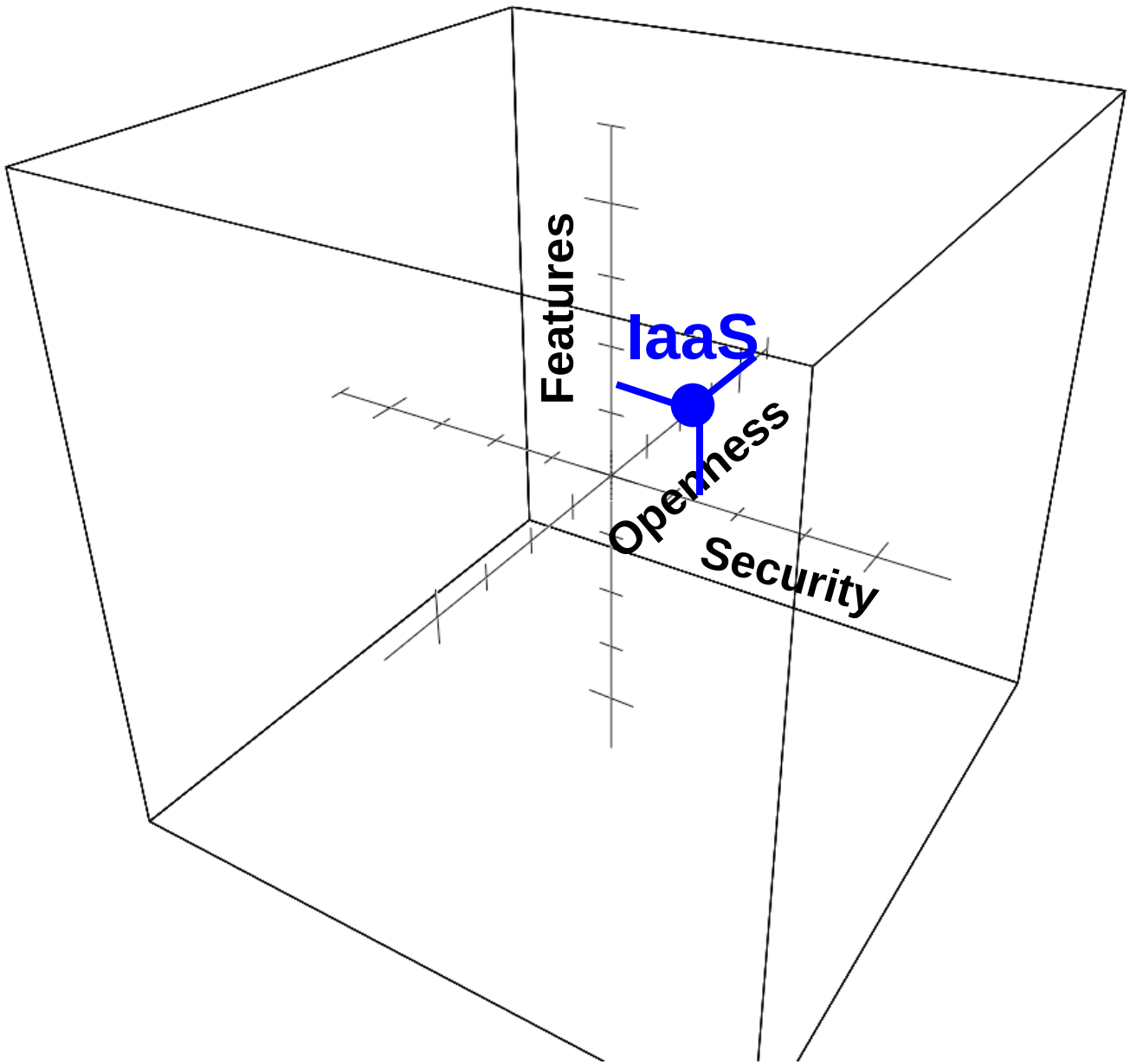
eployment Models

	Managed By[1]	Infrastructure Owned By[2]	Infrastructure Located[3]	Accessible and Consumed By[4]
Public	Third Party Provider	Third Party Provider	Off-Premise	Untrusted
Managed	Third Party Provider	Third Party Provider	On-Premise	Trusted & Untrusted
Private	Organization Third Party Provider	Organization Third Party Provider	On-Premise Off-Premise	Trusted
Hybrid	Both Organization & Third Party Provider	Both Organization & Third Party Provider	Both On-Premise & Off-Premise	Trusted & Untrusted

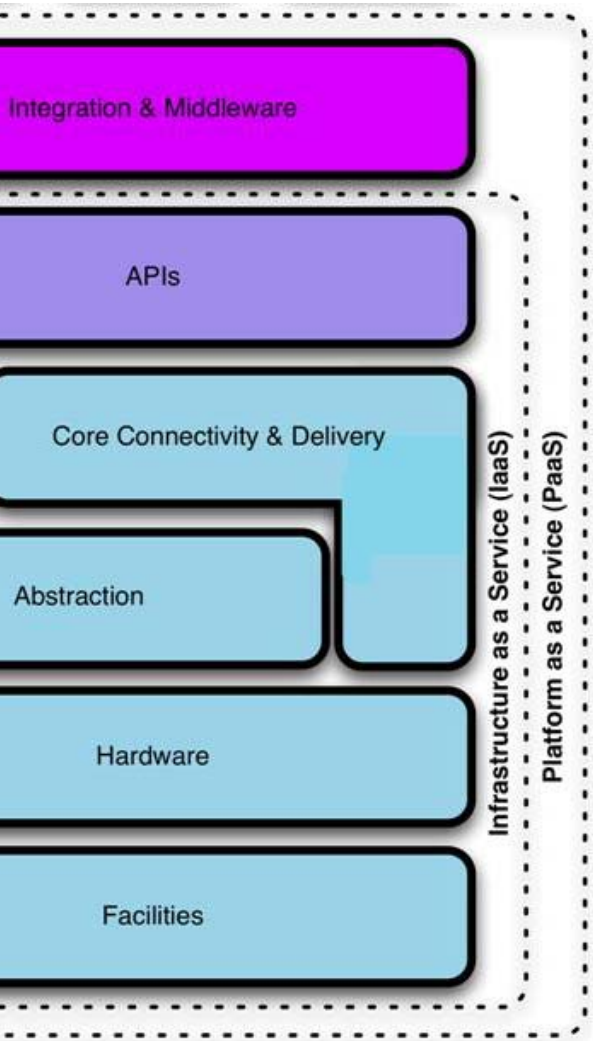
[1] *Management includes: operations, security, compliance, etc…*
[2] *Infrastructure implies physical infrastructure such as facilities, compute, network & storage equipment*
[3] *Infrastructure Location is both physical and relative to an Organization's management umbrella*
[4] *Trusted consumers of service are those who are considered part of an organization's legal/contractual umbrella including employees, contractors, & business partners. Untrusted consumers are those that may be authorized to consume some/all services but are not logical extensions of the organization.*

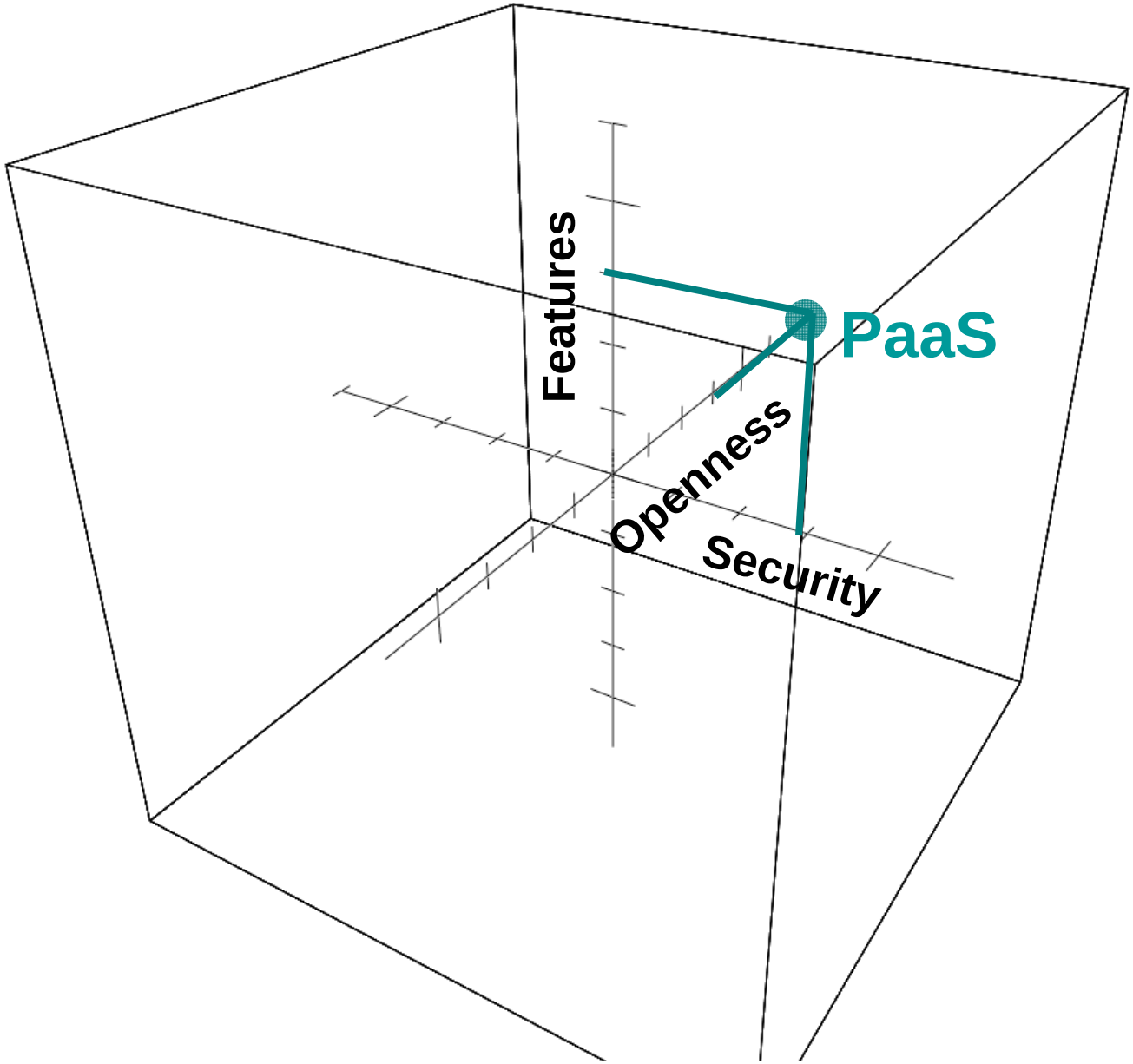
Infrastructure as a Service



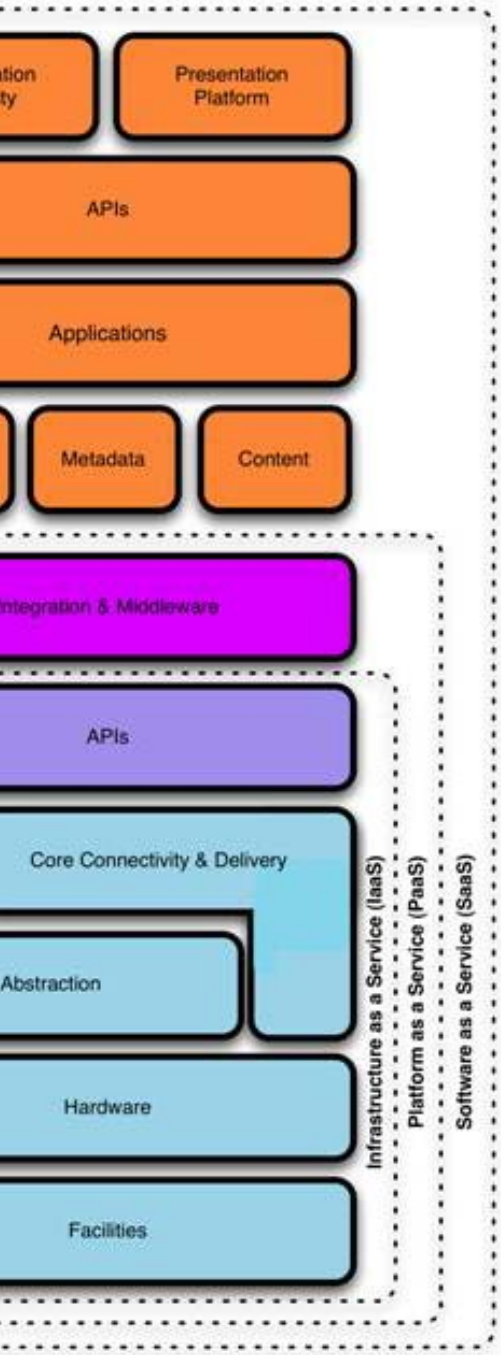


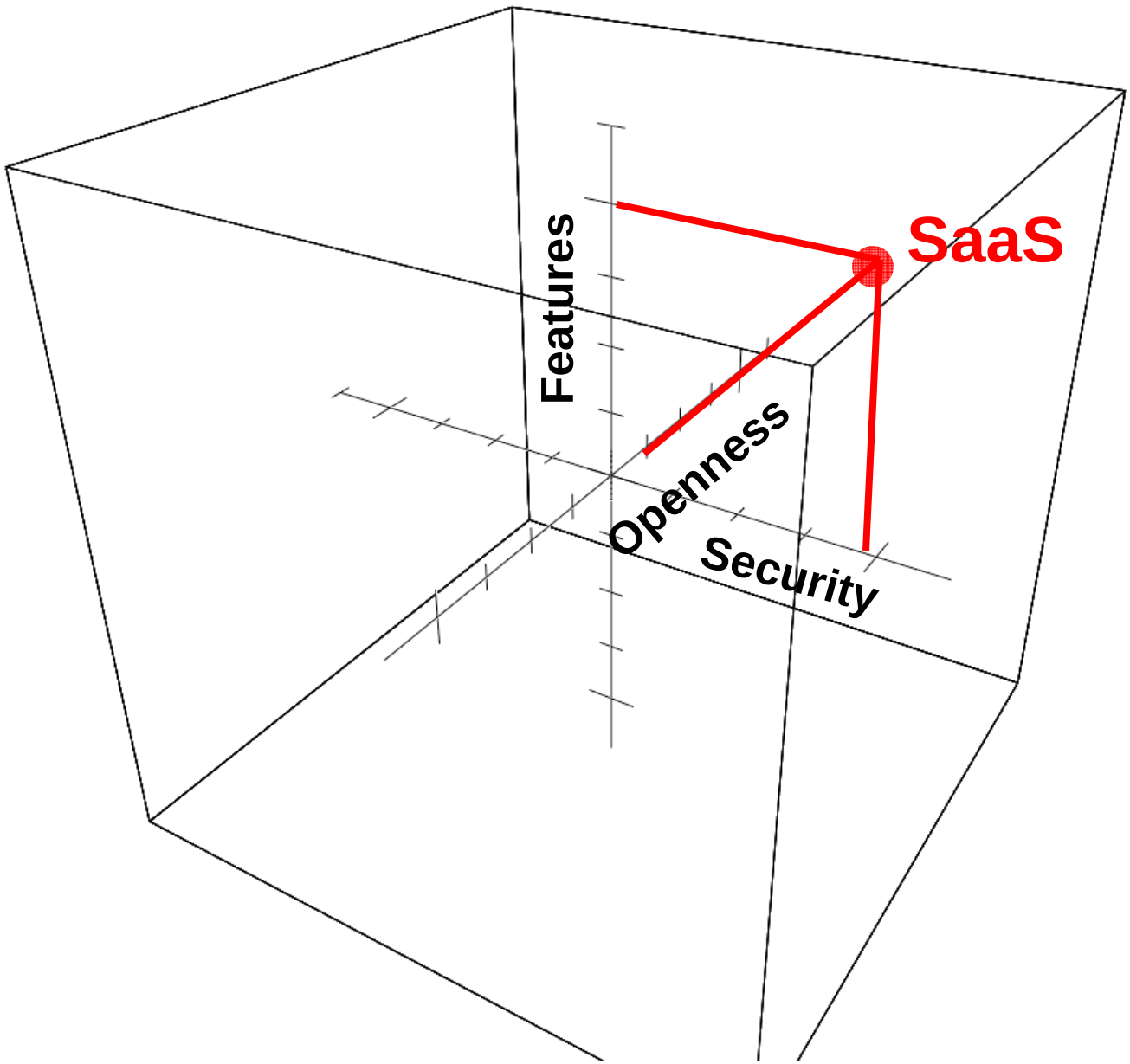
...ation as a Service





Software as a Service



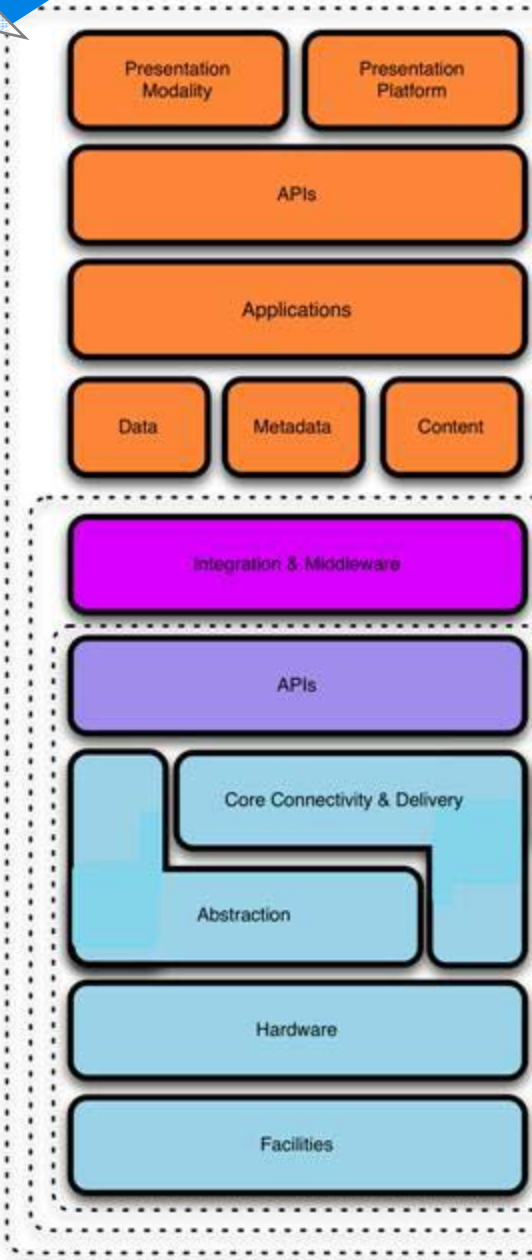


-T -T Model

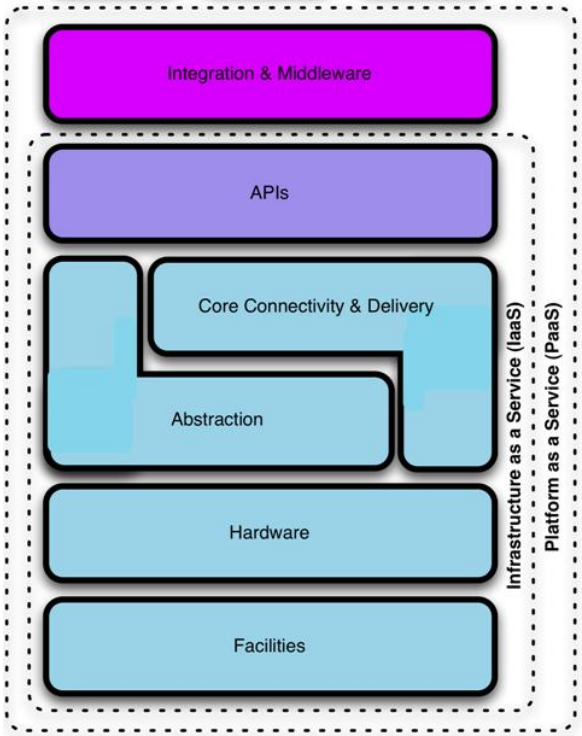
You “RFP” security in

ou build ecurity in

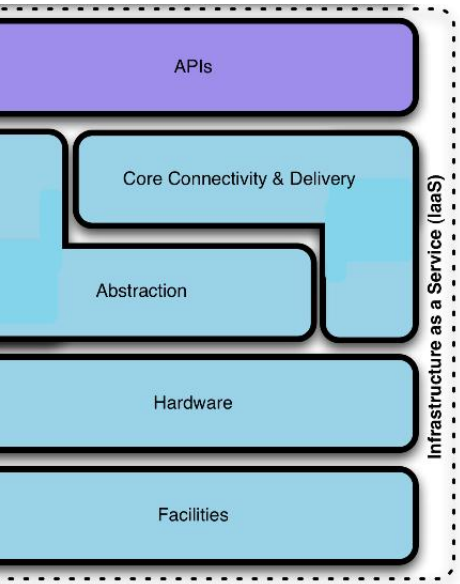
SaaS



PaaS



IaaS



Sampling From the 15 omains

overnance & ERM

- A portion of cloud cost savings must be invested in provider scrutiny
- Third party transparency of cloud provider
- Financial viability of cloud provider.
- Alignment of key performance indicators
- PII best suited in private/hybrid cloud outside of significant due diligence of public cloud provider
- Increased frequency of 3rd party risk assessments

egal

- Contracts must have flexible structure for dynamic cloud elationships
- Plan for both an expected and unexpected termination of elationship and an orderly return of your assets.
- Find conflicts between the laws the cloud provider must omply with and those governing the cloud customer
- Gain a clear expectation of the cloud provider's response egal requests for information.
- Secondary uses of data
- Cross-border data transfers

lectronic Discovery

Cloud Computing challenges the presumption that rganizations have control over the data they are legally esponsible for.

Cloud providers must assure their information security ystems are capable to preserve data as authentic and eliable. Metadata, logfiles, etc.

Mutual understanding of roles and responsibilities: litigatio old, discovery searches, expert testimony, etc.

Going forward, the Records Information Management (RI omain of knowledge must be adapted to Cloud Computi

ompliance & Audit

- lassify data and systems to understand complianc equirements
- nderstand data locations, copies
- aintain a right to audit on demand
- AS 70 Type II audits and ISO 27001 certifications robably better than nothing
- oing forward, need uniformity in comprehensive ertification scoping

nformation Lifecycle Mgt

Understand the logical segregation of information a
protective controls implemented in storage, transfe
backups; segregation of duties within personnel.

Understand the privacy restrictions inherent in data
entrusted to your company, how it impacts legality
using cloud provider.

Data retention assurance easy, data destruction ma
be very difficult.

Recovering true cost of a breach: penalties vs risk
ransference

ortabilty & interoperabilit

nderstand and implement layers of abstraction

or Software as a Service (SaaS), perform regular data extraction
nd backups to a usable format

or Infrastructure as a Service (IaaS), deploy applications in runti
a way that is abstracted from the machine image.

or Platform as a Service (PaaS), careful application developmen
echniques and thoughtful architecture should be followed to
inimize potential lock-in for the customer. “loose coupling”

nderstand who the competitors are to your cloud providers and
hat their capabilities are to assist in migration.

dvocate open standards.

raditional, BCM/DR

Cloud providers should adopt as a security baseline the
host stringent requirements of any customer.

Compartmentalization of job duties and limit knowledge o
ustomers.

Onsite inspections of cloud provider facilities whenever
ossible.

nspect cloud provider disaster recovery and business
ontinuity plans.

dentify physical interdependencies in provider infrastructu

ata Center Operations

ompartmentalization of systems, networks, management, rovisioning and personnel.

now cloud provider's other clients to assess their impact on you

nderstand how resource sharing occurs within your cloud provid
o understand impact during your business fluctuations.

or IaaS and PaaS, the cloud provider's patch management polic
nd procedures have significant impact

loud provider's technology architecture may use new and unpro
ethods for failover. Customer's own BCP plans should address
mpacts and limitations of Cloud computing.

est cloud provider's customer service function regularly to
etermine their level of mastery in supporting the services.

ncident Response

Any data classified as private for the purpose of data brea
egulations should always be encrypted to reduce the
onsequences of a breach incident.

Cloud providers need application layer logging framework
o provide granular narrowing of incidents to a specific
ustomer.

Cloud providers should construct a registry of application
wners by application interface (URL, SOA service, etc.).

Cloud providers and customers need defined collaboratio
or incident response.

pplication Security

aaS, PaaS and SaaS create differing trust boundaries for
he software development lifecycle, which must be
ccounted for during the development, testing and
roduction deployment of applications.

or IaaS, need trusted virtual machine images.

pply best practices available to harden DMZ host systen
o virtual machines.

ecuring inter-host communications must be the rule, the
an be no assumption of a secure channel between hosts

anaging and protecting application “secret keys” is critic

nderstand how malicious actors are likely to adapt their
ttack techniques to cloud platforms

nerypti0n & Key Mgt

rom a risk management perspective, unencrypted data xistent in the cloud may be considered “lost” by the ustomer.

pplication providers who are not controlling backend ystems should assure that data is encrypted when being tored on the backend.

se encryption to separate data holding from data usage.

egregate the key management from the cloud provider osting the data, creating a chain of separation.

hen stipulating standard encryption in contract language

dentity & Access Mgt

ust have a robust federated identity management architecture and strategy
ternal to the organization.

sist upon standards enabling federation: primarily SAML, WS-Federation a
berty ID-FF federation

alidate that cloud provider either support strong authentication natively or v
elegation and support robust password policies that meet and exceed interr
olicies.

nderstand that the current state of granular application authorization on the
f cloud providers is non-existent or proprietary.

onsider implementing Single Sign-on (SSO) for internal applications, and
veraging this architecture for cloud applications.

sing cloud-based “Identity as a Service” providers may be a useful tool for
bstracting and managing complexities such as differing versions of SAML, e

torage

nderstand the storage architecture and abstraction layers to veri
hat the storage subsystem does not span domain trust boundarie

scertain if knowing storage geographical location is possible.

nderstand the cloud provider's data search capabilities.

nderstand cloud provider storage retirement processes.

nderstand circumstances under which storage can be seized by
hird party or government entity.

nderstand how encryption is managed on multi-tenant storage.

an the cloud provider support long term archiving, will the data b
vailable several years later?

irtualization

irtualized operating systems should be augmented by third party
ecurity technology.

he simplicity of invoking new machine instances from a VM platf
reates a risk that insecure machine images can be created. Sec
y default configuration needs to be assured by following or
xceeding available industry baselines.

irtualization also contains many security advantages which can
inimize application instability and simplify recovery.

eed granular monitoring of traffic crossing VM backplanes

dministrative access and control of virtualized operating systems
rucial

ummary

- Cloud Computing is real and transformational
- Cloud Computing can and will be secured
- Broad governance approach needed
- Tactical fixes needed
- Combination of updating existing best practices and creating completely new best practices
- Common sense not optional

an to Action

oin us, help make our work better

Discussions & announcements on LinkedIn

Hold regional CSA Meetups

CSA organizing meetings for Version 2.0 of Guidan
n early June

Other research initiatives and events being planned

ontact

w.cloudsecurityalliance.org

o@cloudsecurityalliance.org

ups.google.com/cloudsecurityalliance

itter: @cloudsa, #csaguide

kedIn: www.linkedin.com/groups?gid=1864210

ristofer Hoff, choff@packetfilter.com | @beake
ationalsurvivability.com/blog

Thank You!