cloud security alliance℠

Achieving Security Assurance and Compliance in the Cloud

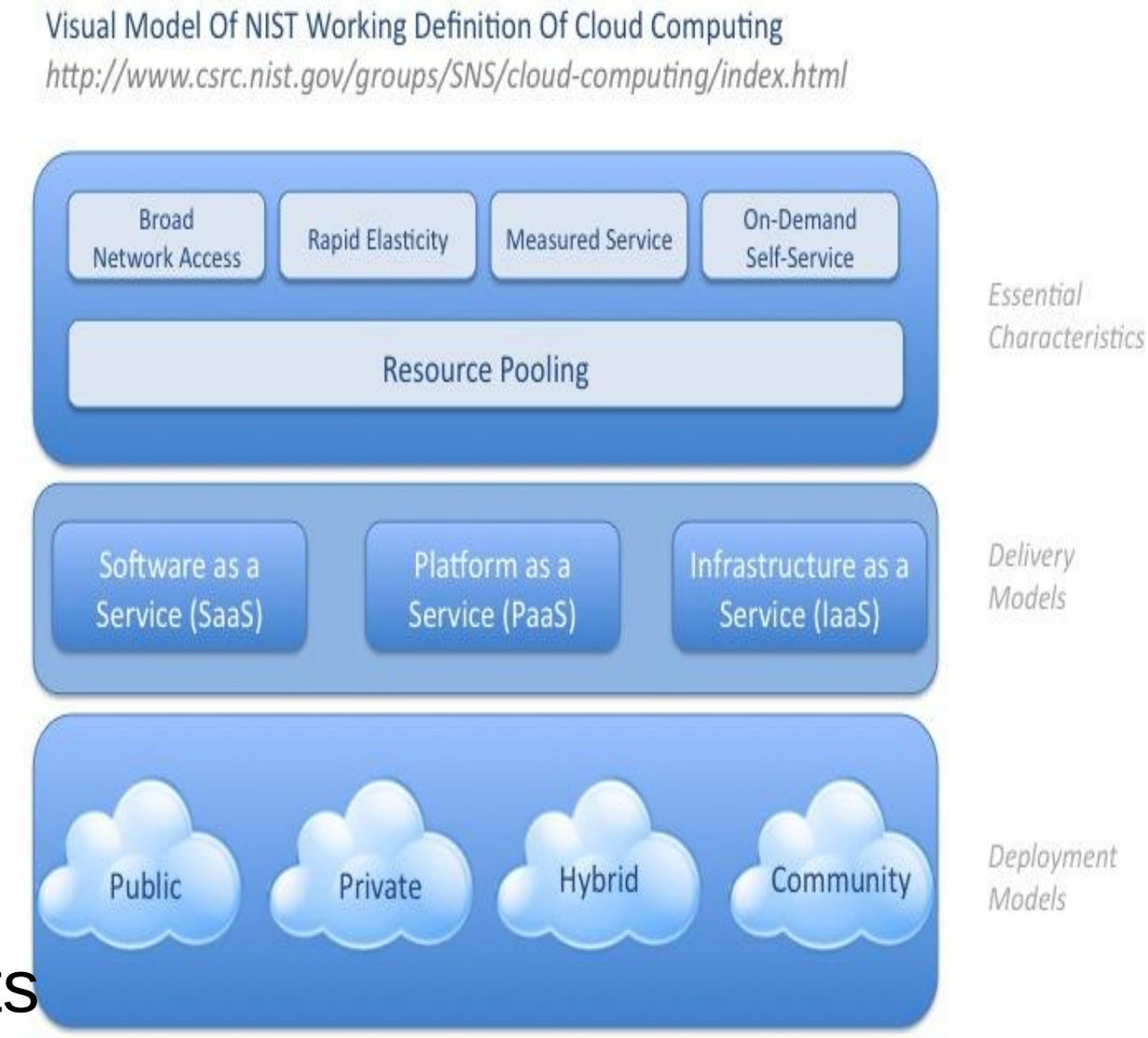
Jason Witty
Executive Committee, CSA
International Info Security Exec, Bank of America

Cloud: Dawn of a New Age

- Cloud – overhyped in the short run, underestimated in the long term
- Changes everything: business models, venture capital, R&D, ……
- Driving a new macroeconomic reality

What is Cloud Computing?

- Compute as a utility: third major era of computing
- Cloud enabled by
  - Moore's Law
  - Hyperconnectivity
  - SOA
  - Provider scale
- Key characteristics
  - Elastic & on-demand
  - Multi-tenancy
  - Metered service
- IaaS may track energy costs



What is Different in the Cloud?

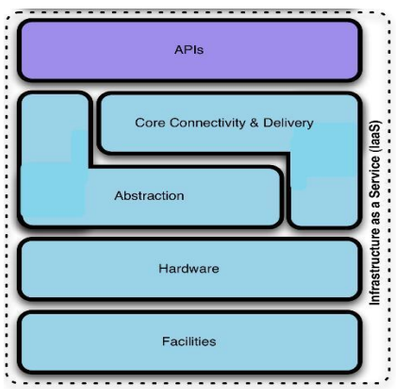
Role Clarity

Security ~ THEM

Security ~ YOU

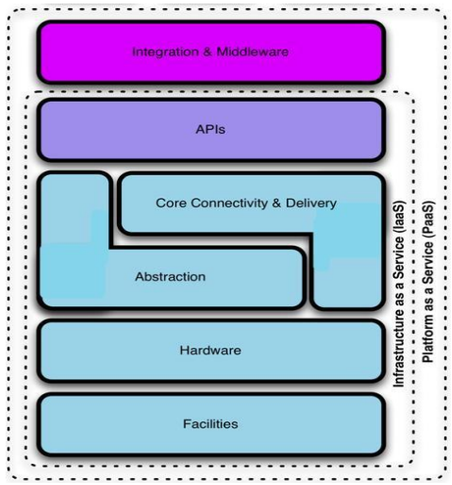
IaaS

Infrastructure as a Service



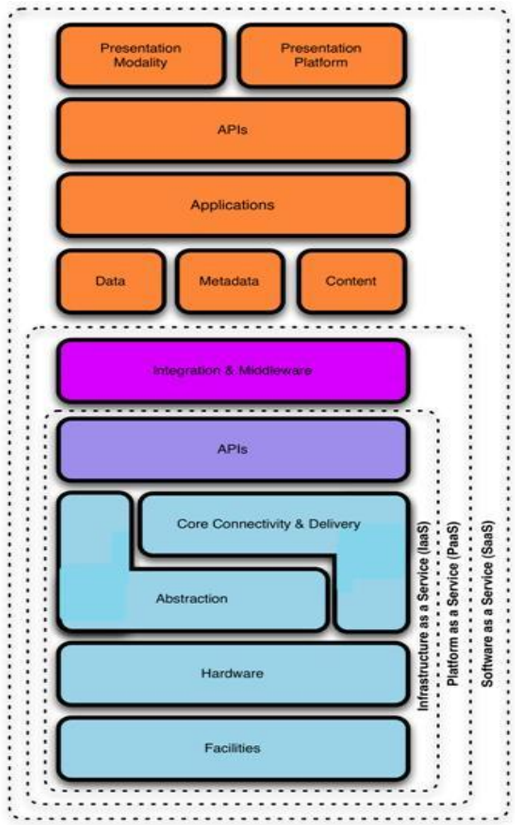
PaaS

Platform as a Service



SaaS

Software as a Service

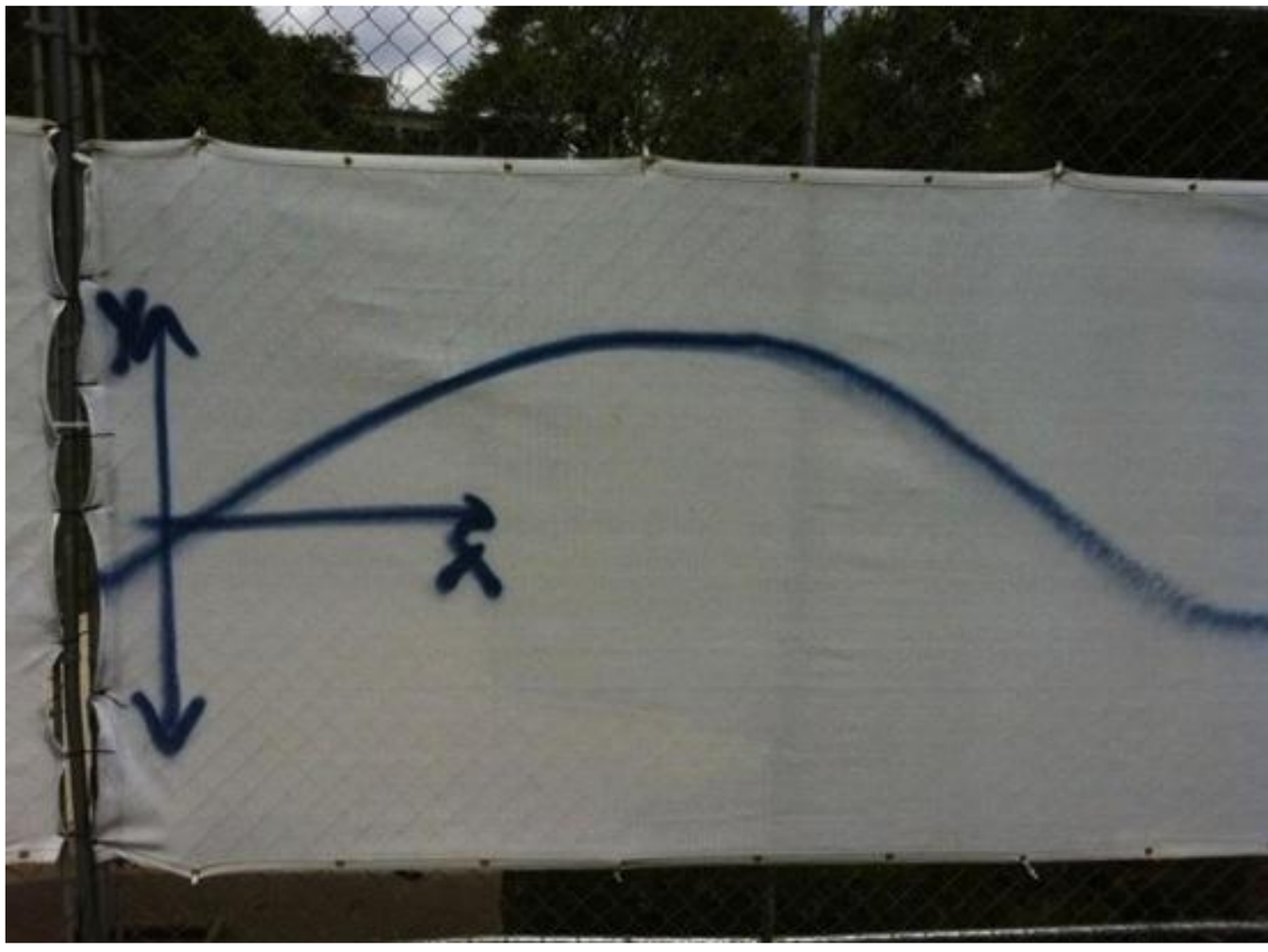


cloud security alliance℠

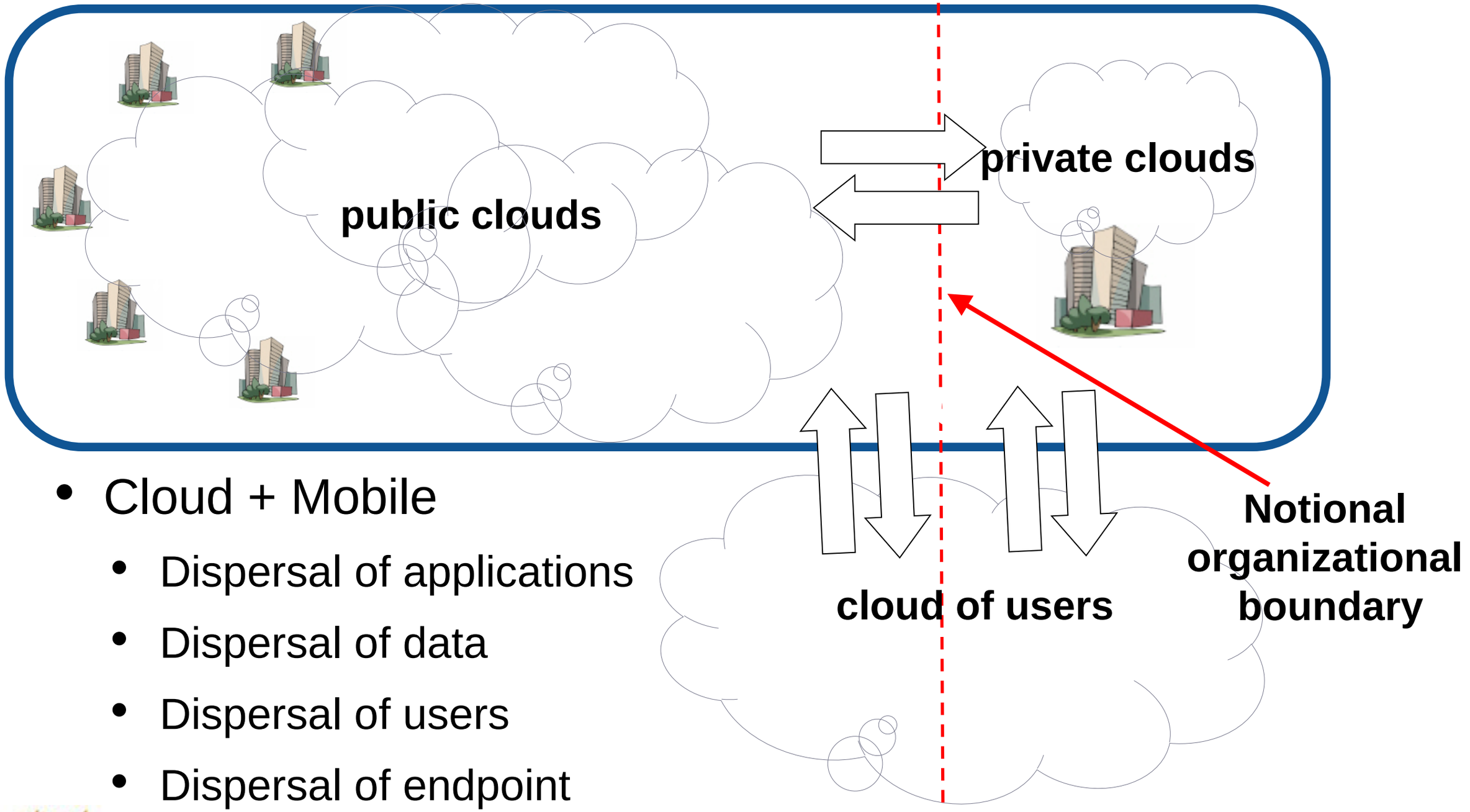
www.cloudsecurityalliance.org

Math favors the (public) Cloud

- Commoditization of compute and storage
  - IaaS to track energy costs
- Efficiency ratios
  - Cloud admin Nx better than IT admin
- Agility
  - Cost of time
- Ask a software co CEO
  - Can’t afford the shrinkwrap business model



2011-2014: the Hybrid Enterprise



- Cloud + Mobile
  - Dispersal of applications
  - Dispersal of data
  - Dispersal of users
  - Dispersal of endpoint devices

Cloud Forcing Key Issues

- Critical mass of separation between data owners and data processors
- Anonymity of geography of data centers & devices
- Anonymity of provider
- Transient provider relationships
- Physical controls must be replaced by virtual controls
- Identity management has a key role to play
- Cloud WILL drive change in the security status quo
- Reset button for security ecosystem

What are the Trust issues?

- Will my cloud provider be transparent about governance and operational issues?
- Will I be considered compliant?
- Do I know where my data is?
- Will a lack of standards drive unexpected obsolescence?
- Is my provider really better at security than me?
- Are the hackers waiting for me in the cloud?
- Will I get fired?

Key Problems of Tomorrow

- Keeping pace with cloud changes
- Globally incompatible legislation and policy
- Non-standard Private & Public clouds
- Lack of continuous Risk Mgt & Compliance monitoring
- Incomplete Identity Mgt implementations
- Haphazard response to security incidents

About the Cloud Security Alliance

- Global, not-for-profit organization
- Over 19,000 individual members, 100 corporate members
- Building best practices and a trusted cloud ecosystem
- Agile philosophy, rapid development of applied research
- GRC: Balance compliance with risk management
- Reference models: build using existing standards
- Identity: a key foundation of a functioning cloud economy
- Champion interoperability
- Advocacy of prudent public policy

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

www.cloudsecurityalliance.org

How do we build the “Trusted Cloud”?

Here's How…

- Strategy
- Education
- Security Framework
- Assessment
- Build for the Future

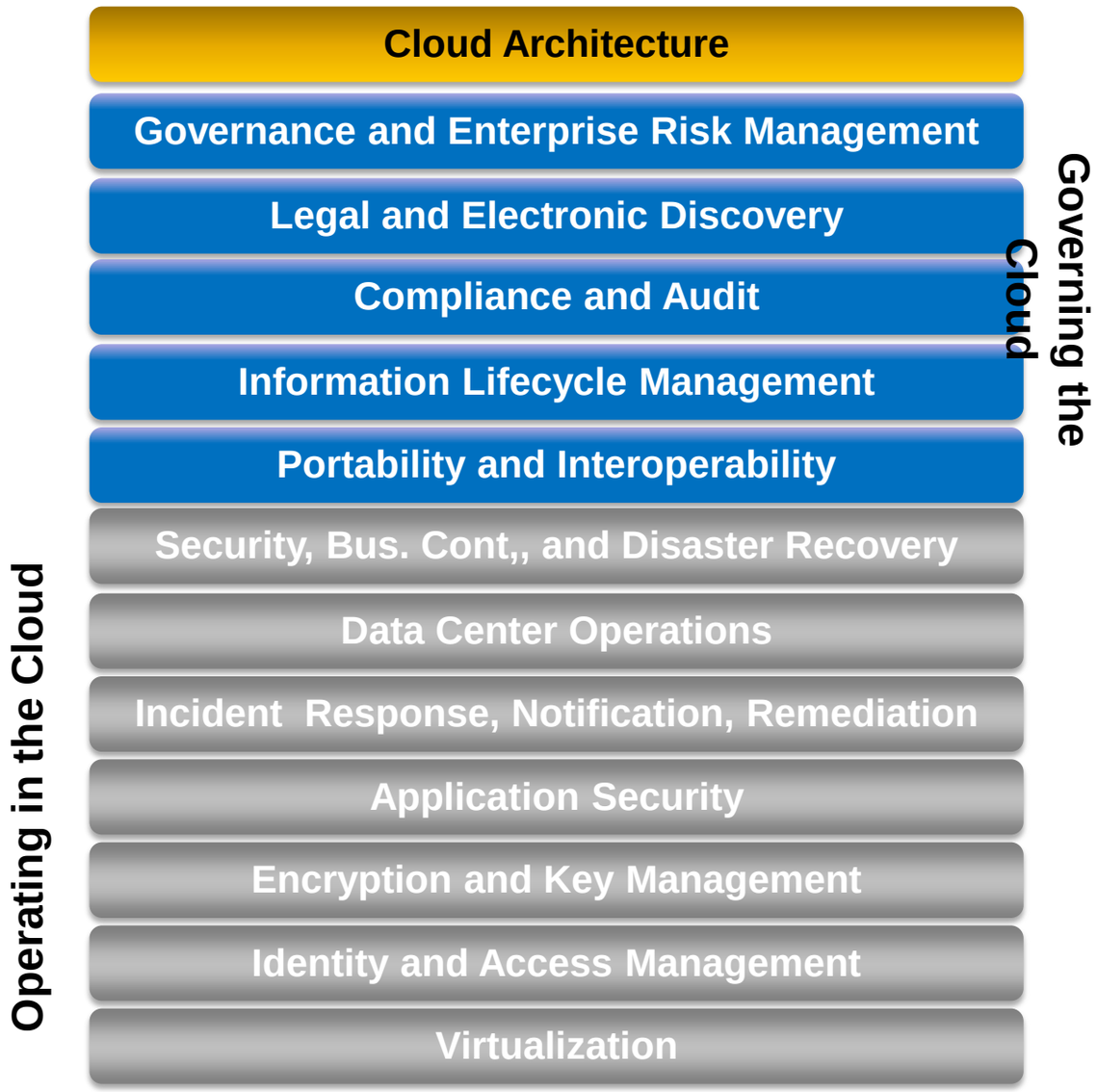
Strategy

- IT Architecture supporting Hybrid enterprise
  - Federated IdM
  - Service Oriented Architecture “loose coupling” principles
- Consider cloud as an option to any new IT initiative
  - What are the cost differences?
  - What are the feature/functionality differences?
  - Does the application support different cloud deployments and multiple providers?
- Risk Management
  - Sensitivity of application and data, new risks introduced by cloud, risk tolerance levels

Education

CSA Guidance Research

- Popular best practices for securing cloud computing
- V2.1 released 12/2009
- V3 target Q3 2011
- wiki.cloudsecurityalliance .org/guidance



Guidance > 100k downloads: cloudsecurityalliance.org/guidance

Guidance Highlights – 1/2

- Governance, ERM: Secure the cloud before procurement – contracts, SLAs, architecture
- Governance, ERM: Know provider's third parties, BCM/DR, financial viability, employee vetting
- Legal: Plan for provider termination & return of assets
- Compliance: Identify data location when possible
- ILM: Persistence, Protection
- Portability & Interoperability: SOA "loose coupling" principles

Guidance Highlights – 2/2

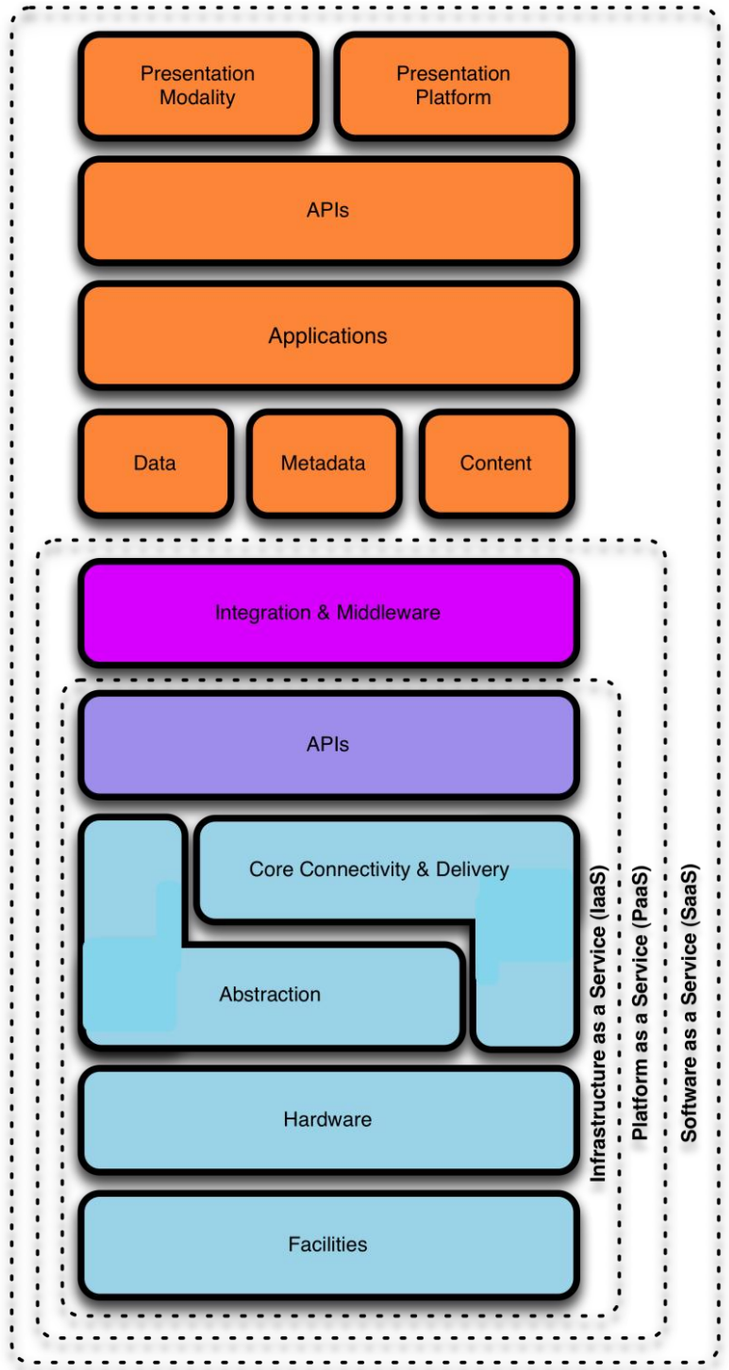
- BCM/DR: provider redundancy vs your own
- DC Ops: provisioning, patching, logging
- Encryption: encrypt data when possible, segregate key mgt from cloud provider
- AppSec: Adapt secure software development lifecycle
- Virtualization: Harden, rollback, port VM images
- IdM: Federation & standards e.g. SAML, OpenID

CCSK – Certificate of Cloud Security Knowledge

- Benchmark of cloud security competency
- Measures mastery of CSA guidance and ENISA cloud risks whitepaper
- Understand cloud issues

- Look for the CCSKs at cloud providers, consulting partners
- Online web-based examination
- www.cloudsecurityalliance.org/certifyme

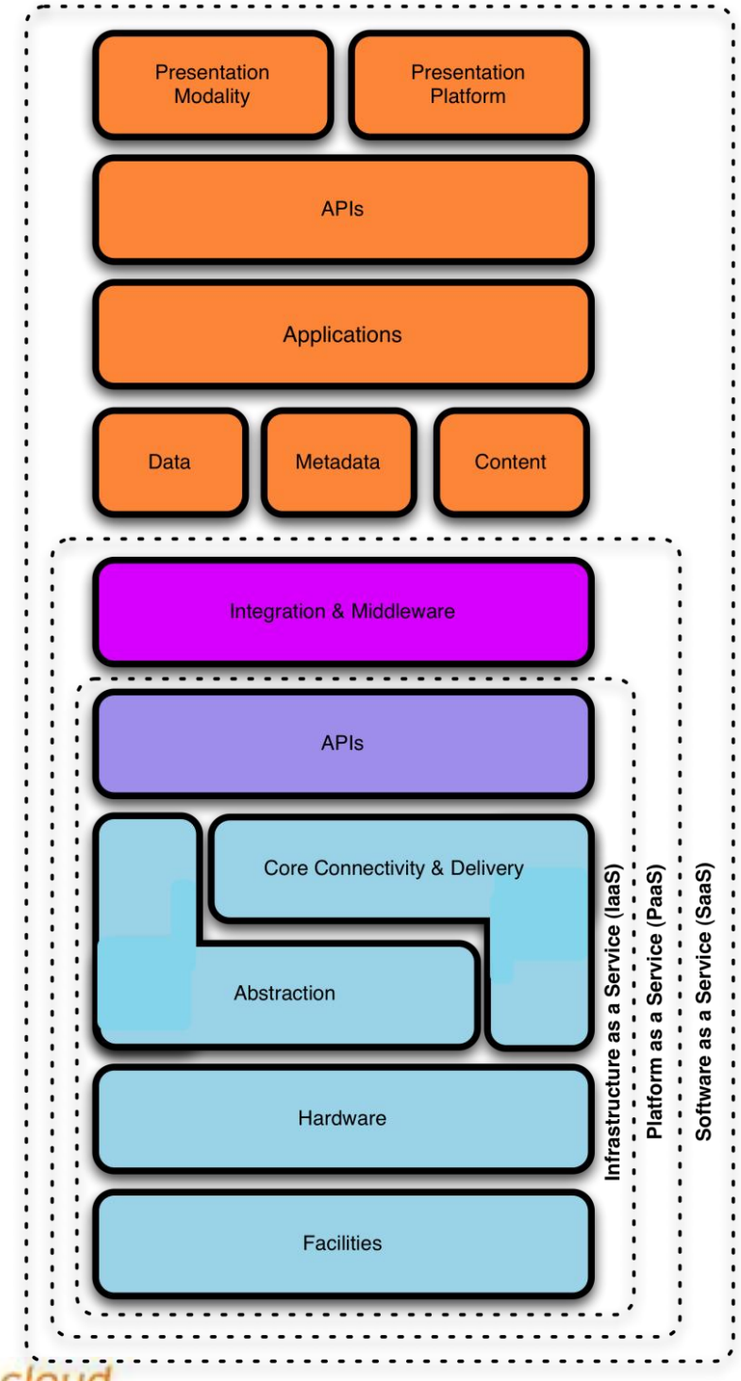
Security Framework



cloud security alliance℠

www.cloudsecurityalliance.org

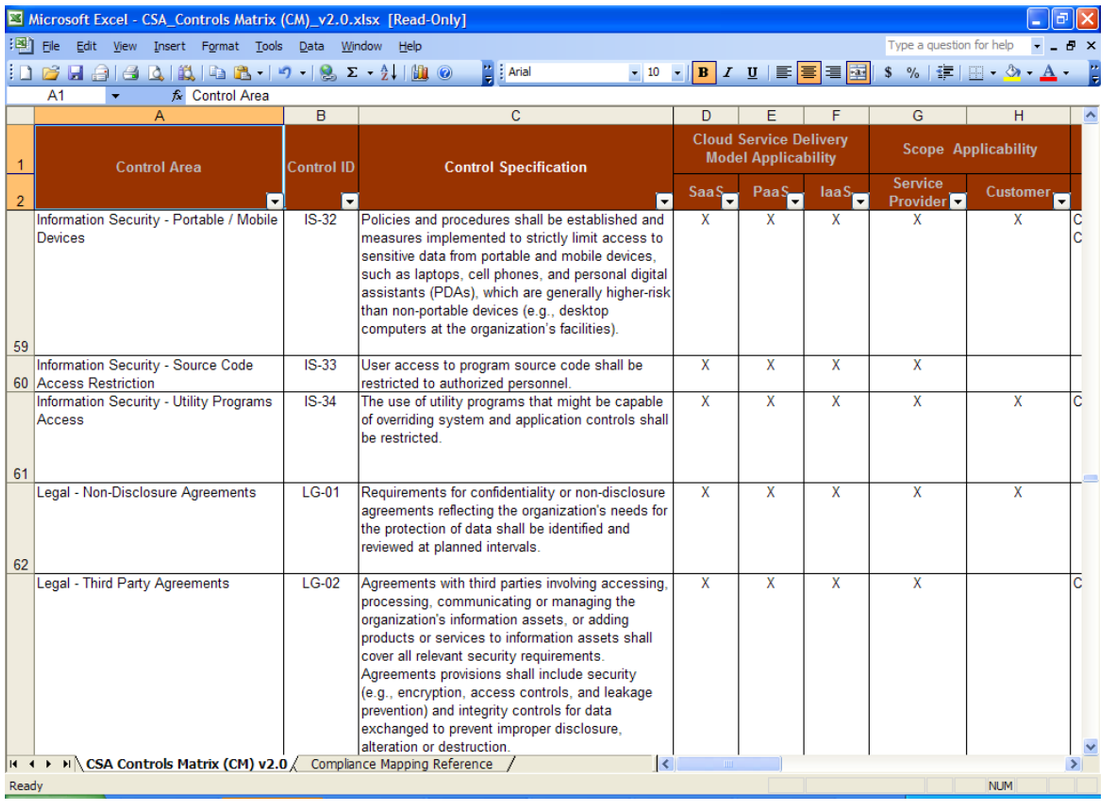
CSA Reference Model



- CSA Cloud Reference Model
  - IaaS (Compute & storage) is the foundation
  - PaaS (Rapid application dev) adds middleware to IaaS
  - SaaS represents complete applications on top of PaaS

Cloud Controls Matrix

- Controls derived from guidance
- Mapped to familiar frameworks: ISO 27001, COBIT, PCI, HIPAA
- Rated as applicable to S-P-I
- Customer vs Provider role
- Help bridge the “cloud gap” for IT & IT auditors


Microsoft Excel - CSA_Controls Matrix (CM)_v2.0.xlsx [Read-Only]

	Control Area	Control ID	Control Specification	Cloud Service Delivery Model Applicability			Scope Applicability		
				SaaS	PaaS	IaaS	Service Provider	Customer	
59	Information Security - Portable / Mobile Devices	IS-32	Policies and procedures shall be established and measures implemented to strictly limit access to sensitive data from portable and mobile devices, such as laptops, cell phones, and personal digital assistants (PDAs), which are generally higher-risk than non-portable devices (e.g., desktop computers at the organization's facilities).	X	X	X	X	X	C C
60	Information Security - Source Code Access Restriction	IS-33	User access to program source code shall be restricted to authorized personnel.	X	X	X	X		
61	Information Security - Utility Programs Access	IS-34	The use of utility programs that might be capable of overriding system and application controls shall be restricted.	X	X	X	X	X	C
62	Legal - Non-Disclosure Agreements	LG-01	Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of data shall be identified and reviewed at planned intervals.	X	X	X	X	X	
	Legal - Third Party Agreements	LG-02	Agreements with third parties involving accessing, processing, communicating or managing the organization's information assets, or adding products or services to information assets shall cover all relevant security requirements. Agreements provisions shall include security (e.g., encryption, access controls, and leakage prevention) and integrity controls for data exchanged to prevent improper disclosure, alteration or destruction.	X	X	X	X		C

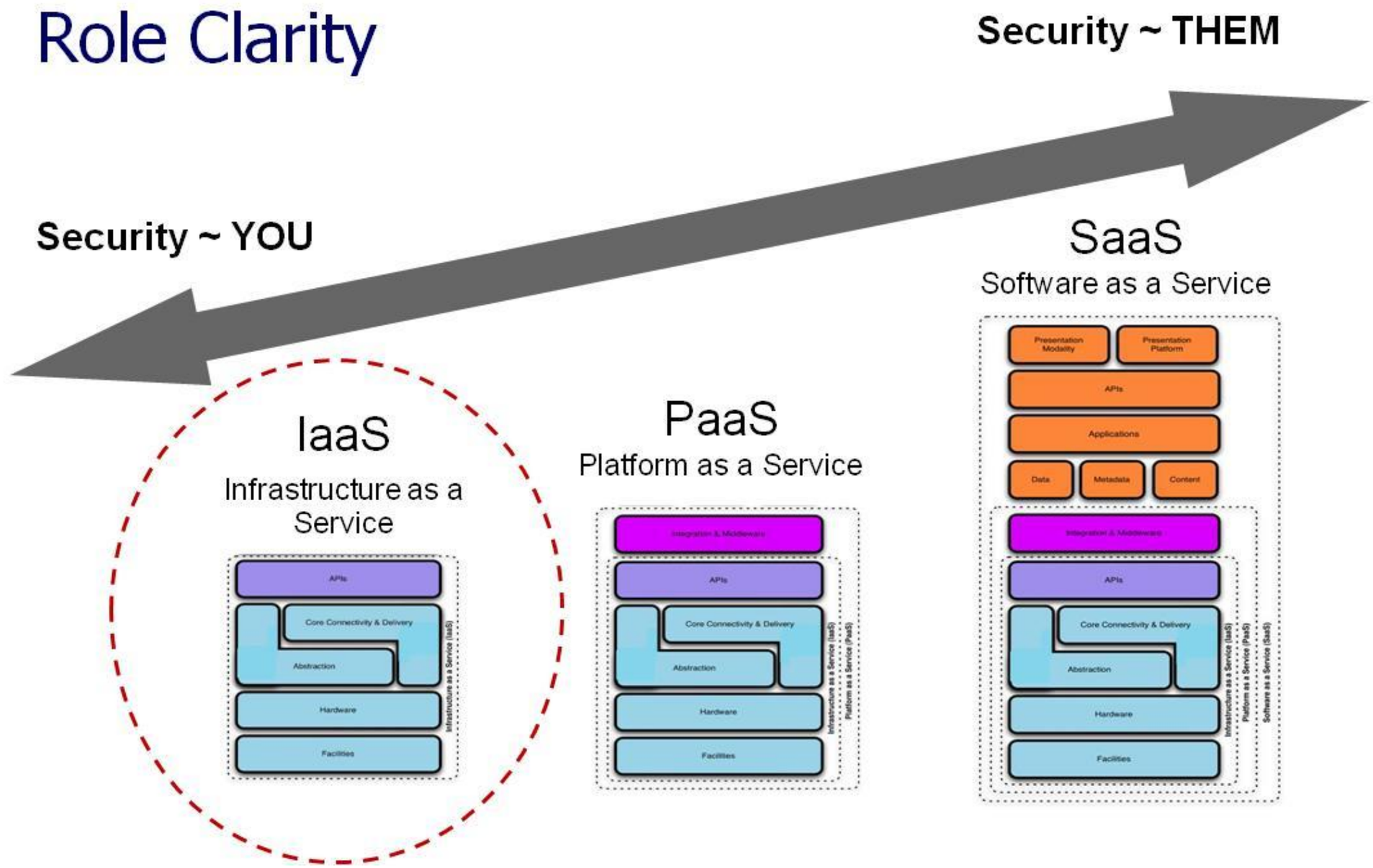
CSA Controls Matrix (CM) v2.0 | Compliance Mapping Reference

Ready NUM

- www.cloudsecurityalliance.org/cm.html

Assessment

Assessment responsibility



Consensus Assessment Initiative

- Research tools and processes to perform shared assessments of cloud providers
- Integrated with Controls Matrix
- Ver 1 CAI Questionnaire released Oct 2010, approx 140 provider questions to identify presence of security controls or practices
- Use to assess cloud providers today, procurement negotiation, contract inclusion, quantify SLAs
- www.cloudsecurityalliance.org/cai.html

Build for the future

www.cloudsecurityalliance.org

CloudAudit

- Open standard and API to automate provider audit assertions
- Change audit from data gathering to data analysis
- Necessary to provide audit & assurance at the scale demanded by cloud providers
- Uses Cloud Controls Matrix as controls namespace
- Use to instrument cloud for continuous controls monitoring

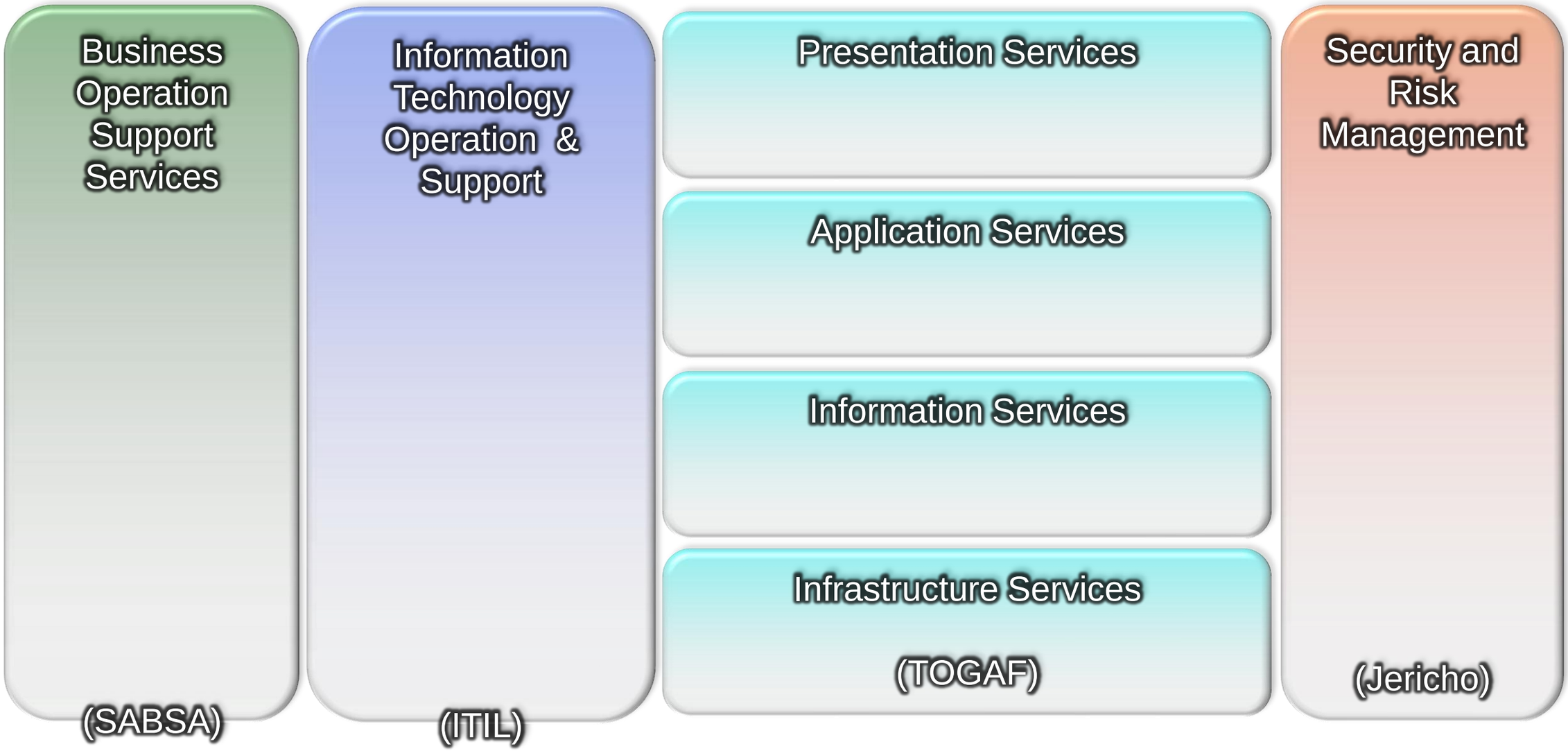
CloudSIRT

- Consensus research for emergency response in Cloud
- Enhance community's ability to respond to incidents
- Standardized processes
- Supplemental best practices for SIRTs
- Hosted Community of Cloud SIRTs
- www.cloudsecurityalliance.org/cloudsirt.html

Trusted Cloud Initiative

- Comprehensive Cloud Security Reference Architecture
- Secure & interoperable Identity in the cloud
- Getting SaaS, PaaS to be “Relying Parties” for corporate directories
- Scalable federation
- Outline responsibilities for Identity Providers
- Assemble reference architectures with existing standards
- www.cloudsecurityalliance.org/trustedcloud.html

Reference model structure



Trusted Cloud Initiative

www.cloudsecurityalliance.org

Security as a Service

- Information Security Industry Re-invented
- Define Security as a Service
- Articulate solution categories within Security as a Service
- Guidance for adoption of Security as a Service
- Align with other CSA research
- Develop deliverables as a proposed 14th domain within CSA Guidance version 3.
- www.cloudsecurityalliance.org/secaas.html

What might Cloud 2.0 look like?

- Less centralized than you think: cloud brokering, SOA, REST, evade energy costs, grid
- Regulated – if we don't do it ourselves
- Disruptive technologies, e.g. format preserving encryption, new secure hypervisors, Identity Mgt everywhere
- New cloud business app models
- Greater policy harmonization (maritime law?)
- 4 of 10 biggest IT companies of 2020 do not exist

Going to the Cloud securely

- Challenges remain
- More tools available than you think
- Waiting not an option
- Many types of clouds
- Identify IT options appropriate for specific cloud
- Leverage business drivers & risk mgt
- Be Agile!

Contact

- Help us secure cloud computing
- www.cloudsecurityalliance.org
- info@cloudsecurityalliance.org
- LinkedIn: www.linkedin.com/groups?gid=1864210
- Twitter: @cloudsa

Thank you!

cloud security alliance

www.cloudsecurityalliance.org