THE SECURITY STANDARD™

Securing the Enterprise from a Dangerous Cyberworld

September 19-20, 2011 • Marriott Brooklyn Bridge, New York City

Produced by
CSO

Assessing Risks in the Cloud

Jason Witty

SVP, International Information Security
Executive, Global Information Security

Bank of America Corporation

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

cloud security alliance℠

The revolution has tinder

- Social networking, blogging and microblogging
  - Egalitarianism of media and communications
- Mobile computing
  - Empowering the citizens
- Cloud computing
  - Egalitarianism of IT

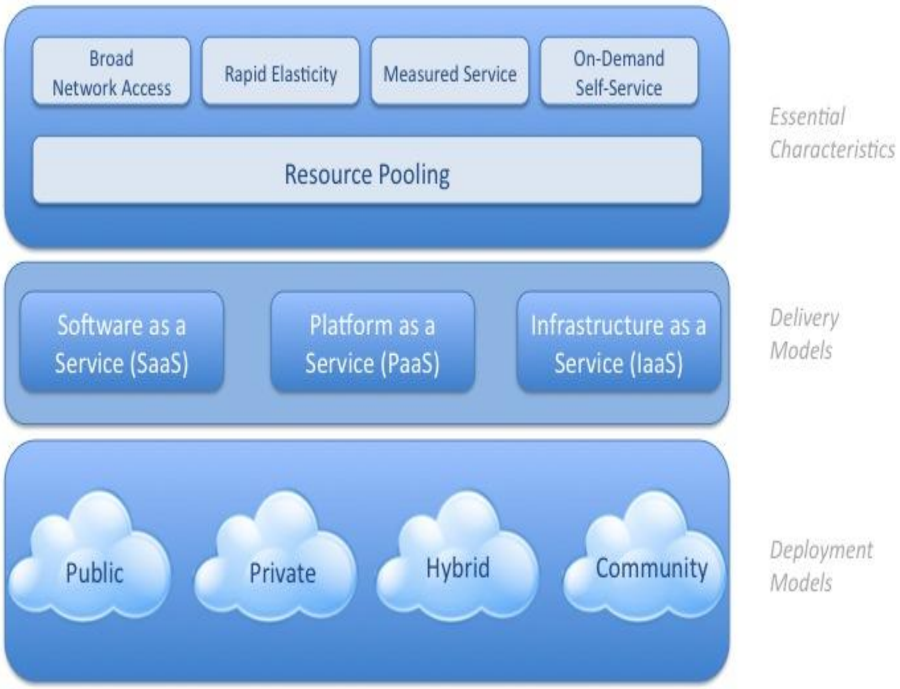
- What can’t this change?
- Timing is everything

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
  - Broad Network Access
  - Rapid Elasticity
  - Metered service
  - On-demand self-service
  - Multi-tenancy/resource pooling

Visual Model Of NIST Working Definition Of Cloud Computing

http://www.csrc.nist.gov/groups/SNS/cloud-computing/index.html



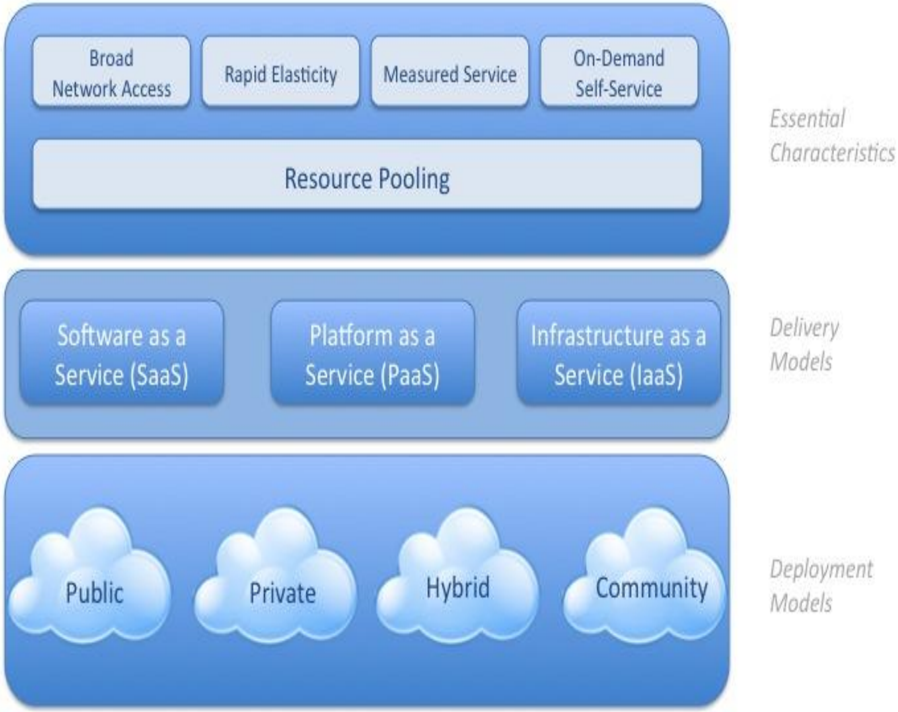
What is Cloud Computing?

Delivery Models

- Software as a Service
- Platform as a Service
- Infrastructure as a Service

Visual Model Of NIST Working Definition Of Cloud Computing

http://www.csrc.nist.gov/groups/SNS/cloud-computing/index.html



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)

Delivery Models

Public

Private

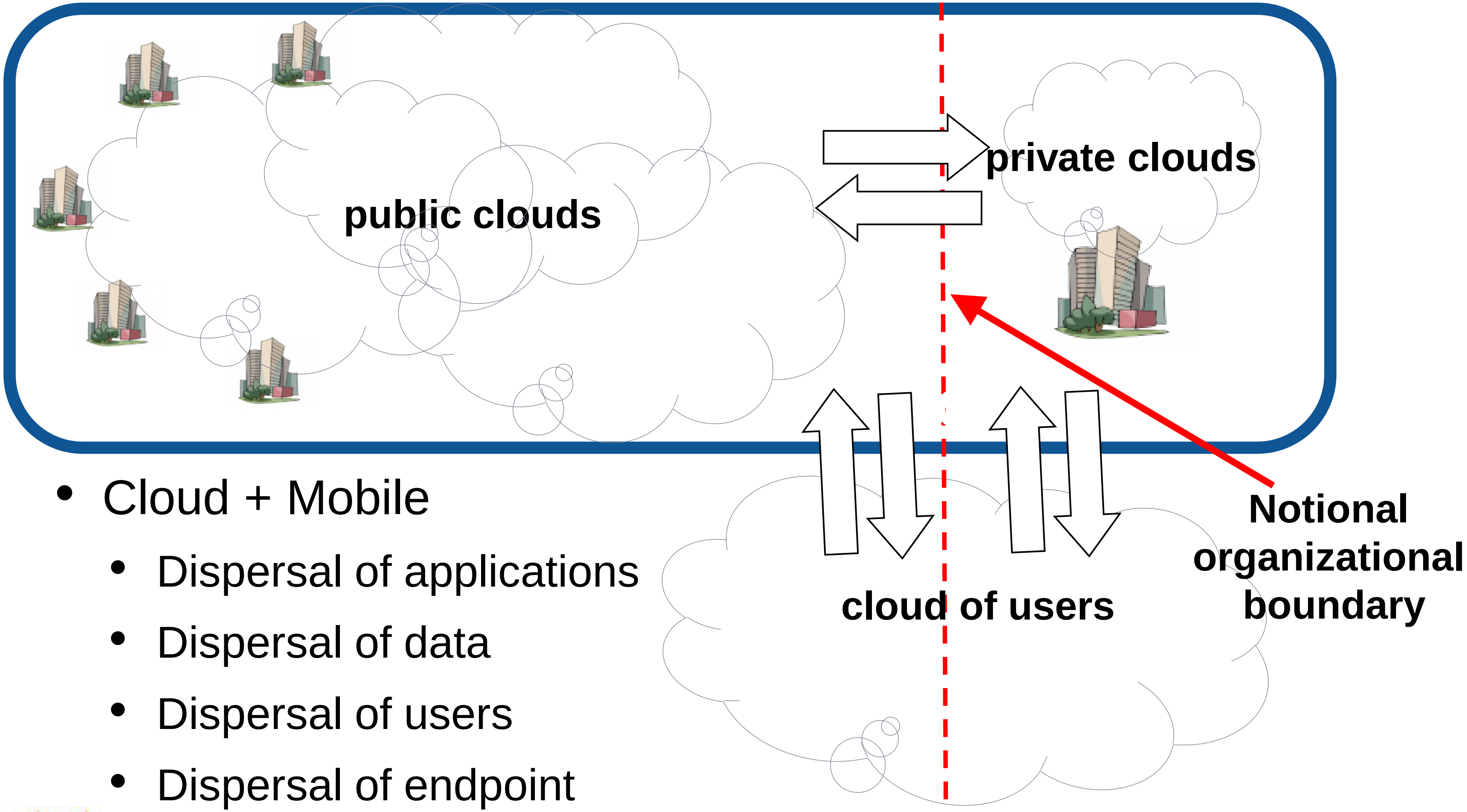
Hybrid

Community

Deployment Models

2011-2014: the Hybrid Enterprise

Deployment Models



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

What is Different in the Cloud?

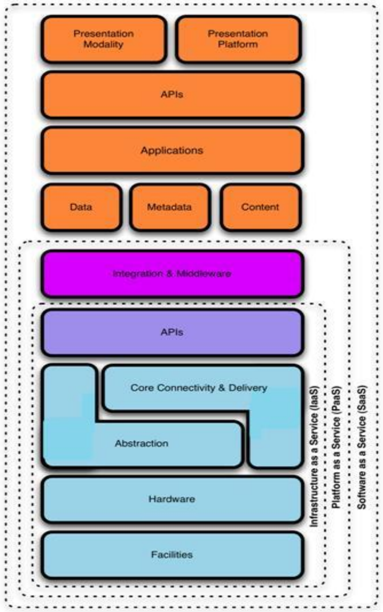
Role Clarity

Security ~ THEM

Security ~ YOU

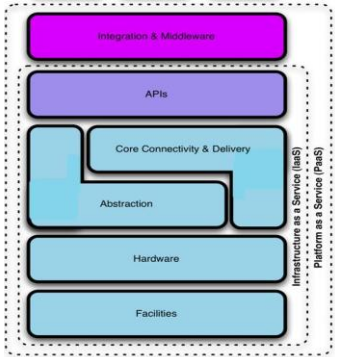
SaaS

Software as a Service



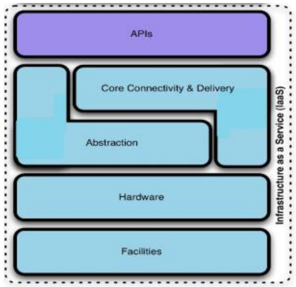
PaaS

Platform as a Service


Integration & Middleware
APIs
Core Connectivity & Delivery
Abstraction
Hardware
Facilities
Infrastructure as a Service (IaaS)
Platform as a Service (PaaS)

IaaS

Infrastructure as a Service


APIs
Core Connectivity & Delivery
Abstraction
Hardware
Facilities
Infrastructure as a Service (IaaS)

www.cloudsecurityalliance.org

Cloud Forcing Key Issues Today

- 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 Management & Compliance monitoring
- Incomplete Identity Management implementations
- Haphazard response to security incidents

About the Cloud Security Alliance

- Global, not-for-profit organization
- Over 23,000 individual members, 100 corporate members, 50 chapters
- 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
  - Enable innovation
  - 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."

How do we build the "Trusted Cloud"?

Here's How…

Cloud SIRT

CCSK™
Certificate of
Cloud Security Knowledge

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

CCM™
Cloud Controls Matrix

CAI™
Consensus Assessments
Initiative

Cloud
Audit

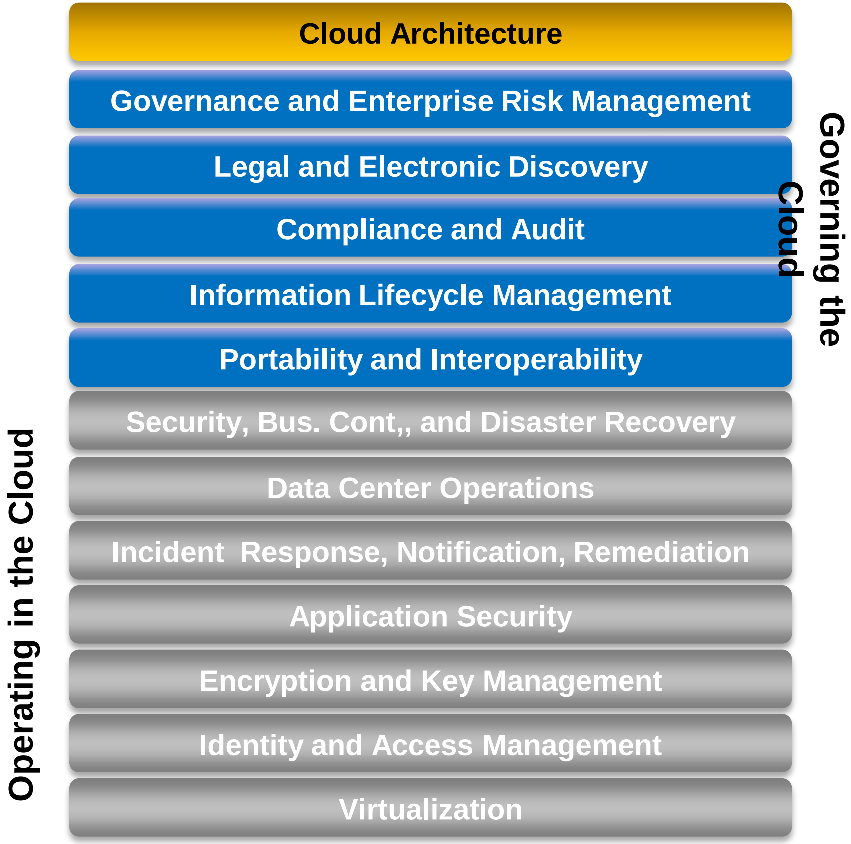
Strategy

- 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



Cloud Architecture

Governance and Enterprise Risk Management

Legal and Electronic Discovery

Compliance and Audit

Information Lifecycle Management

Portability and Interoperability

Security, Bus. Cont,, and Disaster Recovery

Data Center Operations

Incident Response, Notification, Remediation

Application Security

Encryption and Key Management

Identity and Access Management

Virtualization

Governing the Cloud

Operating in the Cloud

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 management 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

Training Courses

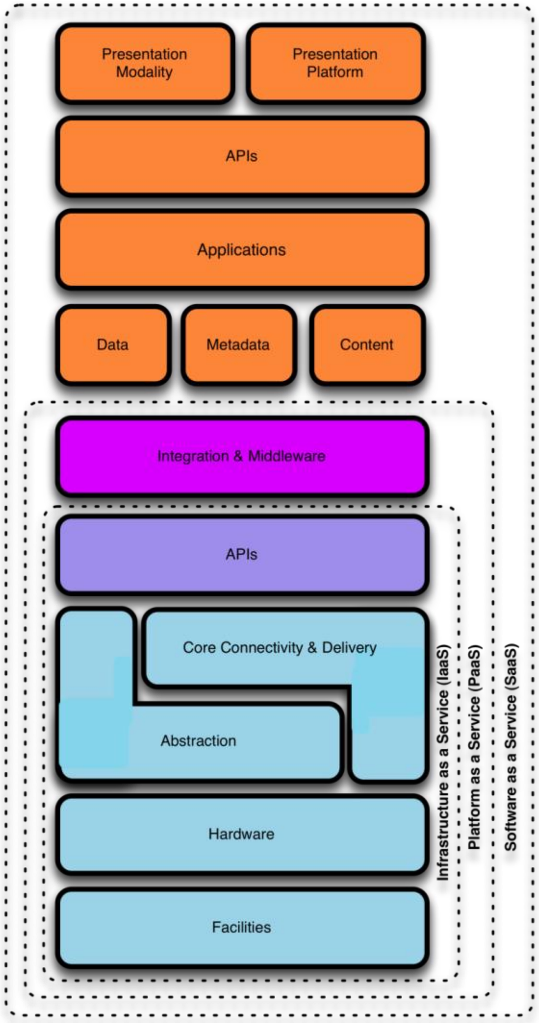
- CCSK Basic
  - One day course to enable student to pass CCSK
- CCSK Plus
  - Two day course includes practical cloud lab work
- GRC Stack Training
  - One day course to use GRC Stack components
- PCI/DSS In the Cloud
  - Achieving PCI compliance in cloud computing

https://cloudsecurityalliance.org/education/training/

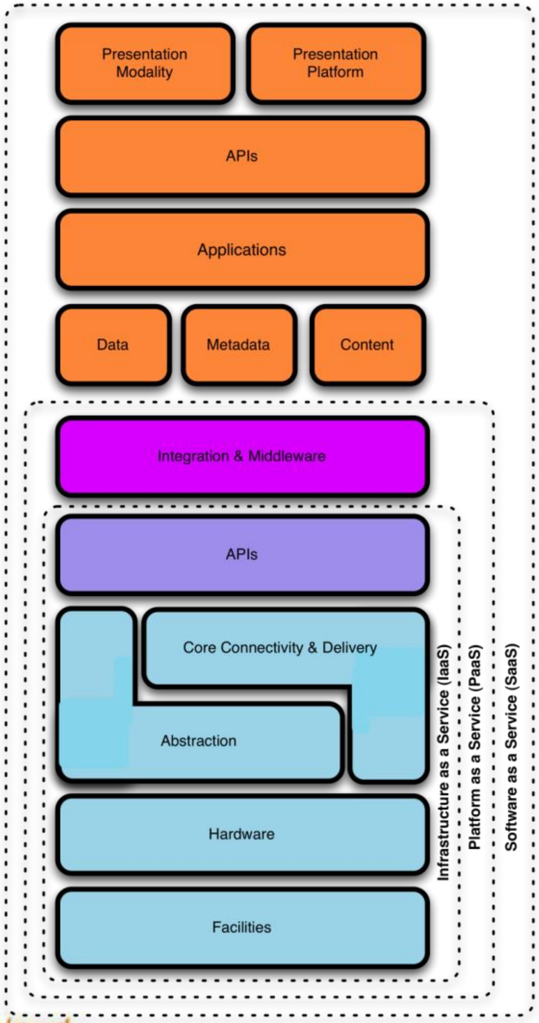
Upcoming Conferences

- CSA Summit Korea, Sept 29, Seoul
- CSA Summit Europe, Oct 10, London (with RSA Europe)
- CSA Congress, Nov 16-17, Orlando
- CSA Summit RSA, Feb 27 2012, San Francisco
- SecureCloud 2012 (partnership with ENISA)

Security Framework



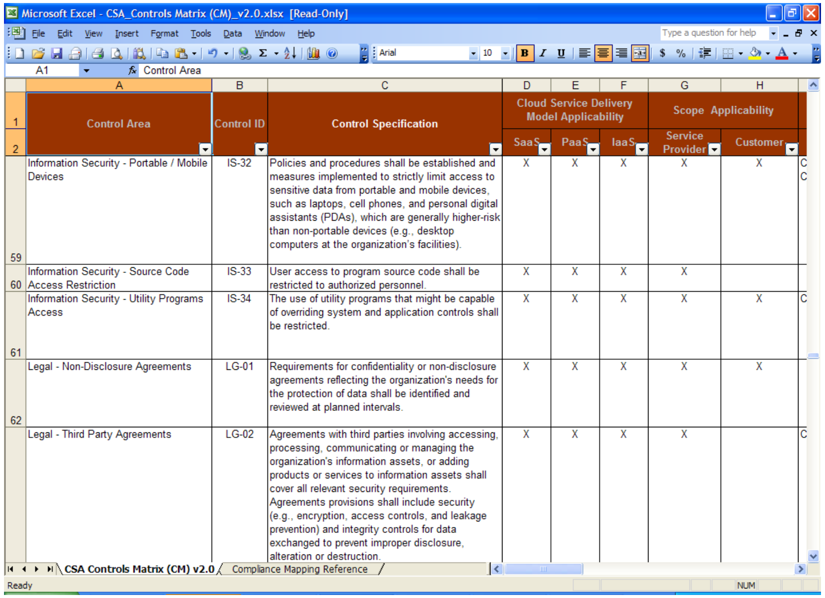
CSA Reference Model



- 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]

A1 Control Area

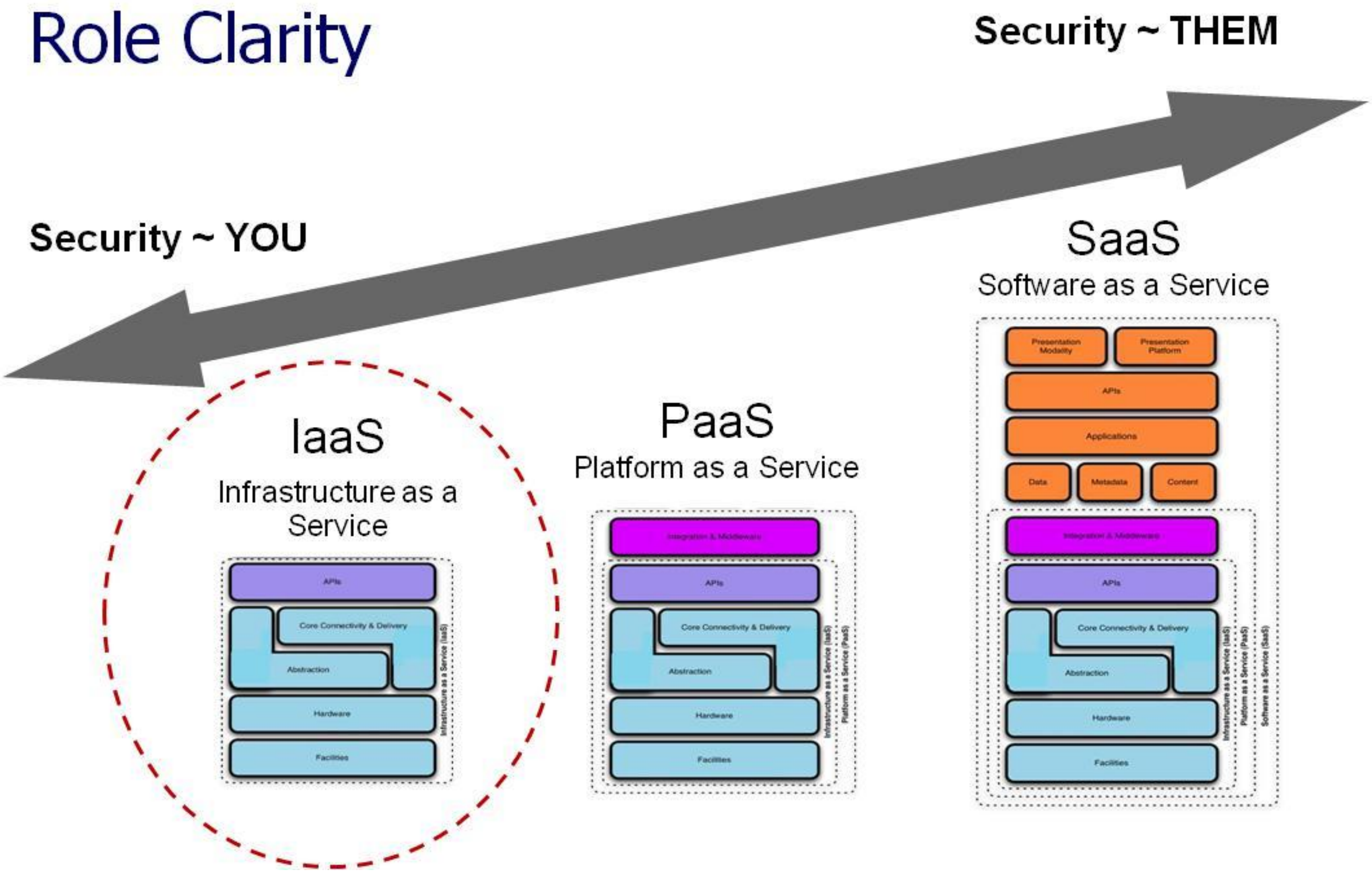
	A	B	C	D	E	F	G	H	
1	Control Area	Control ID	Control Specification	Cloud Service Delivery Model Applicability			Scope Applicability		
2				SaaS	PaaS	IaaS	Service Provider	Customer	
59	Information Security - Portable / Mobile Devices	IS-32	Policies and procedures shall be established and measures implemented 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

- 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

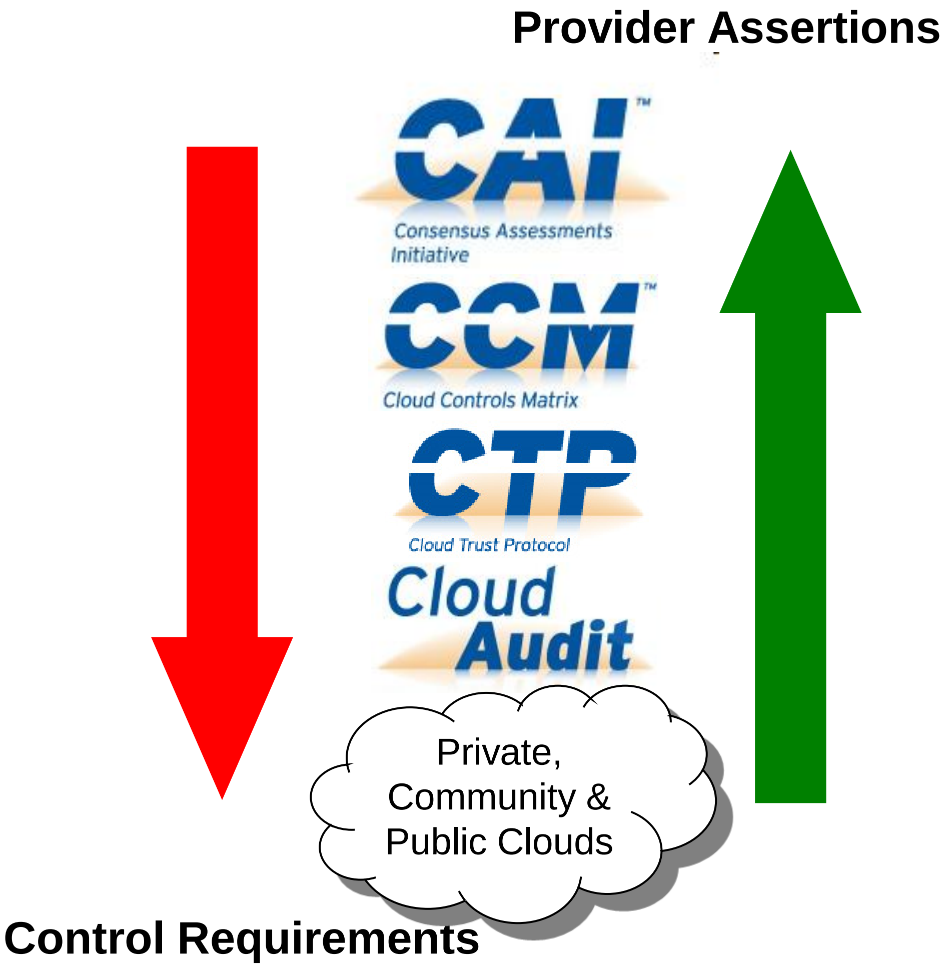
CSA STAR Registry

- CSA STAR (Security, Trust and Assurance Registry)
- Public Registry of Cloud Provider self assessments
- Based on Consensus Assessments Initiative Questionnaire
  - Provider may substitute documented Cloud Controls Matrix compliance
- Voluntary industry action promoting transparency
- Free market competition to provide quality assessments
  - Provider may elect to provide assessments from third parties
- Available October 2011

Build for the future

CSA GRC Stack

- Family of 4 research projects
  - Cloud Controls Matrix
  - Consensus Assessments Initiative
  - Cloud Audit
  - Cloud Trust Protocol
- Tools for governance, risk and compliance mgt
- Enabling automation and continuous monitoring of GRC



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

Cloud Trust Protocol (CTP)

- Developed by CSC, transferred to CSA
- Open standard and API to verify control assertions
- “Question and Answer” asynchronous protocol, leverages SCAP (Secure Content Automation Protocol)
- Integrates with Cloud Audit
- Now we have all the components for continuous controls monitoring

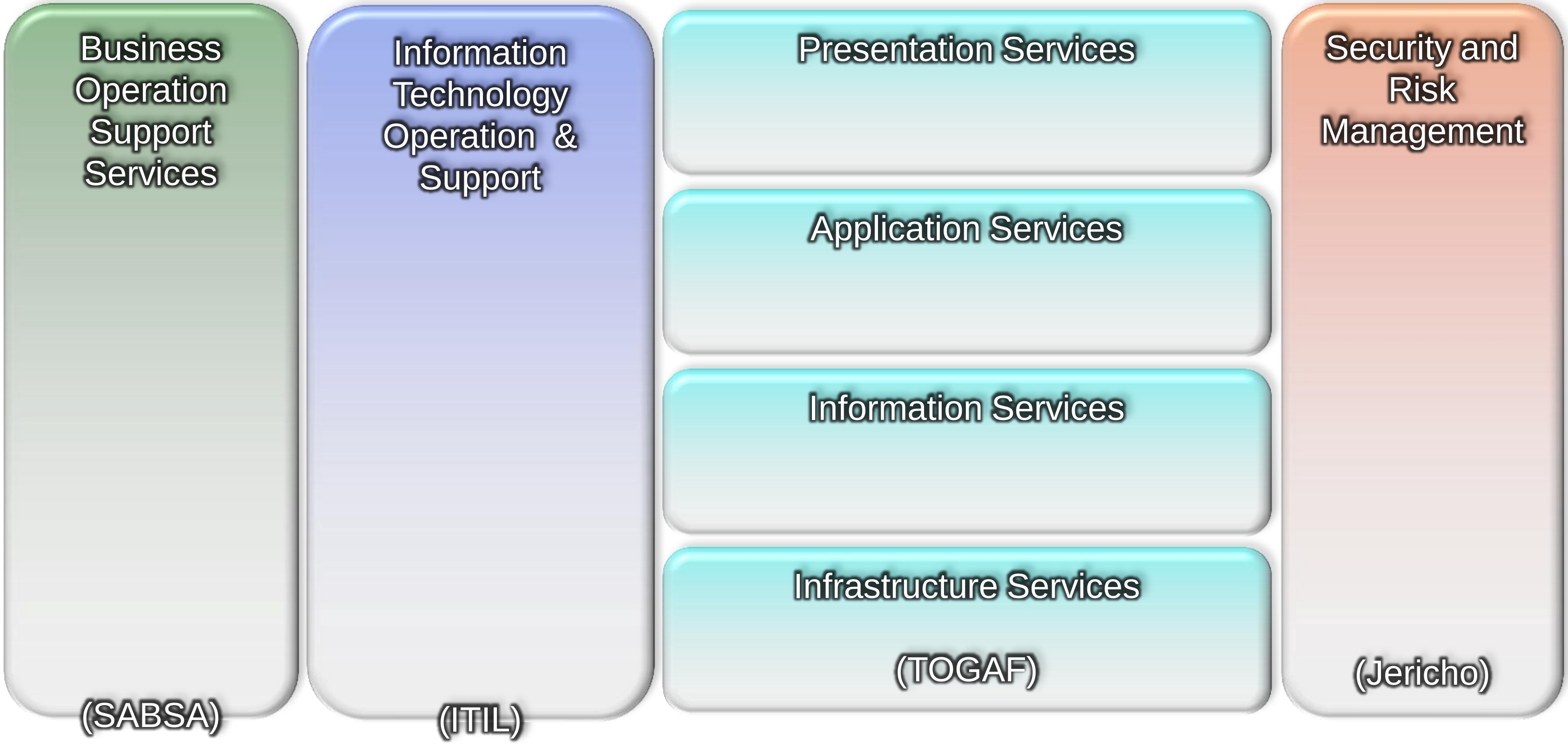
CloudSIRT

- 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



Business Operation Support Services

(SABSA)

Information Technology Operation & Support

(ITIL)

Presentation Services

Application Services

Information Services

Infrastructure Services

(TOGAF)

Security and Risk Management

(Jericho)

Trusted Cloud Initiative

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

Data Governance Project

- Survey of current Cloud Provider data governance practices in the market (e.g. backup, encryption, secure deletion, etc.)
- Structure based on Domain 5: Information Lifecycle Mgt
- Project co-sponsored by CSA Silicon Valley and CSA Singapore
- Target Sept 2011 Report release
- Charter and participation info to be posted on CSA website 1st week of August.

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 Management 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 management
- 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