



# Building an Effective Cloud Security Program

**Becky Swain**

Co-Founder/Chair, CSA CCM  
Board Member, CSA Silicon Valley Chapter  
Partner, EKKO Consulting

**Marlin Pohlman**

Co-Chair, CSA CCM  
Co-Chair/Founder, CSA GRC Stack  
Chief Governance Officer, EMC CTO Office

**Back to Business**

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

Copyright © 2010 Cloud Security Alliance

# What are the Cloud risks?



**Shadow & Consumerization of IT  
Security, Trust & Assurance  
Jurisdictional Data Governance**

# Is Cloud worth it? YES!



Platform for Innovation with Utility IT  
Any Device, Anywhere, Anytime  
Collaboration & Social Media

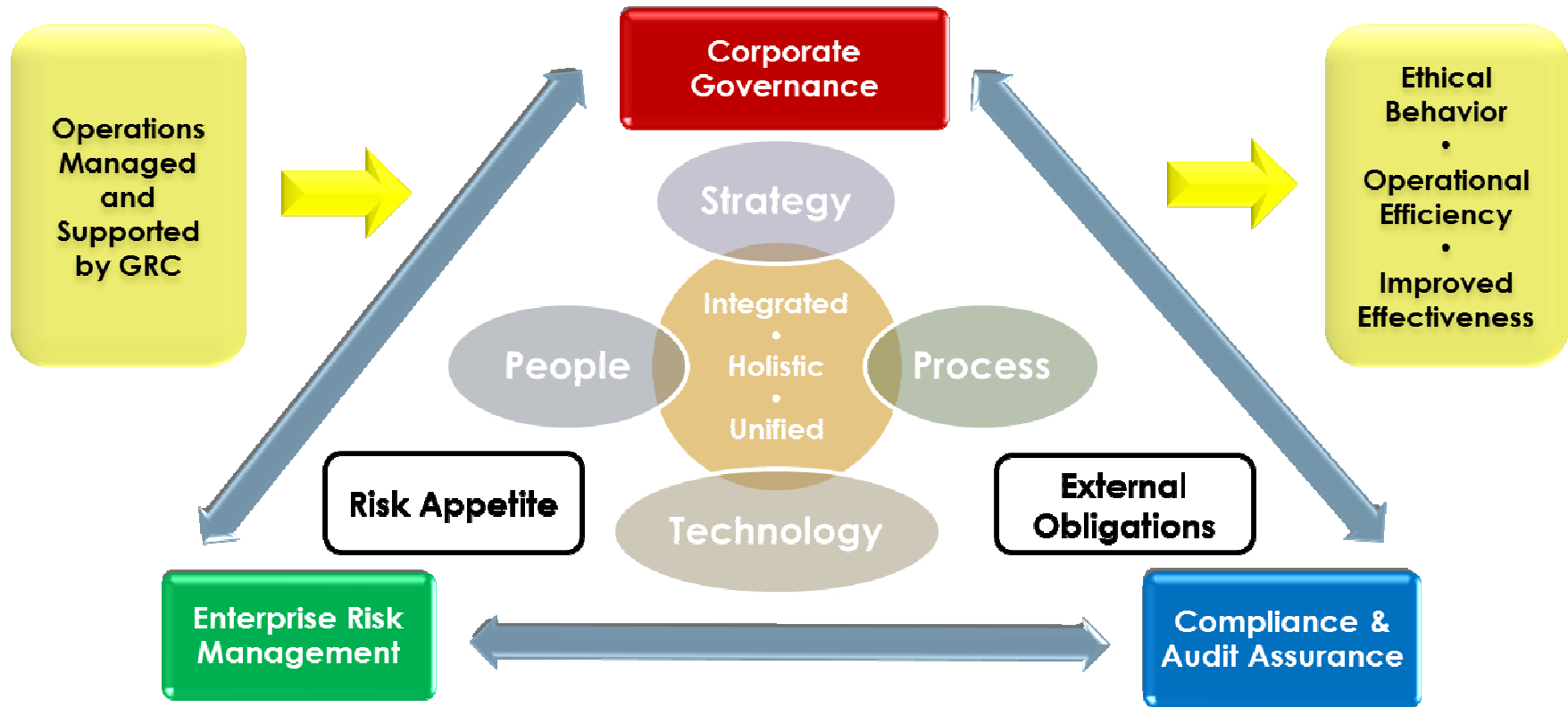


*Back to Business*

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

Copyright © 2010 Cloud Security Alliance

# What is GRC?



# The W's of Cloud Security

- **WHO** are cloud supply chain stakeholders (internal or external)?
- **WHAT** assets (data, credentials, software, hardware) or compliance requirements are impacted?
- **WHERE** are assets hosted (data flows)?
- **HOW** is the environment secured and compliant (architecture security)?
- **WHY?** ... because customers expect it!

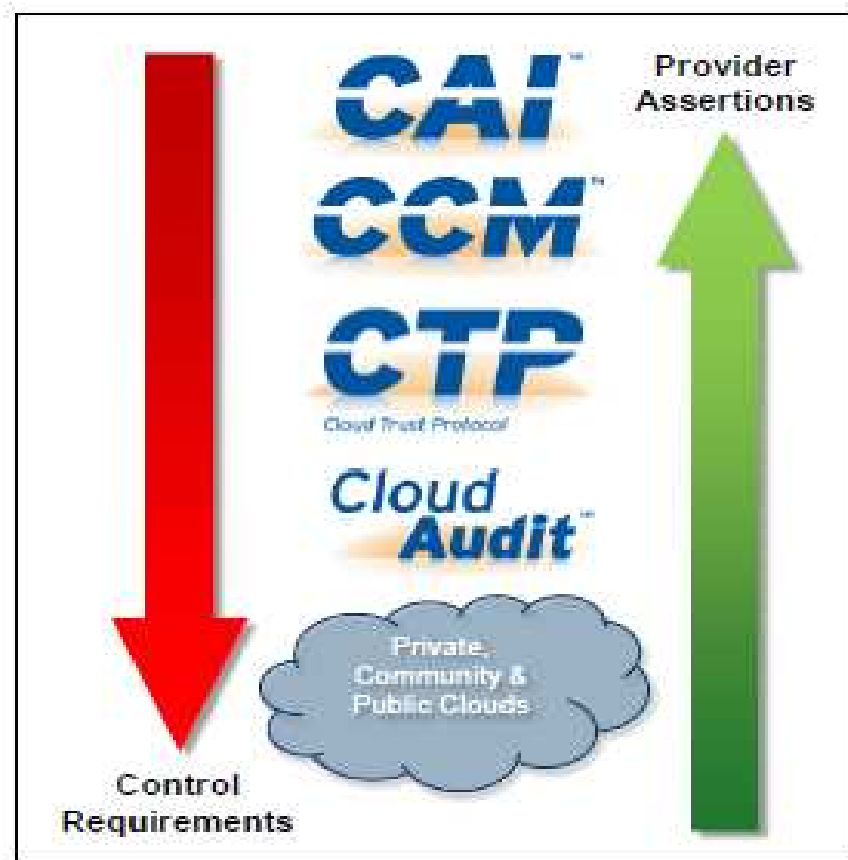
# CSA GRC Stack

## Family of 4 research projects:





- Cloud Controls Matrix (CCM)
- Consensus Assessments Initiative Questionnaire (CAIQ)
- Cloud Trust Protocol (CTP)
- Cloud Audit

*Tools for governance, risk and compliance management.*

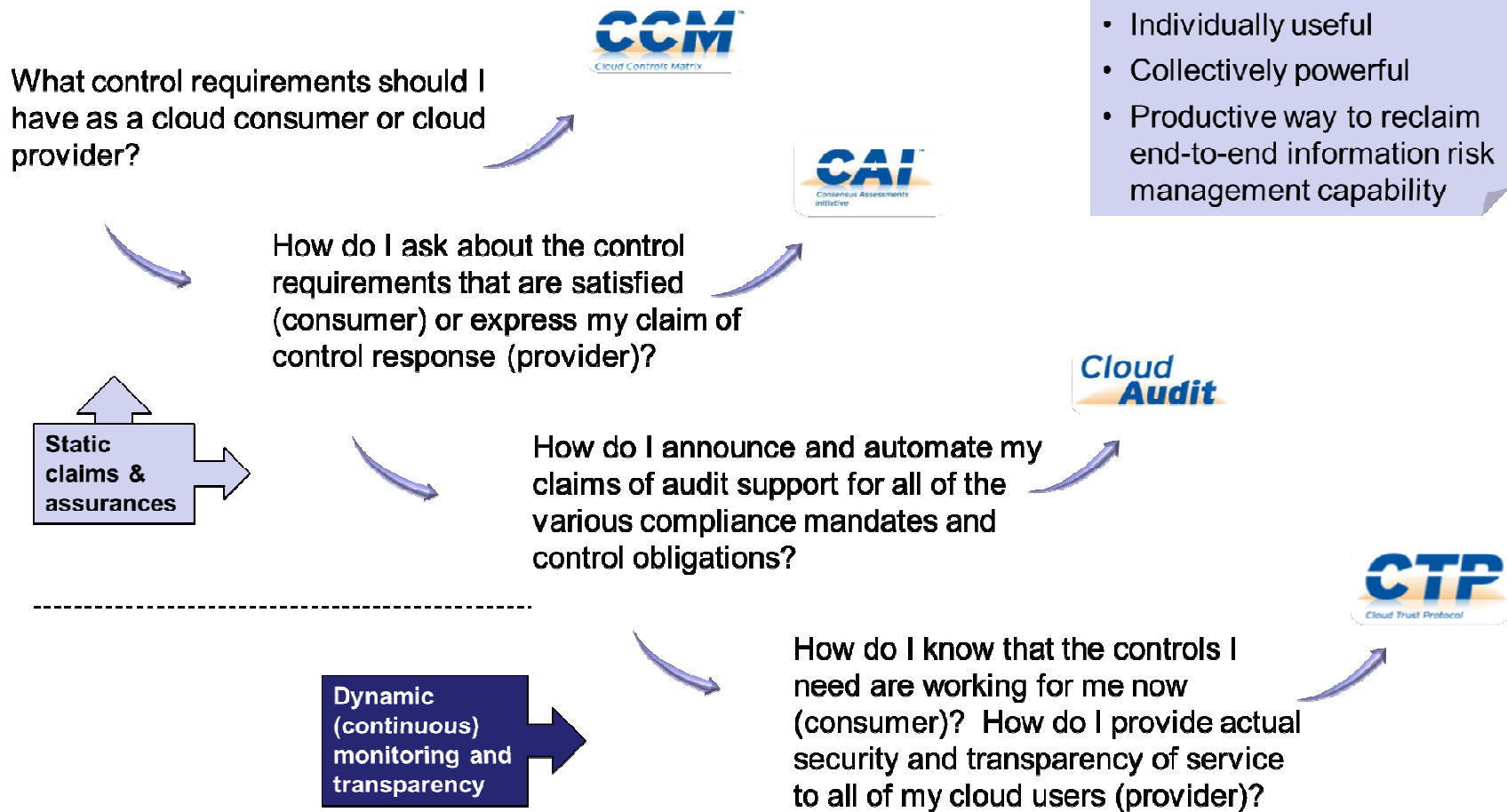
*Enabling automation and continuous monitoring of GRC.*



# CSA GRC Stack (cont.)

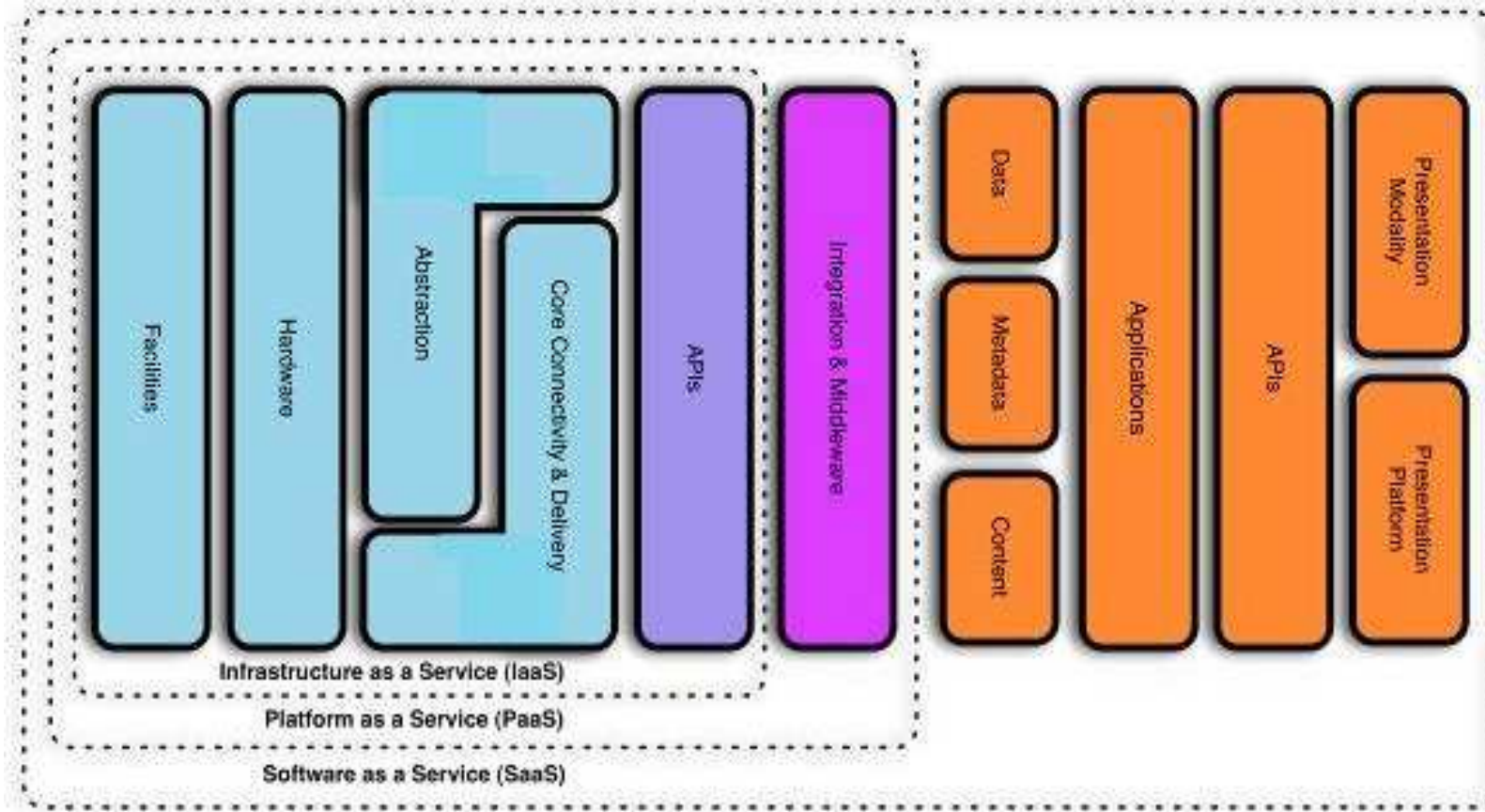
Delivering	← Stack Pack →	Description
<p>Continuous monitoring ... with a purpose</p>		<ul style="list-style-type: none"> <li>• Common technique and nomenclature to request and receive evidence and affirmation of current cloud service operating circumstances from cloud providers</li> </ul>
<p>Claims, offers, and the basis for auditing service delivery</p>		<ul style="list-style-type: none"> <li>• Common interface and namespace to automate the Audit, Assertion, Assessment, and Assurance (A6) of cloud environments</li> </ul>
<p>Pre-audit checklists and questionnaires to inventory controls</p>		<ul style="list-style-type: none"> <li>• Industry-accepted ways to document what security controls exist</li> </ul>
<p>The recommended foundations for controls</p>		<ul style="list-style-type: none"> <li>• Fundamental security principles in specifying the overall security needs of a cloud consumers and assessing the overall security risk of a cloud provider</li> </ul>

# CSA GRC Stack (cont.)





# CSA Cloud Reference Model



# Control Ownership Clarity

CONTROL OWNER?	SaaS	PaaS	IaaS
Data	Joint	Tenant	Tenant
Application	Joint	Joint	Tenant
Compute	Provider	Joint	Tenant
Storage	Provider	Provider	Joint
Network	Provider	Provider	Joint
Physical	Provider	Provider	Provider

# Who is accountable for what?

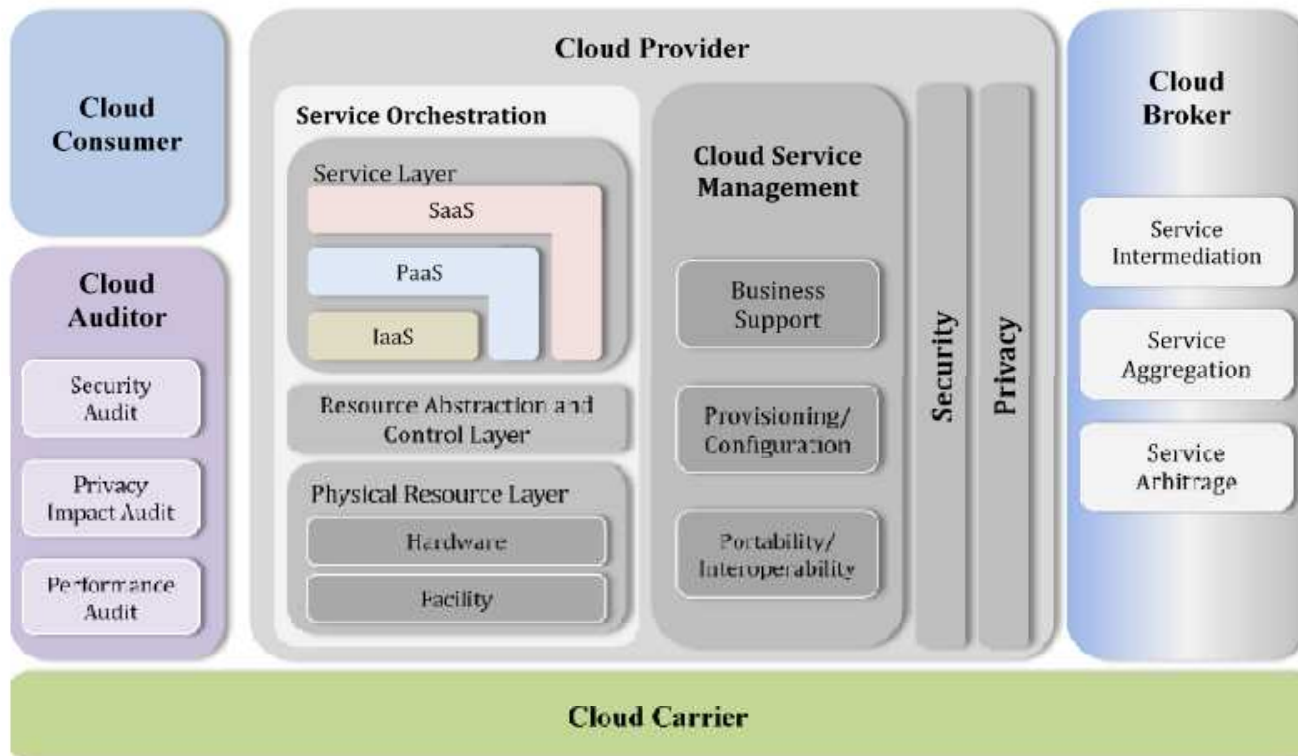


Figure 1: The Conceptual Reference Model

# Cloud Controls Matrix (CCM)



## Leadership Team

- Becky Swain – EKKO Consulting
- Philip Agcailli – Cox Communications
- Marlin Pohlman – EMC, RSA
- Kip Boyle – CSA

- v1.0 (Apr 2010), v1.1 (Dec 2010), v 1.2 (Aug 2011), v2.0 (2012)
- Controls baselined and mapped to:
  - COBIT
  - HIPAA / HITECH Act
  - ISO/IEC 27001-2005
  - NISTSP800-53
  - FedRAMP
  - PCI DSSv2.0
  - BITS Shared Assessments
  - GAPP
  - Jericho Forum
  - NERC CIP

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
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
Information Security - Source Code Access Restriction	IS-33	User access to program source code shall be restricted to authorized personnel.	X	X	X	X	
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
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 renewed 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	



Back to Business

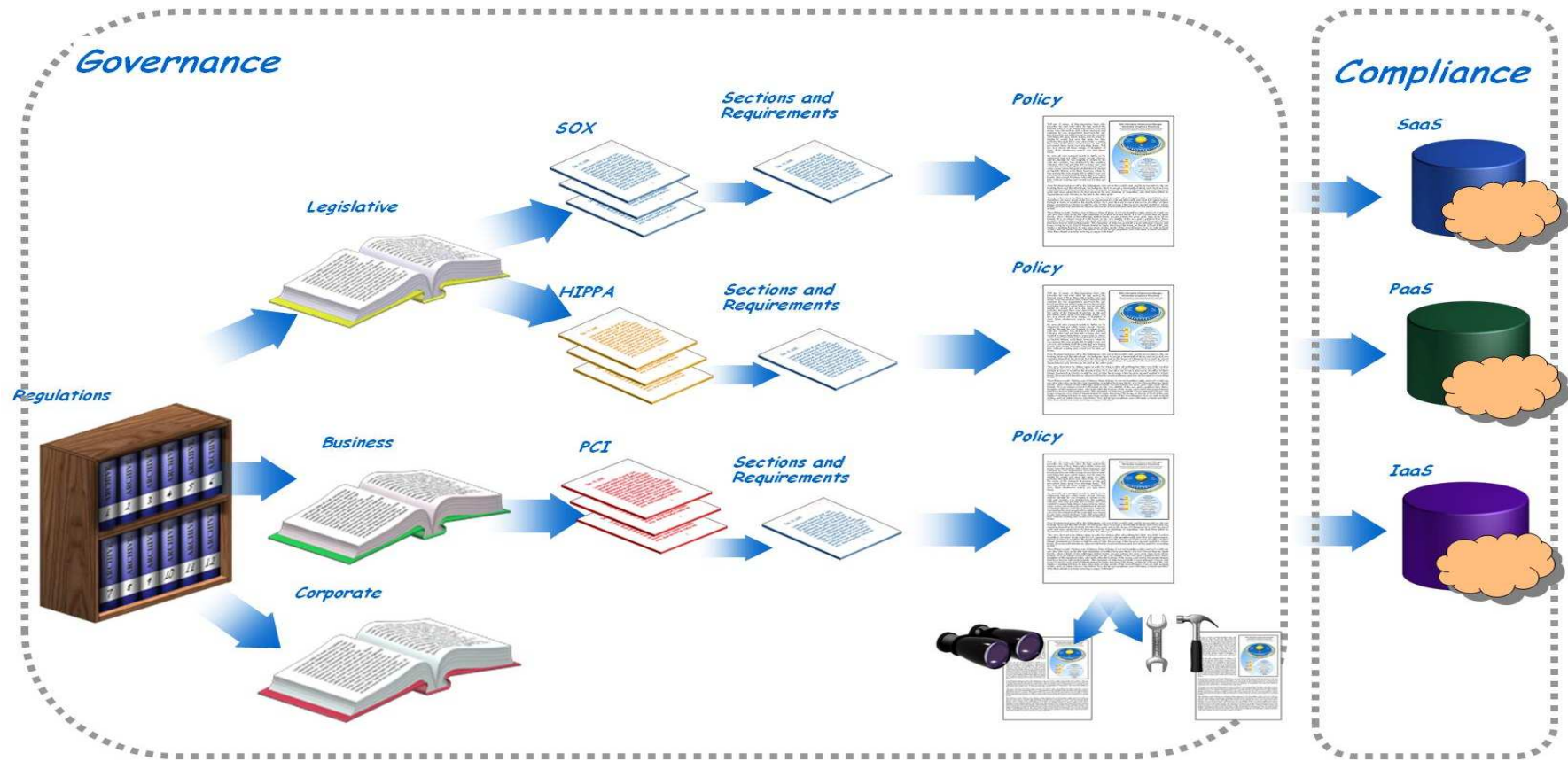
[www.cloudsecurityalliance.org](http://www.cloudsecurityalliance.org)

Copyright © 2010 Cloud Security Alliance

# What is the CCM?

- First ever baseline control framework specifically designed for managing risk in the Cloud Supply Chain:
  - Addressing the inter and intra-organizational challenges of persistent information security by clearly delineating control ownership.
  - Providing an anchor point and common language for balanced measurement of security and compliance postures.
  - Providing the holistic adherence to the vast and ever evolving landscape of global data privacy regulations and security standards.
- Serves as the basis for new industry standards and certifications.

# Optimal & Holistic Compliance



# CCM v1.1 Industry Participation



- Adalberto Afonso A Navarro F do Valle – Deloitte LLP
- Addison Lawrence – Dell
- Akira Shibata – NTT DATA Corp
- Andy Dancer
- Anna Tang – Cisco Systems, Inc.
- April Battle – MITRE
- Chandrasekar Umpathy
- Chris Brenton – Dell
- Dale Pound – SAIC
- Daniel Philpott – Tantus Technologies
- Dr. Anton Chuvakin – Security Warrior Consulting
- Elizabeth Ann Wickham – L47 Consulting Limited
- Gary Sheehan – Advanced Server Mgmt Group, Inc.
- Georg Heß
- Georges Ataya Solvay – Brussels School of Economics & Mgmt
- Glen Jones – Cisco Systems, Inc.
- Greg Zimmerman – Jefferson Wells
- Guy Bejerano - LivePerson
- Henry Ojo – Kamhen Services Ltd,
- Jakob Holm Hansen – Neupart A/S
- Joel Cort – Xerox Corporation
- John DiMaria – HISPI
- John Sapp – McKesson Healthcare, HISPI
- Joshua Schmidt – Vertafore, Inc.
- Karthik Amrutesh – Ernst and Young LLP
- Kelvin Arcelay – Arcelay & Associates
- Kyle Lai – KLC Consulting, Inc.
- Larry Harvey – Cisco Systems, Inc.
- Laura Kuiper – Cisco Systems, Inc.
- Lisa Peterson – Progressive Insurance
- Lloyd Wilkerson – Robert Half International
- Marcelo Gonzalez – Banco Central Republica Argentina
- Mark Lobel – PricewaterhouseCoopers LLP
- Meenu Gupta – Mittal Technologies
- Michael Craigue, Ph.D. – Dell
- Mike Craigue
- MS Prasad, Exec Dir CSA India
- Niall Brownel – LiveOps
- Patrick Sullivan
- Patty Williams – Symetra Financial
- Paul Stephen – Ernst and Young LLP
- Phil Genever-Watling
- Philip Richardson – Logicalis UK Ltd
- Pritam Bankar – Infosys Technologies Ltd.
- Ramesan Ramani – Paramount Computer Systems
- Steve Primost
- Taiye Lambo – eFortresses, Inc .
- Tajeshwar Singh
- Thej Mehta – KPMG LLP
- Thomas Loczewski – Ernst and Young GmbH, Germany
- Vincent Samuel – KPMG LLP
- Yves Le Roux – CA Technologies

***This grass roots movement continues to grow with over 100 volunteer industry experts in the recent release of v1.2!***

# CCM – 11 Domains

1. Compliance (CO)
2. Data Governance (DG)
3. Facility Security (FS)
4. Human Resources (HR)
5. Information Security (IS)
6. Legal (LG)
7. Operations Management (OM)
8. Risk Management (RI)
9. Release Management (RM)
10. Resiliency (RS)
11. Security Architecture



# CCM – 98 Controls

## **Compliance**

- **CO01 – Audit Planning**
- **CO02 – Independent Audits**
- **CO03 – Third Party Audits**
- **CO04 – Contact / Authority Maintenance**
- **CO05 – Information System Regulatory Mapping**
- **CO06 – Intellectual Property**

## **Risk Management**

- **RI01 – Program**
- **RI02 – Assessments**
- **RI03 – Mitigation / Acceptance**
- **RI04 – Business / Policy Change Impacts**
- **RI05 – Third Party Access**

## **Legal**

- **LG01 - Non-Disclosure Agreements**
- **LG02 - Third Party Agreements**

## **Data Governance**

- **DG01 – Ownership / Stewardship**
- **DG02 – Classification**
- **DG03 – Handling / Labeling / Security Policy**
- **DG04 – Retention Policy**
- **DG05 – Secure Disposal**
- **DG06 – Non-Production Data**
- **DG07 – Information Leakage**
- **DG08 – Risk Assessments**

# CCM – 98 Controls (cont.)

## **Human Resources**

- HR01 – Background Screening
- HR02 – Employment Agreements
- HR03 – Employment Termination

## **Release Management**

- RM01 – New Development / Acquisition
- RM02 – Production Changes
- RM03 – Quality Testing
- RM04 – Outsourced Development
- RM05 – Unauthorized Software Installations

## **Resiliency**

- RS01 – Management Program
- RS02 – Impact Analysis
- RS03 – Business Continuity Planning
- RS04 – Business Continuity Testing
- RS05 – Environmental Risks
- RS06 – Equipment Location
- RS07 – Equipment Power Failures
- RS08 – Power / Telecommunications

## **Operational Management**

- OP01 – Policy
- OP02 – Documentation
- OP03 – Capacity / Resource Planning
- OP04 – Equipment Maintenance

# CCM – 98 Controls (cont.)

## **Security Architecture**

- SA01 – Customer Access Requirements
- SA02 – User ID Credentials
- SA03 – Data Security / Integrity
- SA04 – Application Security
- SA05 – Data Integrity
- SA06 – Production / Non-Production Environments
- SA07 – Remote User Multi-Factor Authentication
- SA08 – Network Security
- SA09 – Segmentation
- SA10 – Wireless Security
- SA11 – Shared Networks
- SA12 – Clock Synchronization
- SA13 – Equipment Identification
- SA14 – Audit Logging / Intrusion Detection
- SA15 – Mobile Code

## **Facility Security**

- FS01 – Policy
- FS02 – User Access
- FS03 – Controlled Access Points
- FS04 – Secure Area Authorization
- FS05 – Unauthorized Persons Entry
- FS06 – Off-Site Authorization
- FS07 – Off-Site Equipment
- FS08 – Asset Management

# CCM – 98 Controls (cont.)

## **Information Security**

- **IS01 – Management Program**
- **IS02 – Management Support / Involvement**
- **IS03 – Policy**
- **IS04 – Baseline Requirements**
- **IS05 – Policy Reviews**
- **IS06 – Policy Enforcement**
- **IS07 – User Access Policy**
- **IS08 – User Access Restriction / Authorization**
- **IS09 – User Access Revocation**
- **IS10 – User Access Reviews**
- **IS11 – Training / Awareness**
- **IS12 – Industry Knowledge / Benchmarking**
- **IS13 – Roles / Responsibilities**
- **IS14 – Management Oversight**
- **IS15 – Segregation of Duties**
- **IS16 – User Responsibility**
- **IS17 – Workspace**
- **IS18 – Encryption**
- **IS19 – Encryption Key Management**
- **IS20 – Vulnerability / Patch Management**
- **IS21 – Anti-Virus / Malicious Software**
- **IS22 – Incident Management**
- **IS23 – Incident Reporting**
- **IS24 – Incident Response Legal Preparation**
- **IS25 – Incident Response Metrics**
- **IS26 – Acceptable Use**
- **IS27 – Asset Returns**
- **IS28 – eCommerce Transactions**
- **IS29 – Audit Tools Access**
- **IS30 – Diagnostic / Configuration Ports Access**
- **IS31 – Network Services**
- **IS32 – Portable / Mobile Devices**
- **IS33 – Source Code Access Restriction**
- **IS34 – Utility Programs Access**

# Consensus Assessments Initiative Questionnaire (CAIQ)



## Leaders

- Laura Posey – Microsoft
- Jason Witty – Bank of America
- Marlin Pohlman – EMC, RSA
- Earle Humphreys – ITEEX



Control Group	CGID	CID	Consensus Assessment Questions	Comments and Notes	COBIT	HIPAA	ISO27001	SP800_53
Audit Planning	CO-01	CO-01.1	Do you produce audit assertions using a structured, industry accepted format (ex. CloudAudit/AG URI Ontology, CloudTrust, SCAP/CYBEX, GRC XML, ISACA's Cloud Computing Management Audit/Assurance Program, etc.)?		COBIT 4.1 ME 2.1, ME 2.2 PO 9.5 PO 9.6	45 CFR 164.312(b)	Clause 4.2.3 a) Clause 4.2.3b Clause 5.1 g Clause 6 A.15.3.1	NIST SP800-53 R3 CA-2 NIST SP800-53 R3 CA-7 NIST SP800-53 R3 PL-6
Independent Audits	CO-02	CO-02.1	Do you allow tenants to view your SAS70 Type II/SSAE 16 SOC2/ISAE3402 or similar third party audit reports?		COBIT 4.1 DS5.5, ME2.5, ME 3.1 PO 9.6	45 CFR 164.308 (a)(8) 45 CFR 164.308(a)(1)(i)(D)	Clause 4.2.3e Clause 5.1 g Clause 5.2.1 d) Clause 6 A.6.1.8	NIST SP800-53 R3 CA-1 NIST SP800-53 R3 CA-2 NIST SP800-53 R3 CA-6 NIST SP800-53 R3 RA-5
		CO-02.2	Do you conduct network penetration tests of your cloud service infrastructure regularly as prescribed by industry best practices and guidance?					
		CO-02.3	Do you conduct regular application penetration tests of your cloud infrastructure as prescribed by industry best practices and guidance?					
		CO-02.4	Do you conduct internal audits regularly as prescribed by industry best practices and guidance?					
		CO-02.5	Do you conduct external audits regularly as prescribed by industry best practices and guidance?					
		CO-02.6	Are the results of the network penetration tests available to tenants at their request?					
		CO-02.7	Are the results of internal and external audits available to tenants at their request?					
Third Party Audits	CO-03	CO-03.1	Do you permit tenants to perform independent vulnerability assessments?		COBIT 4.1 ME 2.6, DS 2.1, DS 2.4	45 CFR 164.308(b)(1) (New)	A.6.2.3 A.10.2.1 A.10.2.2 A.10.6.2	NIST SP800-53 R3 CA-3 NIST SP800-53 R3 SA-9 NIST SP800-53 R3 SA-12 NIST SP800-53 R3 SC-7
		CO-03.2	Do you have external third-party conduct vulnerability scans and periodic penetration tests on your applications and networks?			45 CFR 164.308 (b)(4)		
Contact / Authority	CO-04	CO-04.1	Do you maintain liaisons and points of contact with local authorities in		COBIT 4.1 ME 3.1		A.6.1.6	NIST SP800-53 R3 AT-5



Back to Business

[www.cloudsecurityalliance.org](http://www.cloudsecurityalliance.org)  
Copyright © 2010 Cloud Security Alliance

# What is the CAIQ?

- Cloud Supply Chain risk management and due diligence questionnaire (148 questions)
  - Enables 1 or more Cloud service providers to demonstrate compliance with the CSA CCM.
  - Forms the basis for establishing Cloud specific Service Level Objectives that can be incorporated into supplier agreements.
- Along with CSA CCM, integrated into third party GRC solution providers.

# CloudAudit (formerly A6)

- Provides an open, extensible and secure interface for automation of Audit, Assertion, Assessment, and Assurance (A6) of cloud computing environments
- A structure for organizing assertions and supporting documentation for specific controls across different compliance frameworks in a way that simplifies discovery by humans and tools.
  - Define a namespace that can support diverse frameworks.
  - Expressed in namespace – CSA CCM, ISO/IEC 27001, COBIT, HIPAA, NIST SP 800-53, PCI DSS.
  - Defines the mechanisms for requesting and responding to queries relating to specific controls.
  - Integrates with portals and AAA systems.

# Sample Implementation – CSA Compliance Pack



A6: The Automated Audit, Assertion, Assessment, and Assurance API.

enhttps://cloud.enstratus.com/.well-known/cloudaudit/ enStratus Networks LLC Google CONTACT US 612.746.3091

**enSTRATUS**

### Compliance Information

Author: George Reese (george.reese@enstratus.com)  
Date: 2010-08-17T14:01:58Z

- CSA Guidance

For more information on CloudAudit, see [the CloudAudit web site](#).

Copyright © 2010 enStratus Networks LLC CONFIDENTIAL – FOR ENSTRATUS CUSTOMER USE ONLY





# Sample Implementation – CSA Compliance Pack



A6: The Automated Audit, Assertion, Assessment, and Assurance API.

enStratus Networks LLC | Google

enSTRATUS CONTACT US 612.746

**CSA Guidance Assertions for enStratus**

Author: George Reese (george.reese@enstratus.com)  
Date: 2010-08-17T14:01:58Z

Control	Name	Description	Assertion
CO-01	Compliance - Audit Planning	Audit requirements and activities involving checks on operational systems shall be carefully planned and agreed to, to minimize the risk of disruptions to business processes, focusing on data duplication, access, and data boundary limitations.	yes
CO-02	Compliance - Independent Audits	Independent reviews and assessments shall be performed at least annually, or at planned intervals, to ensure the organization is compliant with policies, procedures, standards and applicable regulatory requirements (i.e., internal/external audits, certifications, vulnerability and penetration testing,	no
CO-03	Compliance - Third Party Audits	Third party service providers shall demonstrate compliance with information security and confidentiality, service definitions and delivery level agreements included in third party contracts. The services, reports and records provided by the third party shall be regularly monitored and reviewed, and audits shall be carried out regularly to govern and maintain compliance with the service delivery agreements.	yes



# Sample Implementation – CSA Compliance Pack



A6: The Automated Audit, Assertion, Assessment, and Assurance API.

enStratus Network

enSTRATUS

**Compliance - Audit Planning**

*Assertion: yes*  
*Author: George Reese (george.reese@enstratus.com)*  
*Date: : 2010-08-17T01:30:05Z*

- [enStratus Information Systems Policies and Procedures.pdf](#)

*For more information on CloudAudit, see the CloudAudit web site .*

# Cloud Trust Protocol (CTP)



- Mechanism by which Cloud service consumers ask providers for and receive information about the elements of transparency as applied to cloud service providers to liberate Cloud consumers to bring more sensitive and valuable business functions to the cloud.
- Details a mechanism to communicate enhanced SCAP – CYBEX/RID/CEE exchanges, offers a Representational State Transfer (REST) mechanism with Hypermedia as the Engine of Application State (HATEOAS), and interfaces with CloudAudit.

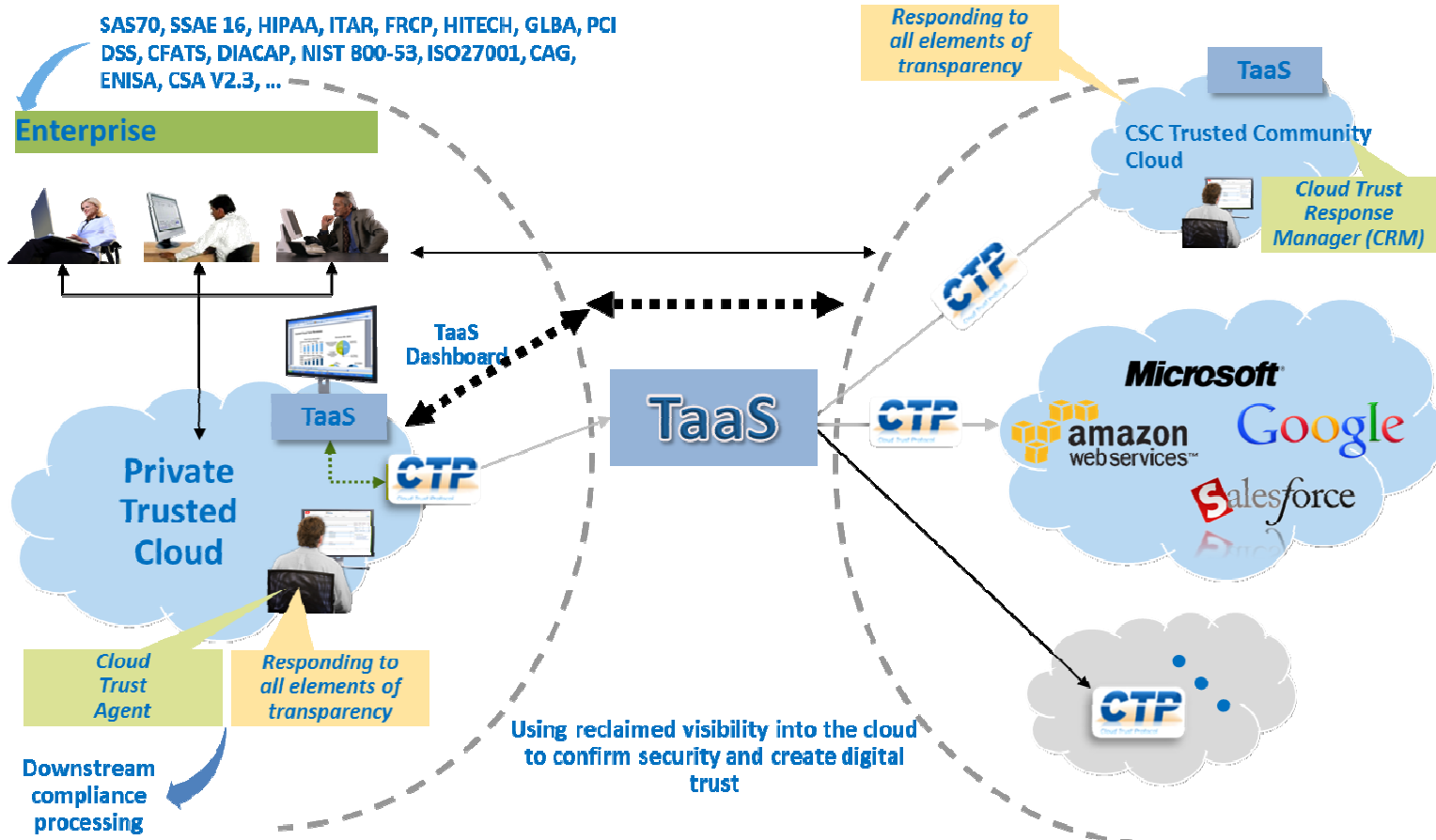
# What is CTP?



## VALUE Captured

*Delivering evidence-based confidence...  
with compliance-supporting data & artifacts.*

# Transparency as a Service (TaaS)



Source: [http://www.csc.com/cloud/insights/57785-into\\_the\\_cloud\\_with\\_ctp](http://www.csc.com/cloud/insights/57785-into_the_cloud_with_ctp)

# Elements of Transparency

Admin & Ops	Specs	Transparency Requests			Extensions
		Assertions	Evidence	Affirmations	
	Configuration definition: 20	Security capabilities and operations: 17	Configuration & vulnerabilities: 3,4,5,6,7	Anchoring: 8, 9, 10 (geographic, platform, process)	
	<div style="border: 1px solid black; background-color: #f0f0f0; padding: 5px; text-align: center;">SCAP</div>	<div style="border: 1px solid black; background-color: #d3d3d3; padding: 5px; text-align: center;">CloudAudit.org</div>	<div style="border: 1px solid black; background-color: #f0f0f0; padding: 5px; text-align: center;">SCAP</div>	<div style="border: 1px solid black; background-color: #ffff00; padding: 5px; text-align: center;">Sign / sealing</div>	
Session start: 1 Session end: 2 Alerts: 18	Users: 19 Anchors: 21 Quotas: 22 Alert conditions: 23		Violation: 11 Audit: 12 Access: 13 Incident log: 14 Config/control: 15 Stats: 16		Consumer/provider negotiated: 24



# CSA Security Trust & Assurance Registry (STAR)



*Public and free registry of Cloud Provider self assessments, demonstrating adoption of:*

- Cloud Controls Matrix (CCM)
  - Consensus Assessments Initiative Questionnaire (CAIQ)
- *Voluntary industry action promoting transparency.*
- *Free market competition to provide quality assessments.*
- *Available October 2011.*



# CSA STAR Listing Process

- Provider fills out CAIQ or customizes CCM
- Uploads document at /star
- CSA performs basic verification
  - Authorized listing from provider
  - Delete SPAM, “poisoned” listing
  - Basic content accuracy check
- CSA digitally signs and posts at /star



# CSA STAR FAQ

- **Where?** [www.cloudsecurityalliance.org/star/](http://www.cloudsecurityalliance.org/star/)
- **Help?** Special LinkedIn support group and private mailbox moderated by CSA volunteers
- **Costs?** Free to post, free to use
- **Is this a new hacker threat vector?** No, it is responsible disclosure of security practices
- **Will CSA police STAR?** Initial verification and maintenance of “Abuse” mailbox
- **Do listings expire?** Yes, 1 year limit

# Why Not Certification or 3<sup>rd</sup> Party Assessment?



- Complex to do certification right
  - Many uses of cloud, many customer needs
  - Different risk profiles for each
- CSA supporting broad industry consortia and standards bodies
  - ISO/IEC, ITU-T
  - Common Assurance Maturity Model (CAMM – 3rd Party assessment)
  - GRC Stack aligns with common requirements (e.g. PCI/DSS, HIPAA, FedRAMP, 27001, CoBIT, etc)
- Self assessment & transparency complements all
  - STAR could be part of SSAE 16 SOC 2 report (SAS 70 Type II replacement)

# Is CSA STAR a temporary or ultimate assurance solution?

- Neither
- Permanent effort to drive transparency, competition, innovation and self regulation with agility – crowdsourcing cloud security
- Does not provide automation, 3<sup>rd</sup> party assessment, relative/absolute scoring, real-time controls monitoring, etc.
- Ultimate assurance is real time GRC (enabled by CloudAudit) complemented by CSA STAR and 3<sup>rd</sup> party attestation – CSA will look to solution providers to deliver this integration.

# CSA STAR – What You Should Do



- ***Providers***

- Start filling out CAIQ and/or CCM
- Ask us for help

- ***Customers***

- Put your providers on notice, point them to CAIQ and/or CCM
- Make CSA STAR entries a standard part of procurement & assessment
- Get ready for October!

***Security Guidance for Critical Areas of Focus in Cloud Computing*** – v1.0 (founding publication), v2.1 (available for download and incorporated into CSA CCSK, v3.0 (in progress)).

Domain 1: Cloud Computing Architectural Framework

Domain 2: Governance, Risk and Compliance

Domain 3: Legal and Electronic Discovery

Domain 4: Audit and Assurance

Domain 5: Information Lifecycle Management

Domain 6: Portability and Interoperability

Domain 7: Traditional Security, Business Continuity and Disaster Recovery

Domain 8: Data Operations

Domain 9: Incident Response, Notification, and Remediation

Domain 10: Application Security

Domain 11: Encryption and Key Management

Domain 12: Identity and Access Management

Domain 13: Security as a Service



# CSA Collaboration with SBOs



**HITRUST**



THE *Open* GROUP



**Back to Business**

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

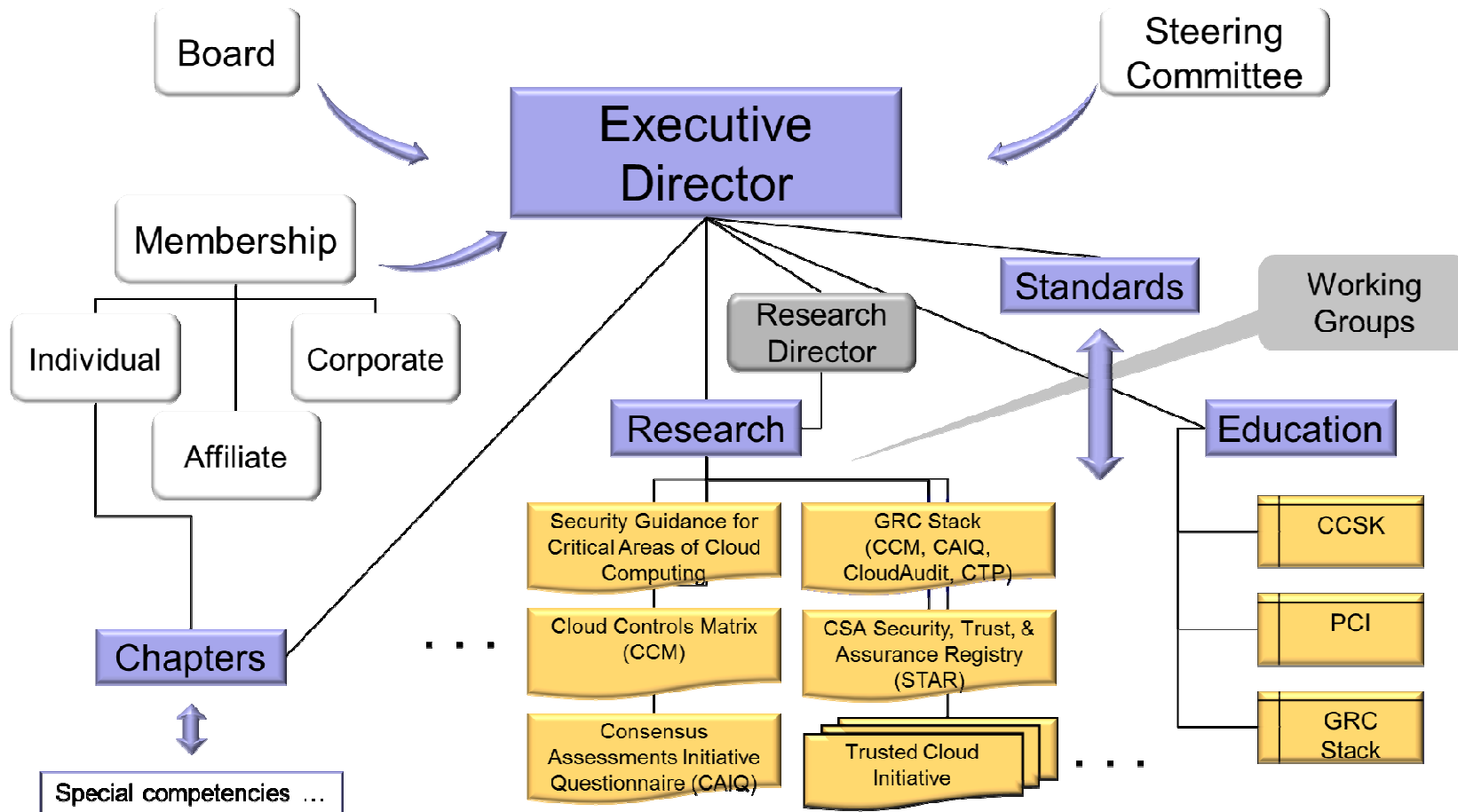
Copyright © 2010 Cloud Security Alliance

# About the Cloud Security Alliance (CSA)



- Non-profit organization formed 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.
  - Promoting a common level of understanding between the consumers and providers of cloud computing regarding the security requirements and attestation of assurance
  - Promoting independent research into best practices for cloud computing security
  - Launching awareness campaigns and educational programs on the appropriate uses of cloud computing and cloud security solutions
  - Creating consensus lists of issues and guidance for cloud security assurance

# CSA Organization & Operations





# CSA Silicon Valley Chapter



- **Mission**: Foster education and transparency of emerging and innovative technologies supporting best in class solutions for Cloud Security.
  - Join and look for chapter announcements from LinkedIn subgroup
  - Monthly chapter meetings, free to attend in person or via conference call (scheduled using the Meetup app)
  - Hosted inaugural CSA Innovation Conference 2011 on October 6<sup>th</sup> in Silicon Valley

# Contact CSA



- *Help us secure cloud computing!*
  - [www.cloudsecurityalliance.org](http://www.cloudsecurityalliance.org)
  - [info@cloudsecurityalliance.org](mailto:info@cloudsecurityalliance.org)
  - LinkedIn: [www.linkedin.com/groups?gid=1864210](http://www.linkedin.com/groups?gid=1864210)
  - Twitter: @cloudsa
  - Join your local CSA Chapter:  
<https://cloudsecurityalliance.org/chapters/>

# THANK YOU!