Cloud Risks and Opportunities

John Howie

About the Cloud Security Alliance

- Global, not-for-profit organization
- Building security best practices for next generation IT
- Research and Educational Programs
- Cloud Provider Certification
- User Certification
- Awareness and Marketing
- The globally authoritative source for Trust in the Cloud

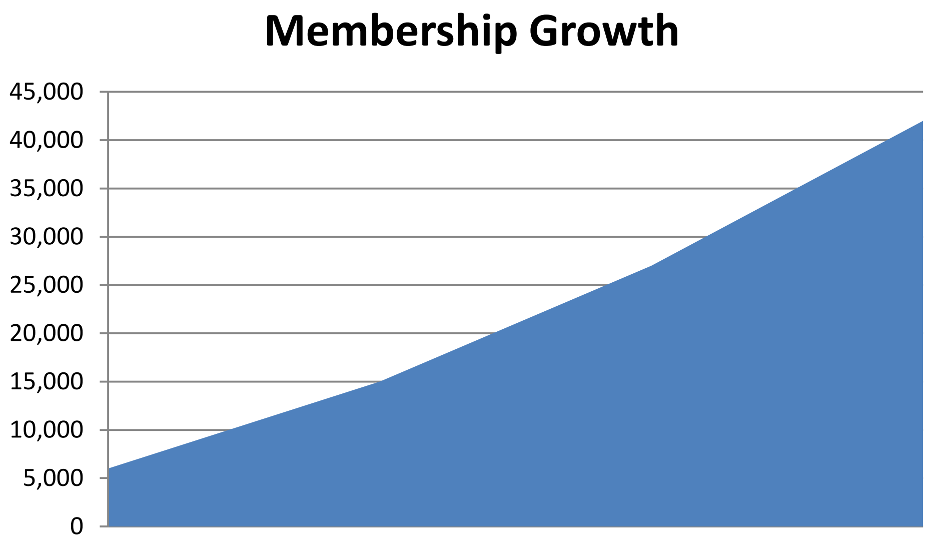
“To promote the use of best practices for providing security assurance within Cloud Computing, and provide education on the uses of Cloud Computing to help secure all other forms of computing.”

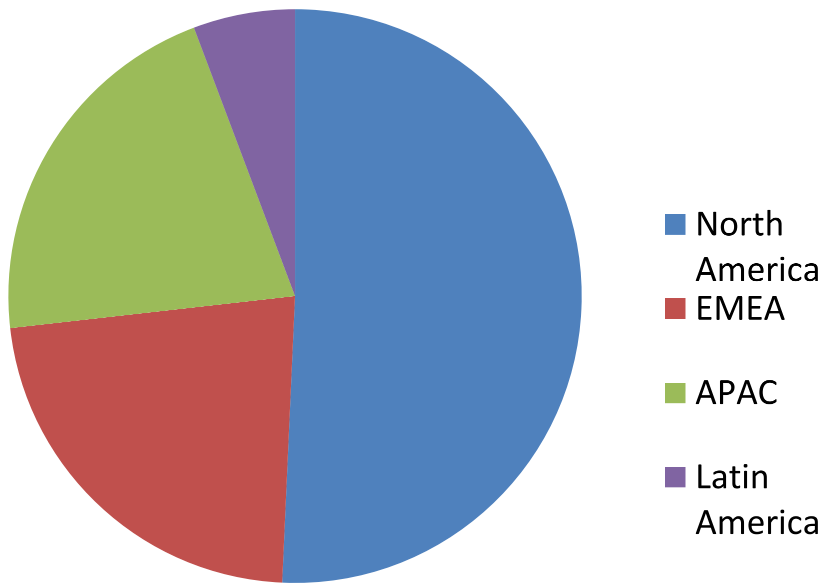
CSA Fast Facts

- Founded in 2009
- Membership stats
  - 48,000 individual members, 66 chapters globally
  - 170+ corporate members
  - Major cloud providers, tech companies, infosec leaders, governments, financial institutions, retail, healthcare and more
- Offices in Seattle USA, Singapore, Greece
- Over 30 research projects in 25 working groups
- Strategic partnerships with governments, research institutions, professional associations and industry

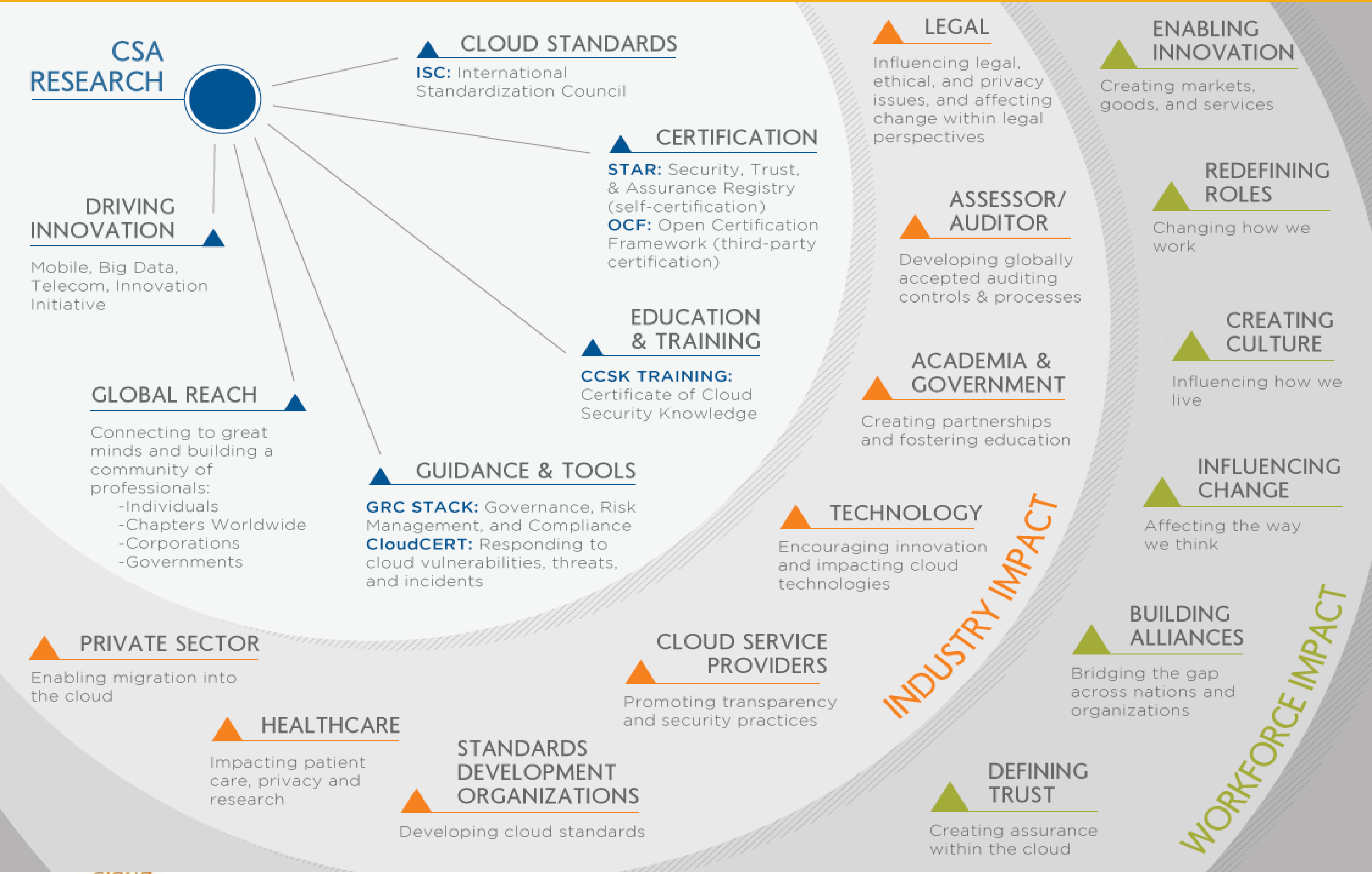
Growing to serve the Industry

- 2009
  - CSA launch at RSA 2009 with Security Guidance for Critical Areas of Focus in Cloud Computing
  - 6,000 members
- 2010
  - Launch Certificate of Cloud Security Knowledge (CCSK)
  - 15,000 members
- 2011
  - Launch CSA Security, Trust and Assurance Registry (STAR)
  - 27,000 members
- 2012
  - Launch CSA Mobile and Big Data research to address emerging needs
  - 42,000 members





IMPACT OF CSA RESEARCH



CSA RESEARCH

CLOUD STANDARDS

ISC: International Standardization Council

CERTIFICATION

STAR: Security, Trust, & Assurance Registry (self-certification)
OCF: Open Certification Framework (third-party certification)

EDUCATION & TRAINING

CCSK TRAINING: Certificate of Cloud Security Knowledge

GUIDANCE & TOOLS

GRC STACK: Governance, Risk Management, and Compliance
CloudCERT: Responding to cloud vulnerabilities, threats, and incidents

GLOBAL REACH

Connecting to great minds and building a community of professionals:

- -Individuals
- -Chapters Worldwide
- -Corporations
- -Governments

DRIVING INNOVATION

Mobile, Big Data, Telecom, Innovation Initiative

INDUSTRY IMPACT

LEGAL

Influencing legal, ethical, and privacy issues, and affecting change within legal perspectives

ASSESSOR/ AUDITOR

Developing globally accepted auditing controls & processes

ACADEMIA & GOVERNMENT

Creating partnerships and fostering education

TECHNOLOGY

Encouraging innovation and impacting cloud technologies

CLOUD SERVICE PROVIDERS

Promoting transparency and security practices

STANDARDS DEVELOPMENT ORGANIZATIONS

Developing cloud standards

HEALTHCARE

Impacting patient care, privacy and research

PRIVATE SECTOR

Enabling migration into the cloud

WORKFORCE IMPACT

ENABLING INNOVATION

Creating markets, goods, and services

REDEFINING ROLES

Changing how we work

CREATING CULTURE

Influencing how we live

INFLUENCING CHANGE

Affecting the way we think

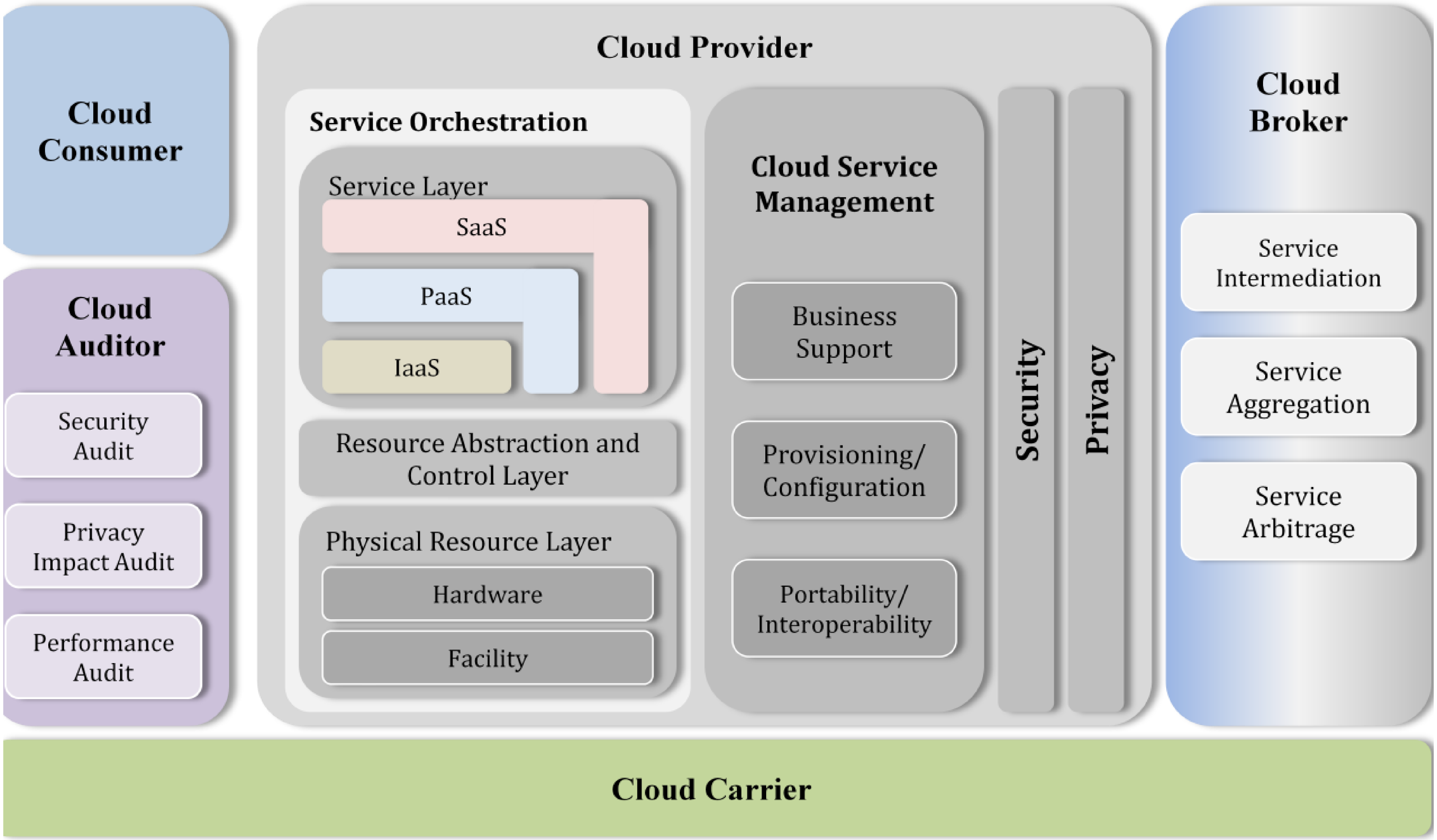
BUILDING ALLIANCES

Bridging the gap across nations and organizations

DEFINING TRUST

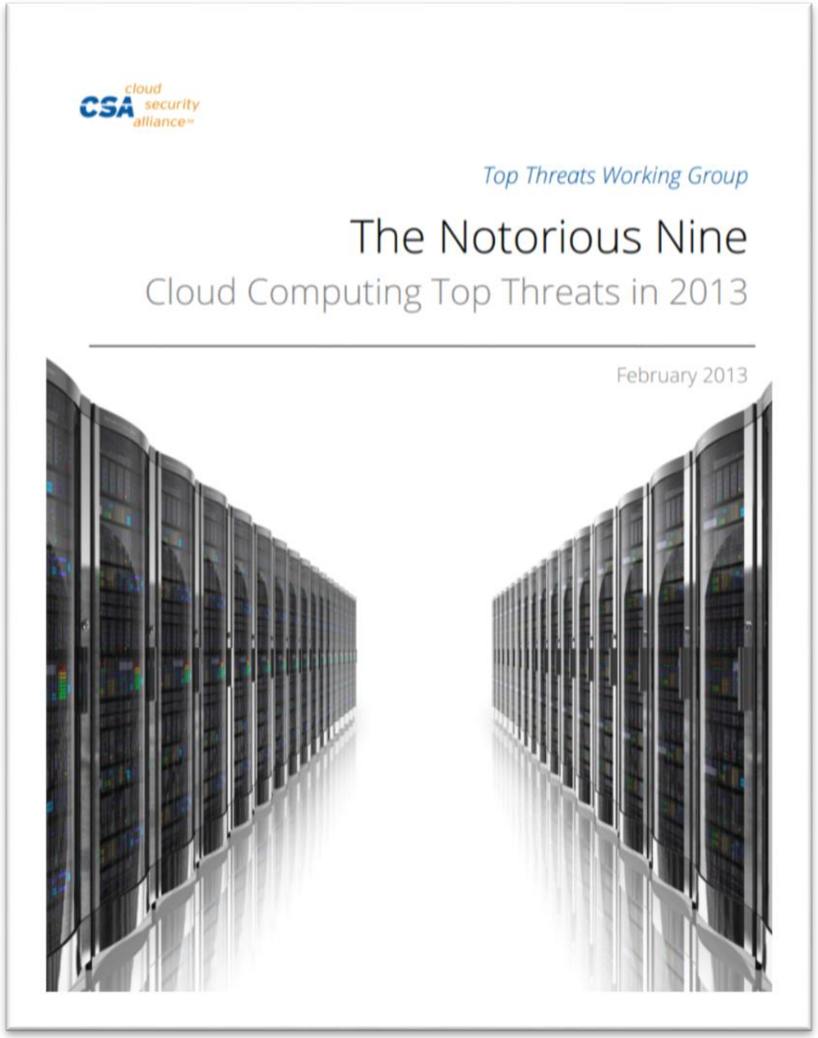
Creating assurance within the cloud

Cloud Actors



CLOUD CONSUMER

About the Notorious Nine



Top Threats Working Group

The Notorious Nine

Cloud Computing Top Threats in 2013

February 2013

The Notorious Nine can be downloaded here

Top Threats™ To Cloud Computing

- Top Threats WG formed in 2009 to engage experts and the broader community to identify top security threats for Cloud Computing
- Purpose of the series of reports was to educate cloud providers/consumers on how to mitigate risk when deploying/adopting cloud computing
- Expanded the report from the “Seven Deadly Sins” to the “Evil 8” to the “Notorious 9” in 2013
- New version mapped to Cloud Controls Matrix and Risk Matrix added (Actual vs. Perceived Risk)

Notorious Nine Methodology

- Surveyed over 300 Security Professionals from 50 countries globally
- Validated that the threat listing reflects the most current concerns of the industry
- Reflected current consensus among experts about the most significant threats to cloud security
- Experts identified nine critical threats to cloud computing in 2013

9 Threats Identified (1 – 4)

- #1 Threat: Data Breaches
  - Ranking Comparison 5 2010 ↗ 1 2013
- #2 Threat: Data Loss
  - Ranking Comparison* 5 2010 ↗ 2 2013

* Data Breaches & Data Loss were considered one threat in the previous report

- #3 Threat: Account or Service Traffic Hijacking
  - Ranking Comparison 6 2010 ↗ 3 2013
- #4 Threat: Insecure Interfaces and APIs
  - Ranking Comparison 2 2010 ↘ 4 2013

9 Threats Identified (5 – 9)

- #5 Threat: Denial of Service
  - Ranking Comparison N/A 2010 → 5 2013
- #6 Threat: Malicious Insiders
  - Ranking Comparison 3 2010 → 6 2013
- #7 Threat: Abuse of Cloud Services
  - Ranking Comparison 1 2010 → 7 2013
- #8 Threat: Insufficient Due Diligence
  - Ranking Comparison 7 2010 → 8 2013
- #9 Threat: Shared Technology Vulnerabilities
  - Ranking Comparison 4 2010 → 9 2013

CLOUD CARRIER

Internet Threats

- Attacks against internet infrastructure continue to plague us
  - Routing hijacks (BGP)
  - DNS compromise
  - PKI
- Some solutions exist, but…
  - The current protocols are fundamentally broken
  - We need to start over (IPv6 is not a solution)

cloud security alliance℠

CLOUD PROVIDER

Traditional Approach

- Traditionally development, test and production environments were strictly separated
  - Developers worked in a dedicated environment and handed completed code over to testers
  - Testers work in a separate environment and perform unit, functional and end-to-end testing
  - Tested and built code is handed over to Operations staff who deploy in pre-production environment to perform deployment and integration testing before signing release off
  - Released code is deployed into production environment by Operations staff
- Developers and testers do not have access to production environment

Modern Approach: DevOps

- Often leveraged in conjunction with Agile Development, Developer Operations (DevOps) is just what it sounds like
  - Developers are responsible for development and operations management of their software
  - Separation between environments can be eroded: code is developed, tested and deployed in production environment
- Rationale behind DevOps is that developers can quickly roll out new features and fix problems as they are discovered
  - Cited as critical market advantage in highly competitive industries such as Search, Social Media, Collaboration, etc.
  - Gaining adoption in traditional business environments, too

DevOps Security Challenge

- PCI DSS v3
  - **6.4.1** Separate development/test environments from production environments, and enforce the separation with access controls.
  - **6.4.2** Separation of duties between development/test and production environments
- ISO/IEC 27002:2005
  - 10.1.4 Separation of development, test, and operational facilities
    - Control: Development, test, and operational facilities should be separated to reduce the risks of unauthorised access or changes to the operational system.

Contact

- For more information, please contact John Howie at:

jhowie@cloudsecurityalliance.org