Healthcare and the Cloud:

Pros & Cons of Security and Privacy

Information Systems Security Association (ISSA) Healthcare SIG

and

Cloud Security Alliance (CSA)

March 16, 2017

Peer Networking
Education & Training
Career Opportunity and Growth
Industry Tools & Resources
Special Offers & Discounts
Insight Into Best Practices

ISSA
Information Systems Security Association

CSA cloud security alliance®

Vince Campitelli
Enterprise Security Specialist
Cloud Security Alliance
c-vcampitelli@cloudsecurityalliance.org

Andy Reeder, CISSP, CISA, CHPC
HIPAA Security Officer
Director, HIPAA Privacy
Rush University Medical Center
Chair, ISSA Healthcare SIG

Webinar Contributors

Dr. James L. Angle
Regional Information Security Manager
Trinity Health

Grant Johnson, CISSP, CISM
Principal and IT Security Consultant
Array Information Technologies, Inc.

Gary Long, CISSP, CISA
Principal Consultant
Long Professional Services

David Presuhn
Sr. Systems Administrator – Connected Device Management
Boston Scientific

Matthew Sharp
CISO
Logicworks

Agenda

- ❑ About the Information Systems Security Association (ISSA)
- ❑ Cloud Adoption in the Healthcare Industry
- ❑ About the Cloud Security Alliance (CSA)
    - ❑ Organization
    - ❑ Membership
    - ❑ Research
    - ❑ Working Groups
    - ❑ Education/Training/Certification
    - ❑ Incident Sharing
    - ❑ Tools and Products
- ❑ Resource Links
- ❑ Questions

ISSA

Information Systems Security Association

Mission Statement

ISSA is a non-profit organization for the information security profession committed to promoting effective cyber security on a global basis.

a) Being a respected forum for networking and collaboration

b) Providing education and knowledge sharing at all career lifecycle stages

c) Being a highly regarded voice of information security that influences public opinion, government legislation, education and technology with objective expertise that supports sound decision-making”

ISSA
Information Systems Security Association

FACTS

- ❑ Founded in 1984.
- ❑ 11,000 members from across the globe.
- ❑ 140 local chapters in 70 countries.
- ❑ Governed by a member elected Board of 13.

ISSA

Information Systems Security Association

Healthcare Special Interest Group (SIG)

Vision: Establish and maintain collaborative models for information security within healthcare organizations.

Mission: Drive collaborative thought and knowledge-sharing for information security leaders within healthcare organizations.

❑ ISSA membership not required to join; no additional cost or requirement.
❑ Over 475+ members from across the globe.
❑ Secure website provides: Group Directory, Event Calendar, Blogs, Forums, and Photo Gallery.

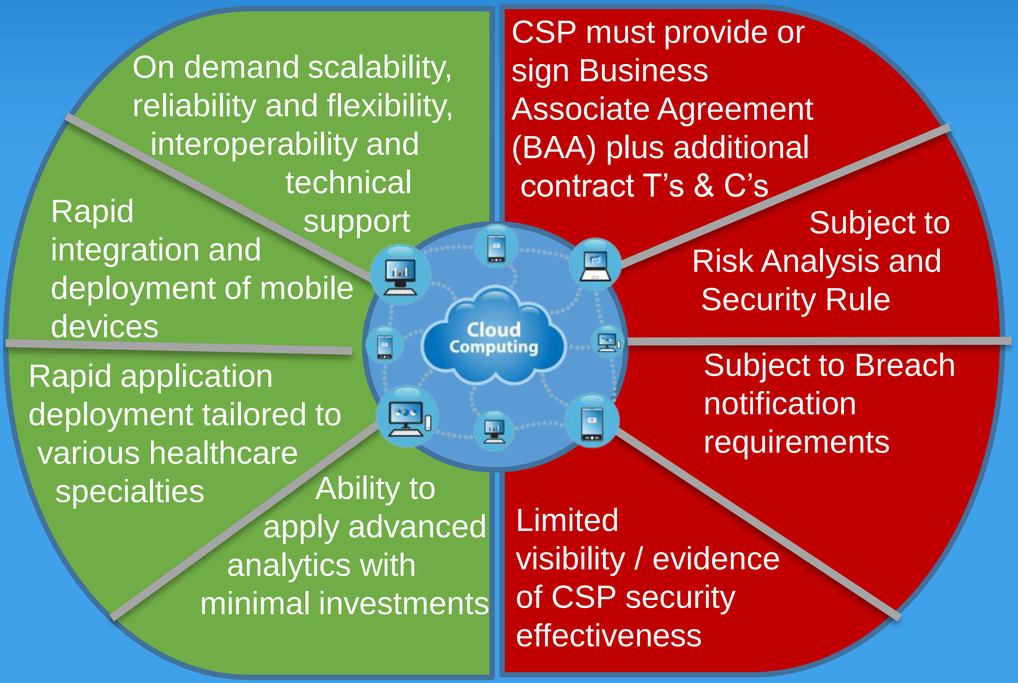
Prognosis for Healthcare & Cloud Adoption

- ❑ **89%** of healthcare organizations (HCO's) are deploying cloud technologies
- ❑ **45%** of HCO's are utilizing (6 – 10) cloud services
- ❑ **Most popular services** – email, patient care, file/data sharing
- ❑ 58% of non-users project cloud adoption in next 2 years
- ❑ **Key drivers** – productivity gains, cost savings, reduced reliance on legacy IT, increased confidence in CSP provided security
- ❑ **Key inhibitors** – data leakage, consistency, integration and relocation
- ❑ **Market leaders** - AWS, Microsoft, Carecloud, ClearData Networks, Oracle Corporation and IBM

Healthcare in the Cloud

Pros

Cons



On demand scalability, reliability and flexibility, interoperability and technical support

Rapid integration and deployment of mobile devices

Rapid application deployment tailored to various healthcare specialties

Ability to apply advanced analytics with minimal investments

CSP must provide or sign Business Associate Agreement (BAA) plus additional contract T's & C's

Subject to Risk Analysis and Security Rule

Subject to Breach notification requirements

Limited visibility / evidence of CSP security effectiveness

HIPAA/HITECH and Cloud Considerations

“**Covered Entity Responsibilities.** If a covered entity knows of an activity or practice of the business associate that constitutes a material breach or violation of the business associate’s obligation, the covered entity must take reasonable steps to cure the breach or end the violation. Violations include the failure to implement safeguards that reasonably and appropriately protect e-PHI.” (**HHS Website**)

❑ Cloud providers with access to a Covered Entities (CE) ePHI are considered Business Associates (BA) and a Business Associate Agreement (BAA) is required.

❑ A breach of ePHI must be reported by the BA to the CE; the CE is required to notify the Office of Civil Rights (OCR) of Reportable Breaches.

CSA cloud security alliance®

❑ Who We Are

❑ What We Do

❑ How We Can Help

CSA – At A Glance

- ❑ Founded in 2009
- ❑ Headquarters in Seattle (Bellingham), Singapore, Edinburgh UK
  - ❑85,000+ Individual members
  - ❑300+ Corporate members
  - ❑75 Chapters
- ❑ Over 30 research projects in 25 working groups
- ❑ Strategic partnerships with governments, research institutions, professional associations and industry
- ❑ CSA Research is FREE!

CSA – Fast Facts

- □ Global, not-for-profit organization
- □ Building security best practices for next generation IT
- □ Research and Educational Programs
- □ Cloud Provider Certification – CSA STAR
- □ User Certification - CCSK
- □ 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 - Membership

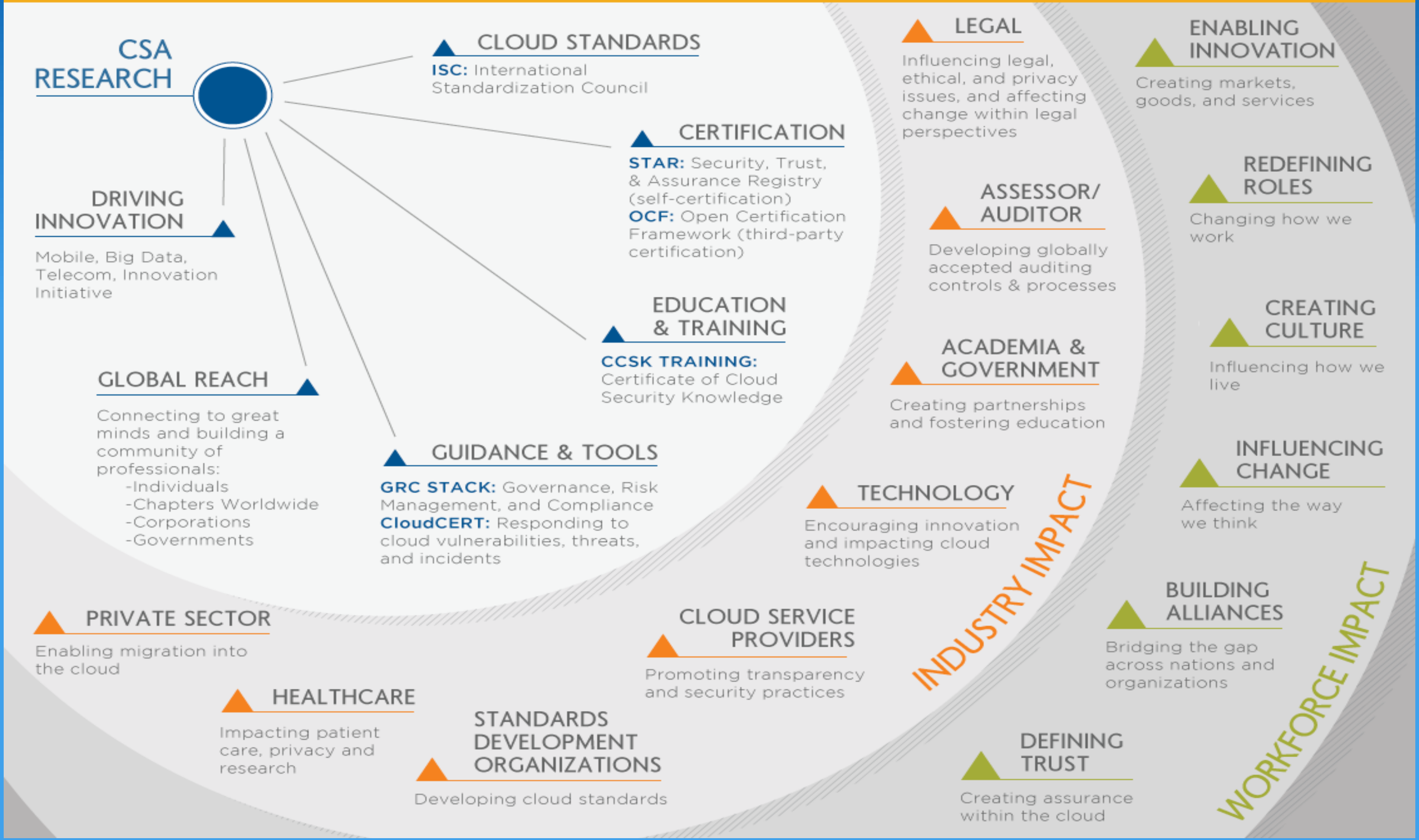
- ❑ **Individuals**
- ❑ **Chapters**
- ❑ **Affiliates**
- ❑ **Corporations**
  - ❑ Solution Provider Member
  - ❑ Enterprise Customer

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.

Active Working Groups

- □ Cloud Controls Matrix / Consensus Assessment Questionnaire
- □ Quantum Safe Security
- □ Big data
- □ Security as a Service
- □ Containers and Microservices
- □ Mobile Application Security Testing
- □ Cyber Incident Sharing Center
- □ Internet of Things (IOT)
- □ Software Defined Perimeter
- □ Security Guidance Group
- □ Healthcare Information Management Group (in the process of being reconstituted)

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)

DRIVING INNOVATION

Mobile, Big Data, Telecom, Innovation Initiative

EDUCATION & TRAINING

CCSK TRAINING: Certificate of Cloud Security Knowledge

GLOBAL REACH

Connecting to great minds and building a community of professionals:
-Individuals
-Chapters Worldwide
-Corporations
-Governments

GUIDANCE & TOOLS

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

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

PRIVATE SECTOR

Enabling migration into the cloud

HEALTHCARE

Impacting patient care, privacy and research

STANDARDS DEVELOPMENT ORGANIZATIONS

Developing cloud standards

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

Education / Training / Certification

- ❑ *Certificate of Cloud Security Knowledge (CCSK)*
  - ❑ Most valuable IT certification 2016 – Certification Magazine
  - ❑ Benchmark of cloud security competency
  - ❑ Based on CSA guidance
  - ❑ Online web-based examination
  - ❑ **www.cloudsecurityalliance.org/education/ccsk/**
  - ❑ Partnered with (ISC)2 to develop complementary certification: CCSP

Cloud CISC

- Cloud Cyber Incident Sharing Center
  - Creating standards for incident sharing & response in the cloud
  - Creating operational incident sharing capabilities
- Threat Intelligence Exchange in operation in partnership with TruStar
  - Anonymization of submission provides key capability to limit attribution
- Corporate members receive 2 complimentary seats
  - Please go to https://www.csa-cloudcisc.org/ to activate your licenses.

CSA’s Tools for Cloud Due Diligence

□ Cloud Controls Matrix (CCM)

□ Consensus Assessment Initiative Questionnaire (CAIQ)

□ STARWatch

□ CSA STAR (Security, Trust and Assurance Registry)

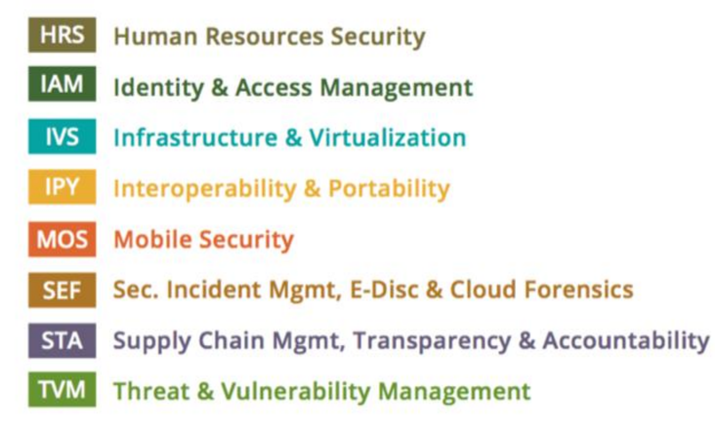
□ Future Innovations – Network integrations/Data Analysis/Intelligent mapping

Cloud Controls Matrix (CCM)

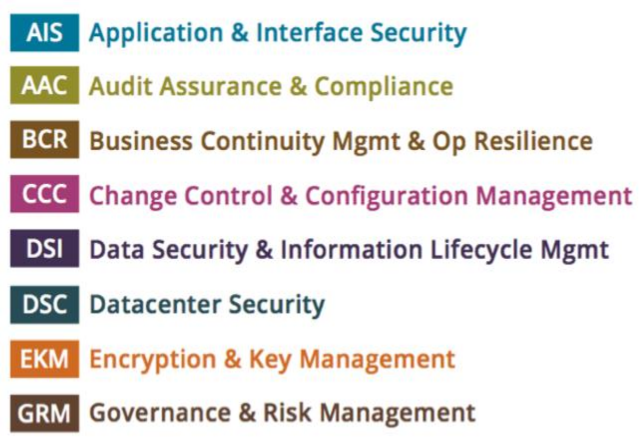
- Industry leading security controls framework for cloud
- First ever baseline control framework specifically designed for Cloud supply chain risk management:
  - Delineates control ownership (Provider, Customer)
  - Ranks applicability to cloud provider type (SaaS vs PaaS vs IaaS)
  - An anchor for security and compliance posture measurement
  - Provides a framework of 16 control domains
- Controls map to global regulations and security standards: e.g. NIST, ISO 27001, COBIT, PCI, HIPAA, FISMA, FedRAMP – mappings growing virally

Cloud Controls Matrix (CCM)

v3.01



HRS	Human Resources Security
IAM	Identity & Access Management
IVS	Infrastructure & Virtualization
IPY	Interoperability & Portability
MOS	Mobile Security
SEF	Sec. Incident Mgmt, E-Disc & Cloud Forensics
STA	Supply Chain Mgmt, Transparency & Accountability
TVM	Threat & Vulnerability Management



AIS	Application & Interface Security
AAC	Audit Assurance & Compliance
BCR	Business Continuity Mgmt & Op Resilience
CCC	Change Control & Configuration Management
DSI	Data Security & Information Lifecycle Mgmt
DSC	Datacenter Security
EKM	Encryption & Key Management
GRM	Governance & Risk Management

16 Domains

133 Controls

Consensus Assessment Initiative Questionnaire (CAIQ)

- Companion to CSA Cloud Controls Matrix (CCM)
- Series of Yes/No/NA questions used to assess compliance with CCM
    - Narrative may be included for each question to explain why the particular answer is given
- Helps organizations build assessment processes for cloud providers
- Helps cloud providers assess their own security posture

STARWatch

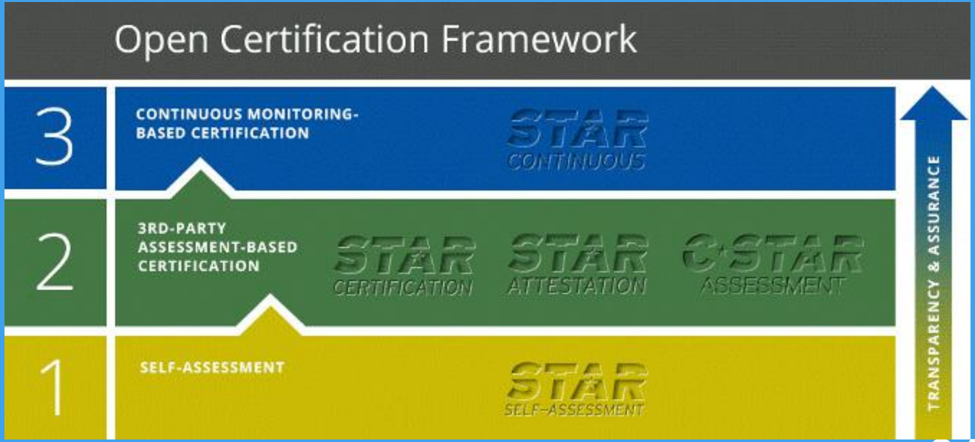
STARWATCH
Assurance on Demand

- CSA STARWatch: SaaS tool to help organizations manage compliance with CSA STAR requirements
  - Currently in Phase I of initial General Release
  - Multi-user access to CCM/CAIQ in a database format
  - Corporate members get a three user license for free
  - https://beta.cloudsecurityalliance.org/en/starwatch
  - Group Demos every Tuesday @ 11am PST register:
    - https://attendee.gotowebinar.com/rt/2646240094069663490

Contact membership@cloudsecurityalliance.org to get your activation code today!

CSA STAR Provider Program

- CSA STAR (Security, Trust and Assurance Registry), 3 Level Provider Certification Program
- Managed by CSA in partnership with world leading ISO certification bodies and audit firms
- Adopted Worldwide by Providers, Enterprises and Governments
- Promotes Transparency within Cloud Ecosystem



Open Certification Framework

3 CONTINUOUS MONITORING-BASED CERTIFICATION — STAR CONTINUOUS

2 3RD-PARTY ASSESSMENT-BASED CERTIFICATION — STAR CERTIFICATION, STAR ATTESTATION, C-STAR ASSESSMENT

1 SELF-ASSESSMENT — STAR SELF-ASSESSMENT

TRANSPARENCY & ASSURANCE

Resource Links

- **ISSA**
  - Home Page: www.ISSA.org
  - Healthcare SIG: www.issa.org/?page=SIGs
- **CSA**
  - Home Page: https://cloudsecurityalliance.org/
  - Membership: https://cloudsecurityalliance.org/membership/
- **Health and Human Services (HHS)**
  - Guidance on HIPAA & Cloud Computing: https://www.hhs.gov/hipaa/for-professionals/special-topics/cloud-computing/index.html
- **National Institute of Standards and Technology (NIST)**
  - The NIST Definition of Cloud Computing: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

Webinar Summary

- **Statistics Illustrate that Cloud Adaptation in the Healthcare Industry is Already Strong and is Trending Higher**
- **The “PROS” of Cloud Computing in Healthcare include:**
  - On demand scalability, reliability and flexibility, interoperability and technical support
  - Rapid integration and deployment of mobile devices
  - Rapid application deployment tailored to various healthcare specialties
  - Ability to apply advanced analytics with minimal investments
- **Covered Entities HIPAA Security Rule Challenges include:**
  - Securing a BAA from the Cloud Provider
  - Receiving Attestation of Compliance from the Cloud Provider
  - Achieving Proper Oversight of the Cloud Provider to Ensure there are not Material Breaches or Violations
  - Investigating Potential Material Breaches or Violations Discovered by the Covered Entity or Reported by the Cloud Provider
- **The Cloud Security Alliance (CSA) has a Strong Portfolio of Security Offerings to Assist Individuals and Organizations**

ISSA Information Systems Security Association

CSA cloud security alliance®