cloud security alliance®

STAR™ Security, Trust, Assurance & Risk Registry

Intro to STAR and CCM

Linda Strick,

Managing Director EMEA,
Cloud Security Alliance

182,000+

MEMBER COMMUNITY

100+

CHAPTERS

500+

CORPORATE MEMBERS

26+

ACTIVE WORKING GROUPS

65,000+

SUBSCRIBERS TO OUR WEBINAR SERIES

14,000+

RESEARCH VOLUNTEERS CONTRIBUTING

Strategic partnerships with governments, research institutions, professional associations and industry

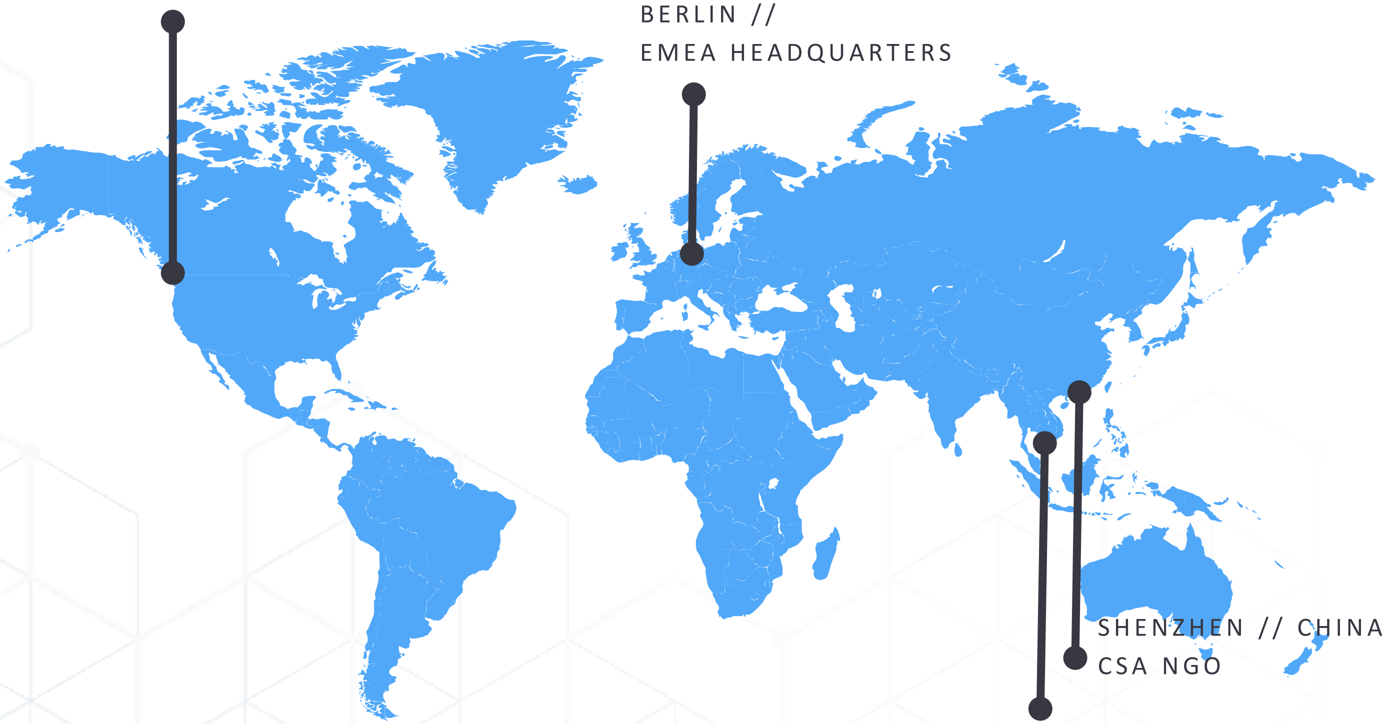
CSA research is FREE!

CSA

OUR COMMUNITY

2009

CSA FOUNDED



SEATTLE/BELLINGHAM, WA // US HEADQUARTERS

BERLIN // EMEA HEADQUARTERS

SHENZHEN // CHINA CSA NGO

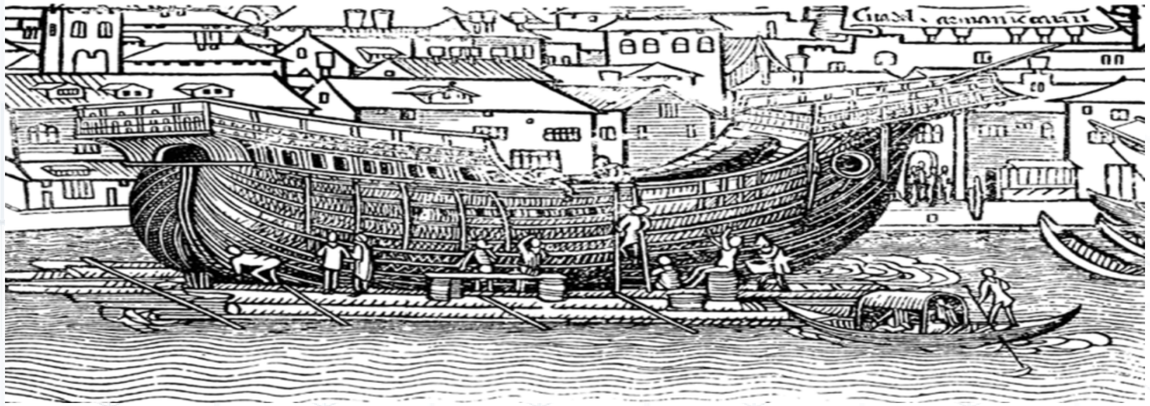
SINGAPORE // ASIA PACIFIC HEADQUARTERS

Problem Statement

- Like many of the surveys, CSA identified gaps within the IT ecosystem that were inhibiting market adoption of secure and reliable cloud services.
- Consumers did not have simple, cost-effective ways to evaluate and compare their providers' resilience, data protection capabilities and service portability.
- CSA recognized that no single certification, regulation or other compliance regime will supplant all others in governing the future of IT as well as the risk of adding more cost and complexity to the already overloaded compliance landscape.
- However, the rise of cloud as a global compute utility creates a mandate to better harmonize compliance concerns and ensure customer focus.

This gap of trust mainly lies down in the difficulties of cloud users in addressing fundamental assurance issues with cloud providers, such as:

- Understanding legal compliance and contractual liabilities,
- Defining and allocating responsibilities
- Enforcing accountability
- Translating requirements into cloud language/controls/checks
- Identifying means for an ex-ante analysis assessment of cloud services and for a continuous monitoring of cloud service contract execution



STAR – World's Cloud Assurance Program

- STAR = Security, Trust, Assurance & Risk
- Launched in 2011, over 2,000 registered services
- Program Pillars
  - Cloud Controls Matrix (CCM) - base control framework and questionnaire
  - STAR Assessment Portfolio - Self Assessment & 3rd Party ISO & SOC based audits
  - STAR Registry - Extensible API-enabled Repository for storing, searching and retrieving assessment information
  - STAR Enabled Partners – Consultants, Auditors & Technology partners (licensees of CCM & STAR API to allow continuous monitoring and other assurance capabilities)
  - STAR Extended – Custom program to extend STAR to other assurance ecosystems and map against other control frameworks (countries & industries)
  - Assurance Education – CCAK, STAR Auditor

CCM™
Cloud Controls Matrix

What's the CCM

- The de-facto standard Cloud Security Framework:10 years supporting CSP, Customers, Auditors, Assurance Providers in building and improving GRC Programs
- Community-driven research
- The Lingua Franca between cloud actors
- Simplifies approach to cloud security implementation, assessment and compliance
- Delineates Security Shared Responsivity Model (SSRM)
- Aligned & mapped to global regulations and most relevant security frameworks
- Valued and adopted by Government, Regulators in the National Cloud Security Program
- Creating Extension for National and Sector Specific Requirements
- Backbone of CSA STAR Program, to assess and compare cloud services

CCM™
Cloud Controls Matrix

Cloud Controls Matrix V4 Structure

A&A	Audit and Assurance
AIS	Application & Interface Security
BCR	Business Continuity Mgmt & Op Resilience
CCC	Change Control and Configuration Management
CEK	Cryptography, Encryption and Key Management
DCS	Datacenter Security
DSP	Data Security and Privacy
GRC	Governance, Risk Management and Compliance
HRS	Human Resources Security
IAM	Identity & Access Management
IPY	Interoperability & Portability
IVS	Infrastructure & Virtualization Security
LOG	Logging and Monitoring
SEF	Sec. Incident Mgmt, E-Disc & Cloud Forensics
STA	Supply Chain Mgmt, Transparency & Accountability
TVM	Threat & Vulnerability Management
UEM	Universal EndPoint Management

Why, What and How

Composed of:

- 17 security domains
- 197 controls

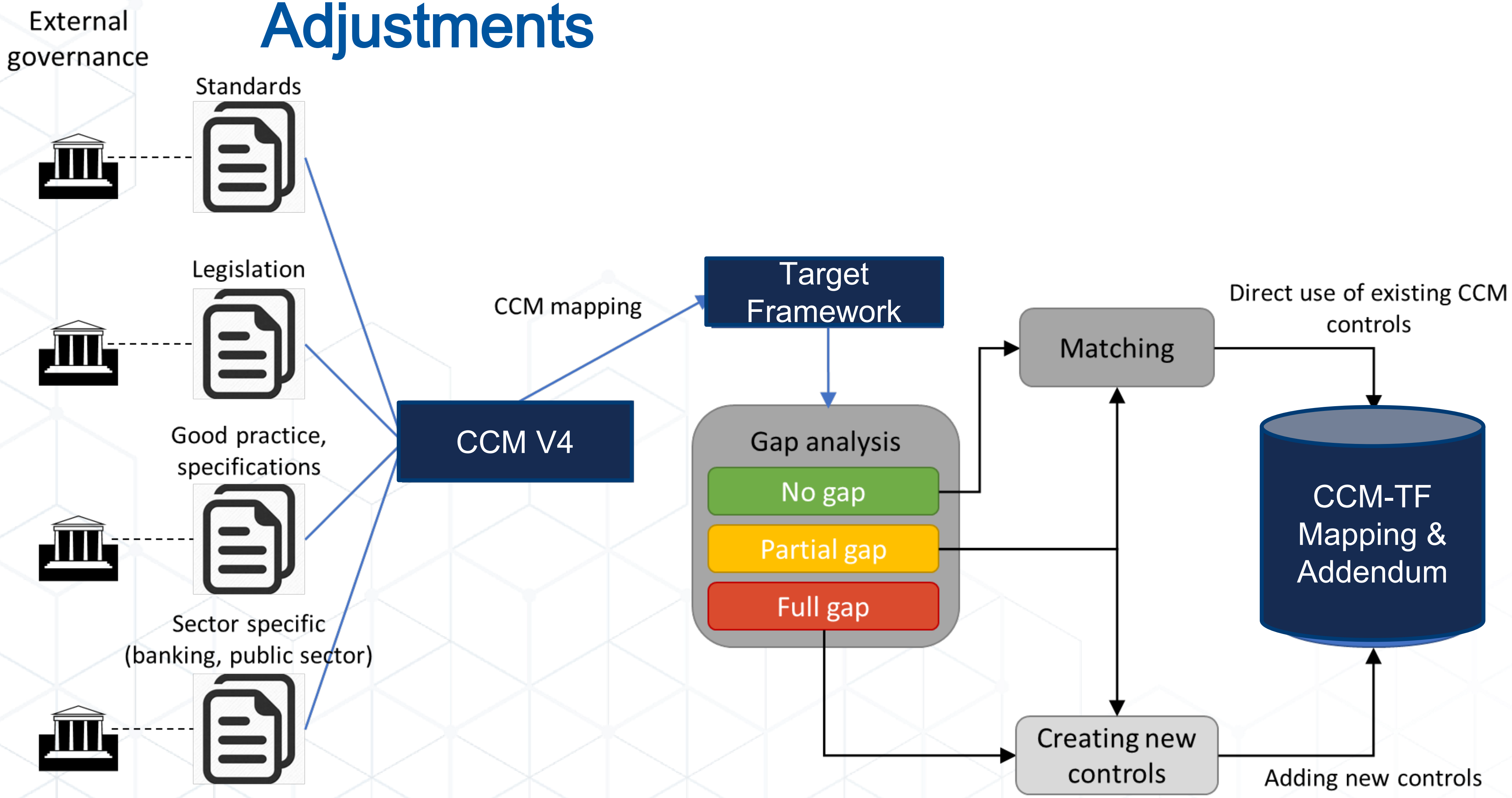
Encompasses:

- Control Applicability and Ownership
- Architectural relevance Cloud Stack Components
- Organizational Relevance

cloud security alliance®

STAR™ Security, Trust, Assurance & Risk Registry

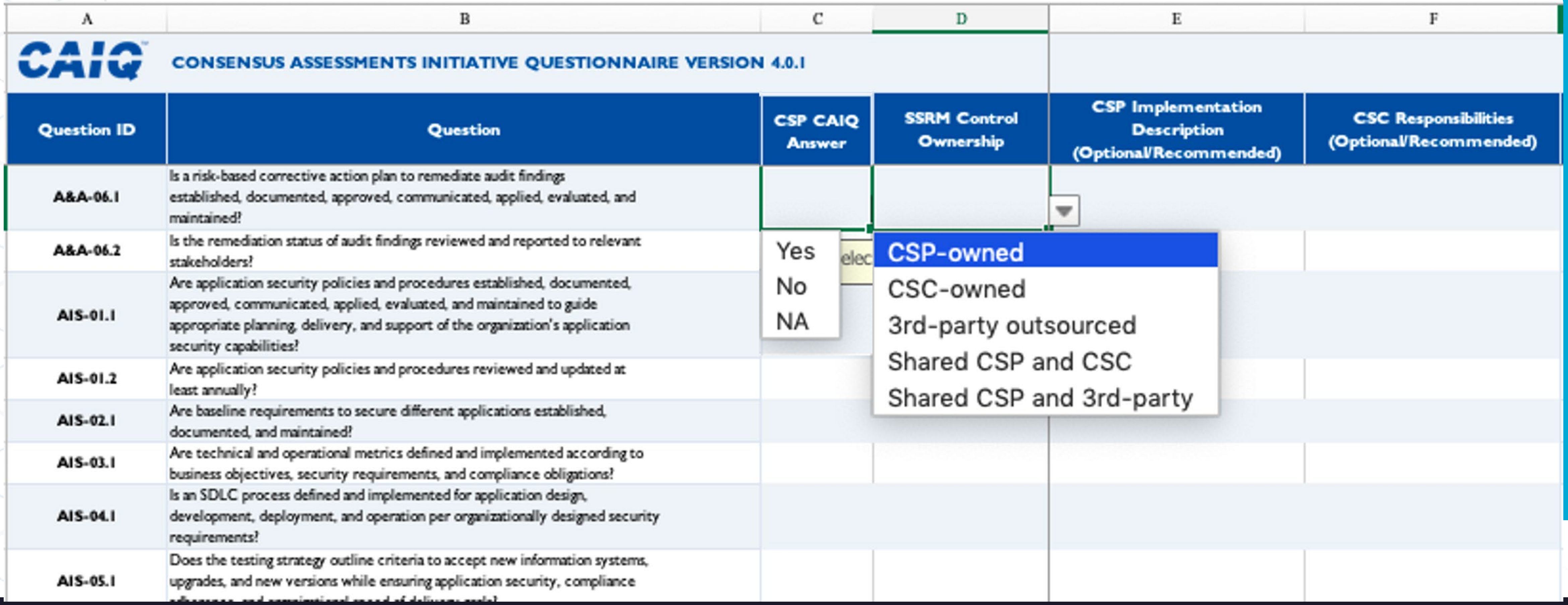
Adjustments



CAIQ™

- It includes a total of 261 questions (compared to 310 of v3.1)
- It helps cloud customers/auditors gauge the security posture of CSPs and determine if their cloud services are suitably secure
- CAIQ questions are tailored to the control specifications of the CCM
- The new structure of CAIQv4 includes new columns related to the Shared Security Responsibility Model (SSRM)

CSP Self-Assessment Columns



CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE VERSION 4.0.1

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)
A&A-06.1	Is a risk-based corrective action plan to remediate audit findings established, documented, approved, communicated, applied, evaluated, and maintained?				
A&A-06.2	Is the remediation status of audit findings reviewed and reported to relevant stakeholders?				
AIS-01.1	Are application security policies and procedures established, documented, approved, communicated, applied, evaluated, and maintained to guide appropriate planning, delivery, and support of the organization's application security capabilities?				
AIS-01.2	Are application security policies and procedures reviewed and updated at least annually?				
AIS-02.1	Are baseline requirements to secure different applications established, documented, and maintained?				
AIS-03.1	Are technical and operational metrics defined and implemented according to business objectives, security requirements, and compliance obligations?				
AIS-04.1	Is an SDLC process defined and implemented for application design, development, deployment, and operation per organizationally designed security requirements?				
AIS-05.1	Does the testing strategy outline criteria to accept new information systems, upgrades, and new versions while ensuring application security, compliance adherence, and organizational speed of delivery goals?				

Summary - Why add CSA STAR to your security systems ?

- Reduce risk
- Be consistent within the organization.
- Avoid conflicting objectives
- Improve internal and external communications.
- Avoid duplication and gain cost savings
- Identify and resolve conflicting responsibilities and relationships
- Gain a structured balance of authority, and accountability
- Focus organization onto business goals
- Absorb informal systems into formal systems
- Harmonize and optimize practices
- Optimize staff training and development

What’s next

How STAR/CCM help with Continuous Assurance

- **Controls Objectives** : Let’s get on the same page at conceptual level (CCM control objectives)
- **Mappings and Gap Analysis** : Let’s understand the connections across difference frameworks
- **Implementation, Auditing and Shared Security Resp. Model Guidelines** : Let’s support implementation and clarify the responsibilities allocation
- **Technical Controls** : Let’s tailor the control objective into the specific domain of applicability (not yet part of the CCM, currently under development, even via the integration of Securosis’ work)
- **Metrics** : Let’s measure objectively the effectiveness and efficiency of a control
- **Addenda** : Let’s extended the scope of CCM/STAR by adding controls as results of Industries/Countries specific requirements
- **Machine readable** : Let’s enable automation (CCM is available in JSON and YAML)
- **OSCAL** : Let’s speak a language we can all understand and foster interoperability (CCM available in OSCAL)
- **Automation and Tool** : Let’s support continuous assurance at scale (Several tools embed CCM controls)
- **Certification and Attestation** : Let’s agree on a repeatable and certifiable approach to measure assurance

Final thoughts

- Continuous Assurance is the result of the process of defining control, establishing metrics to measure their efficiency and effectiveness, monitoring and auditing, and reporting/communicating results and evidence.
- Continuous Assurance needs to be based on agreed-upon standards
- Organizations need:
  - Understanding the details beyond Security Control Objectives
  - Metrics to quantify and report risk
- Risk Quantification supports:
  - Zero Trust based Cyber Security Deployment and Operation
  - Risk Management (e.g., Risk Transfer/Cyber-Insurance),
  - Governance and Corporate Responsibility (e.g., reports to the Board and Regulators).
- Continuous Assurance requires automation
- There is a need and space for better standards and solutions for Continuous Assurance
- AI will help along the way

Helpful Links & Resources

- CSA STAR Program Website
- Visit the STAR Registry
- Download the Cloud Controls Matrix (CCM) and Consensus Assessment Initiative (CAIQ)
- Get Involved in our CSA Research Community
- Support us through Corporate Membership

Linda Strick, Managing Director EMEA

E-mail: lstrick@cloudsecurityalliance.org

https://cloudsecurityalliance.org/