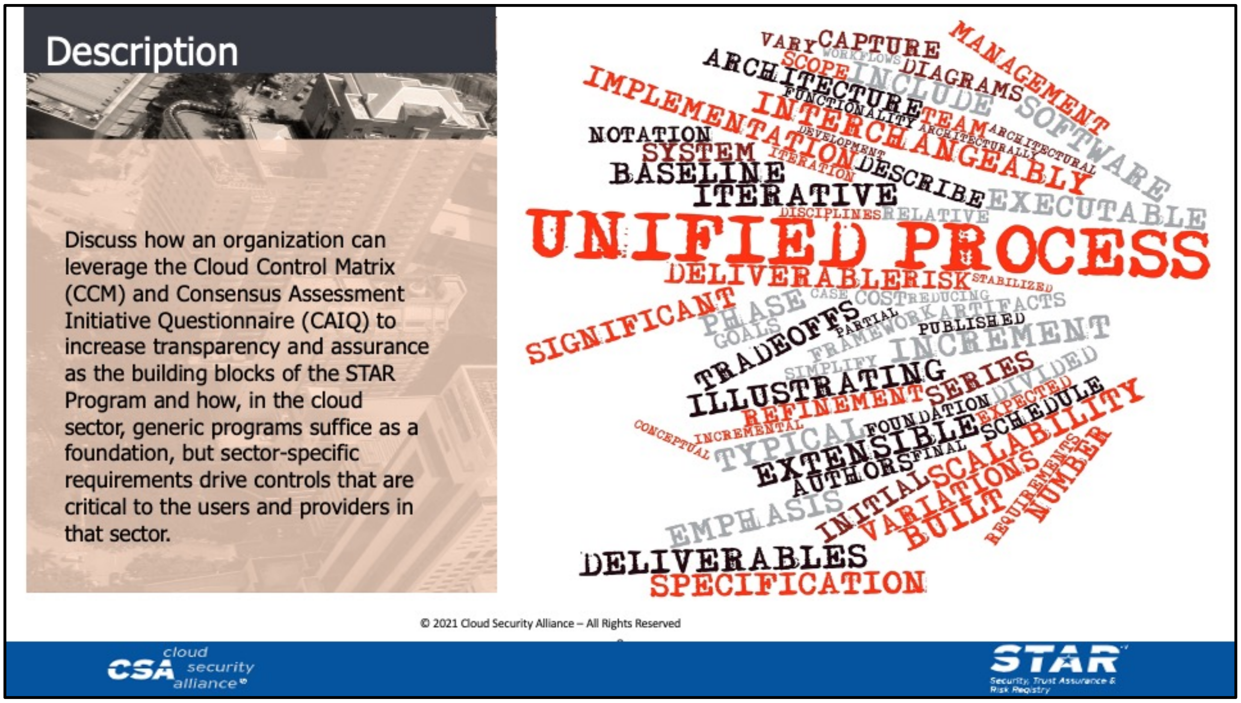
STAR™

Security, Trust, Assurance &
Risk Registry

Leveraging the CAIQ and CCM

PRESENTED BY

John DiMaria; CSSBB, HISP, MHISP, AMBCI, CERP
Assurance Investigatory Fellow; CSA



Description

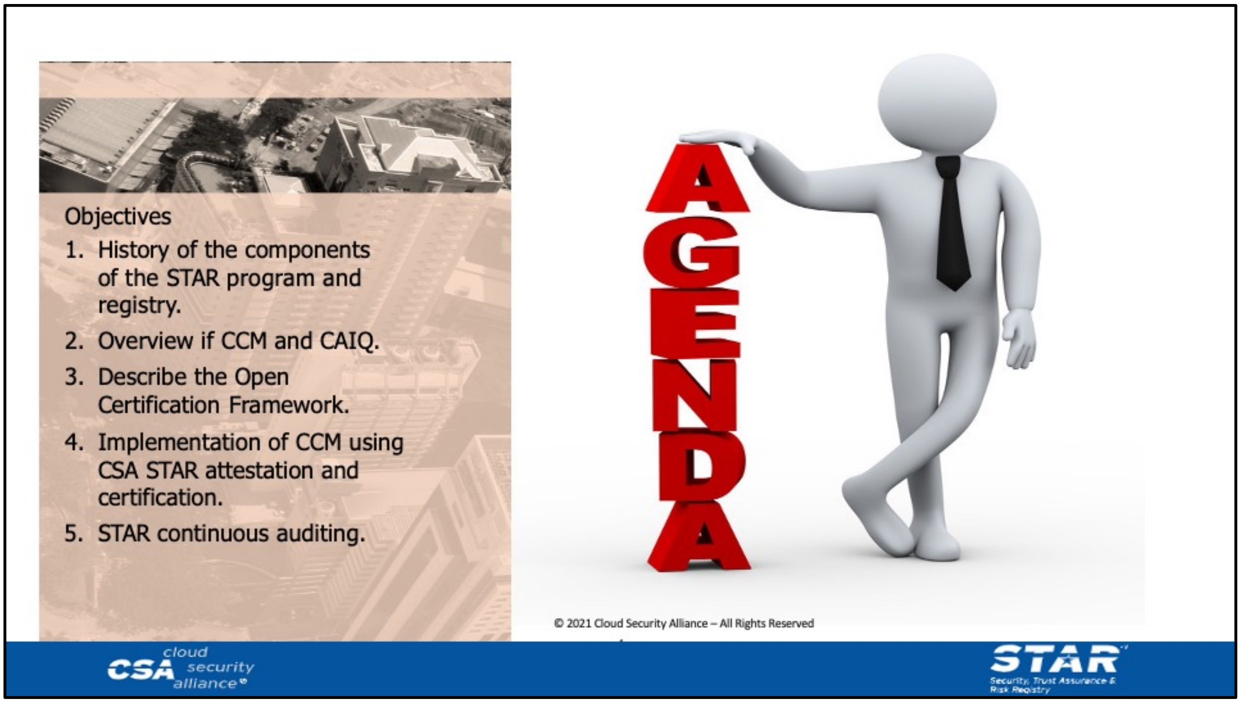
Discuss how an organization can leverage the Cloud Control Matrix (CCM) and Consensus Assessment Initiative Questionnaire (CAIQ) to increase transparency and assurance as the building blocks of the STAR Program and how, in the cloud sector, generic programs suffice as a foundation, but sector-specific requirements drive controls that are critical to the users and providers in that sector.

© 2021 Cloud Security Alliance – All Rights Reserved

CSA cloud security alliance®

STAR Security, Trust Assurance & Risk Registry

I am going to take you on a journey that will allow you to see how organizations leverage the Cloud Control Matrix (CCM) and Consensus Assessment Initiative Questionnaire (CAIQ) to increase transparency and assurance as the building blocks of an integrated holistic ISMS



Objectives

1. History of the components of the STAR program and registry.
2. Overview if CCM and CAIQ.
3. Describe the Open Certification Framework.
4. Implementation of CCM using CSA STAR attestation and certification.
5. STAR continuous auditing.

CSA cloud security alliance®
STAR Security, Trust Assurance & Risk Registry

Proliferation of compliance schemes

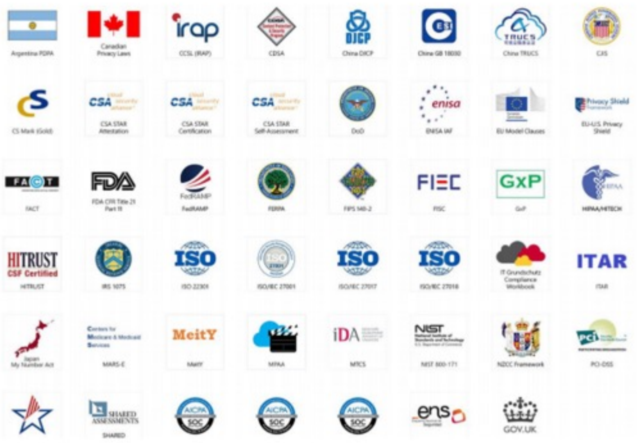
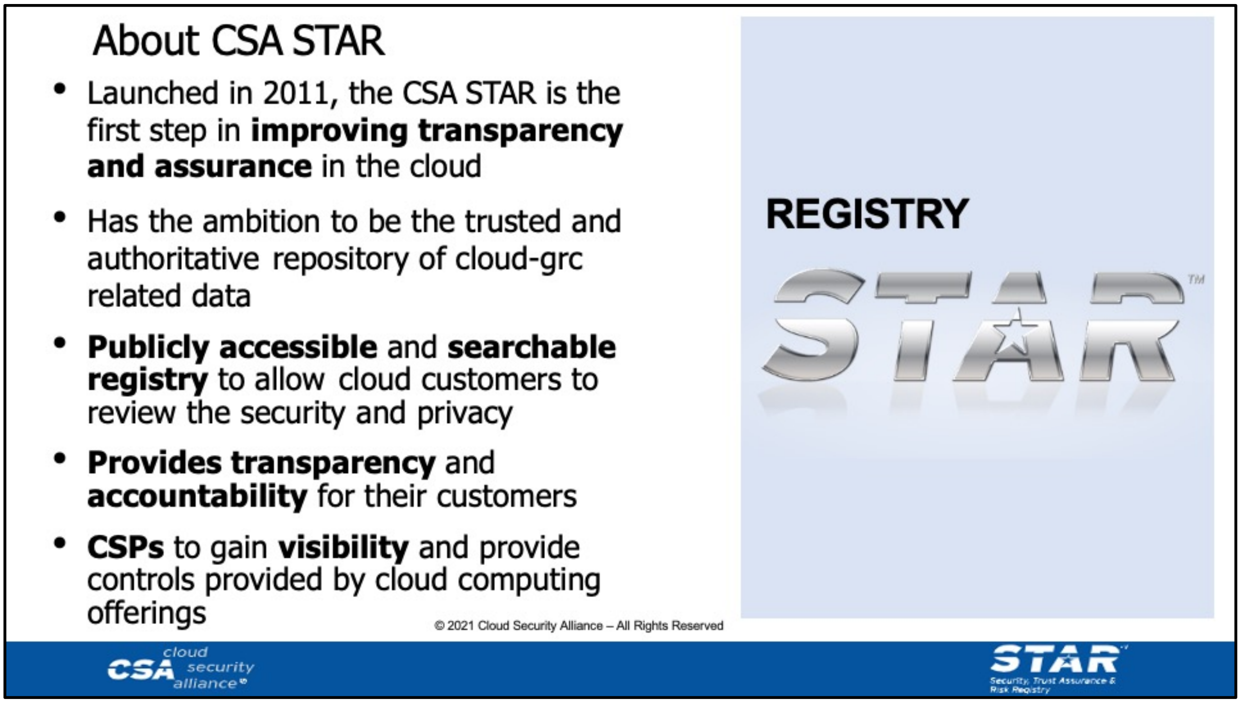


Fig1. Compliance Templates Provided By Microsoft



About CSA STAR

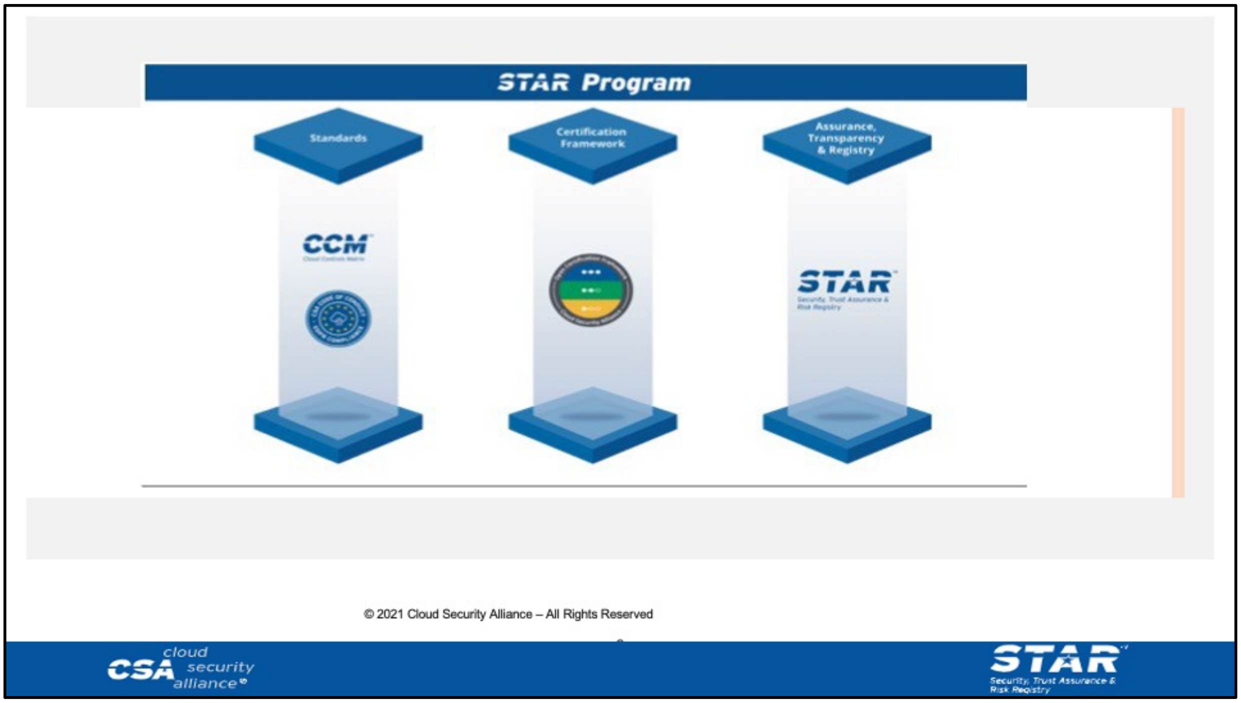
- Launched in 2011, the CSA STAR is the first step in **improving transparency and assurance** in the cloud
- Has the ambition to be the trusted and authoritative repository of cloud-grc related data
- **Publicly accessible** and **searchable registry** to allow cloud customers to review the security and privacy
- **Provides transparency** and **accountability** for their customers
- **CSPs** to gain **visibility** and provide controls provided by cloud computing offerings

REGISTRY

STAR™

CSA cloud security alliance®

STAR Security, Trust Assurance & Risk Registry



STAR Program

Standards

Certification Framework

Assurance, Transparency & Registry

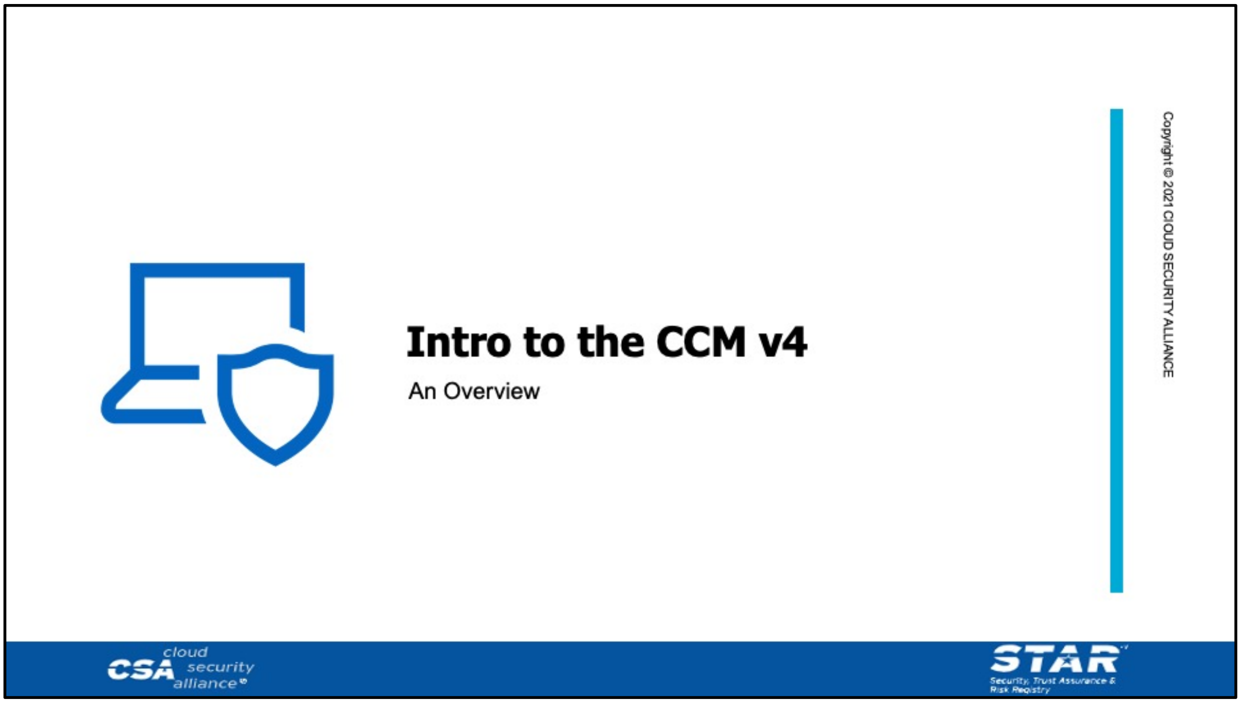
CCM
Cloud Controls Matrix
STAR
Security, Trust Assurance & Risk Registry

CSA cloud security alliance
STAR
Security, Trust Assurance & Risk Registry

The STAR Program is based on 3 pillars:

1. Technical standard and best practices (CCM is a IOCM approach to IS) Managing all frameworks under one roof and but one holistic process.
2. An Certification framework
3. A public repository and database

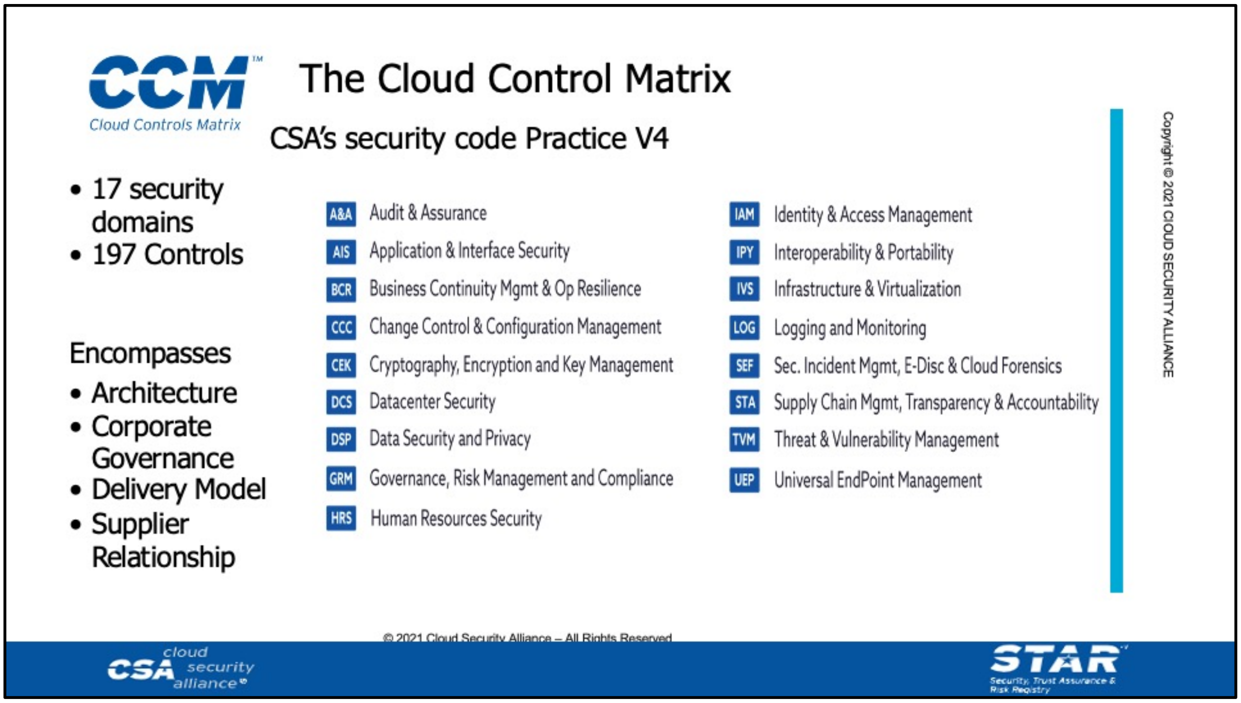
Each of the STAR pillars offer to organization tools to establish and maintain an effective and efficient cloud security and privacy governance and compliance posture.



Intro to the CCM v4

An Overview

CSA cloud security alliance
STAR
Security, Trust Assurance & Risk Registry



CCM
Cloud Controls Matrix

The Cloud Control Matrix

CSA's security code Practice V4

- 17 security domains
- 197 Controls

Encompasses

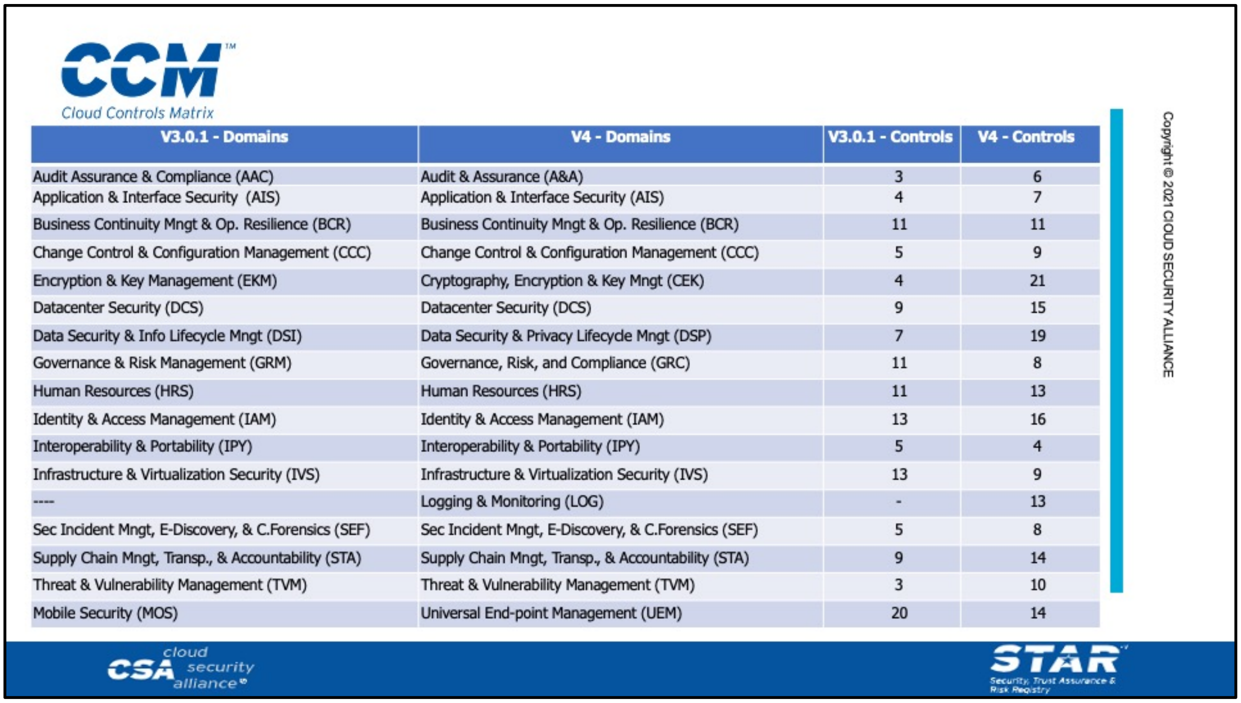
- Architecture
- Corporate Governance
- Delivery Model
- Supplier Relationship

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

CSA cloud security alliance

STAR Security, Trust Assurance & Risk Registry

- Backbone of CSA STAR to assess & compare cloud service providers (CSPs)
- Research driven by cloud customers, providers, & assurance professionals
- Simplifies approach to implementation, validation, & compliance across all clouds
- Delineates control owners aligned to a shared responsibilities model for providers & consumers (SSRM)
- Provides per control service delivery model applicability for SaaS, PaaS, & IaaS
- Aligned & mapped to global regulations and the most relevant security frameworks

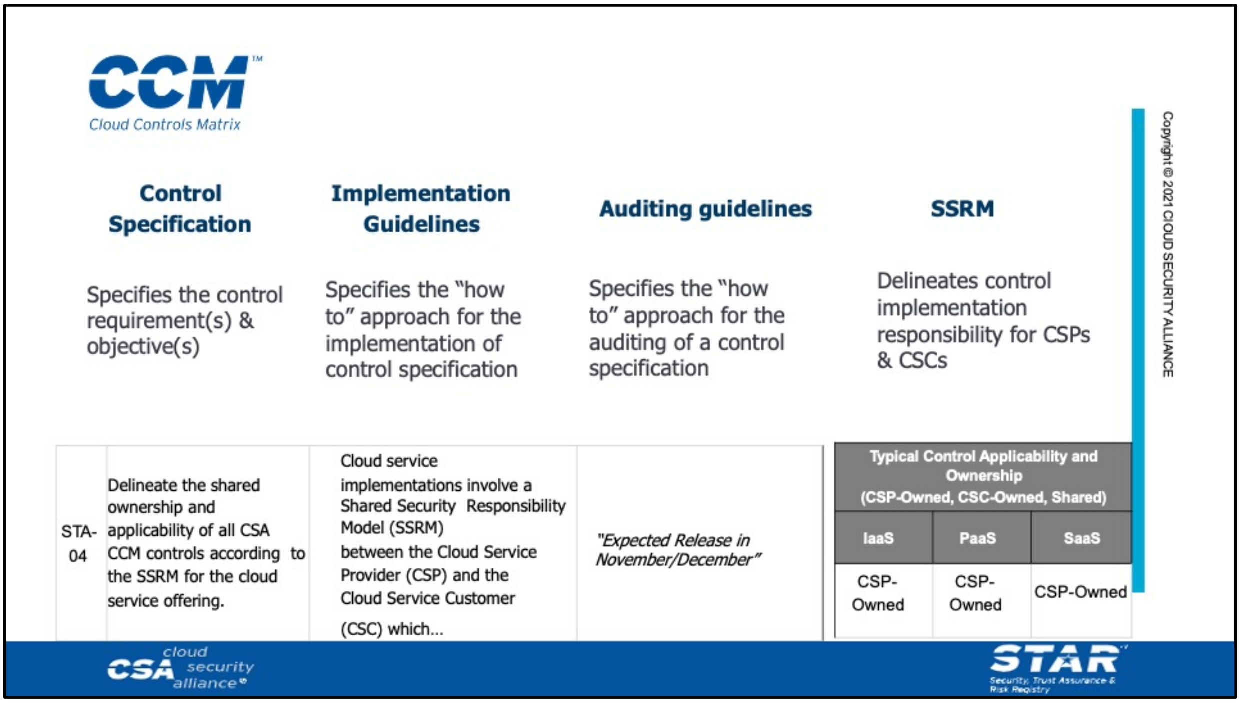


CCM™
Cloud Controls Matrix

V3.0.1 - Domains	V4 - Domains	V3.0.1 - Controls	V4 - Controls
Audit Assurance & Compliance (AAC)	Audit & Assurance (A&A)	3	6
Application & Interface Security (AIS)	Application & Interface Security (AIS)	4	7
Business Continuity Mngt & Op. Resilience (BCR)	Business Continuity Mngt & Op. Resilience (BCR)	11	11
Change Control & Configuration Management (CCC)	Change Control & Configuration Management (CCC)	5	9
Encryption & Key Management (EKM)	Cryptography, Encryption & Key Mngt (CEK)	4	21
Datacenter Security (DCS)	Datacenter Security (DCS)	9	15
Data Security & Info Lifecycle Mngt (DSI)	Data Security & Privacy Lifecycle Mngt (DSP)	7	19
Governance & Risk Management (GRM)	Governance, Risk, and Compliance (GRC)	11	8
Human Resources (HRS)	Human Resources (HRS)	11	13
Identity & Access Management (IAM)	Identity & Access Management (IAM)	13	16
Interoperability & Portability (IPY)	Interoperability & Portability (IPY)	5	4
Infrastructure & Virtualization Security (IVS)	Infrastructure & Virtualization Security (IVS)	13	9
----	Logging & Monitoring (LOG)	-	13
Sec Incident Mngt, E-Discovery, & C.Forensics (SEF)	Sec Incident Mngt, E-Discovery, & C.Forensics (SEF)	5	8
Supply Chain Mngt, Transp., & Accountability (STA)	Supply Chain Mngt, Transp., & Accountability (STA)	9	14
Threat & Vulnerability Management (TVM)	Threat & Vulnerability Management (TVM)	3	10
Mobile Security (MOS)	Universal End-point Management (UEM)	20	14

CSA cloud security alliance®

STAR Security, Trust Assurance & Risk Registry



CCM™
Cloud Controls Matrix

Control Specification

Specifies the control requirement(s) & objective(s)

Implementation Guidelines

Specifies the "how to" approach for the implementation of control specification

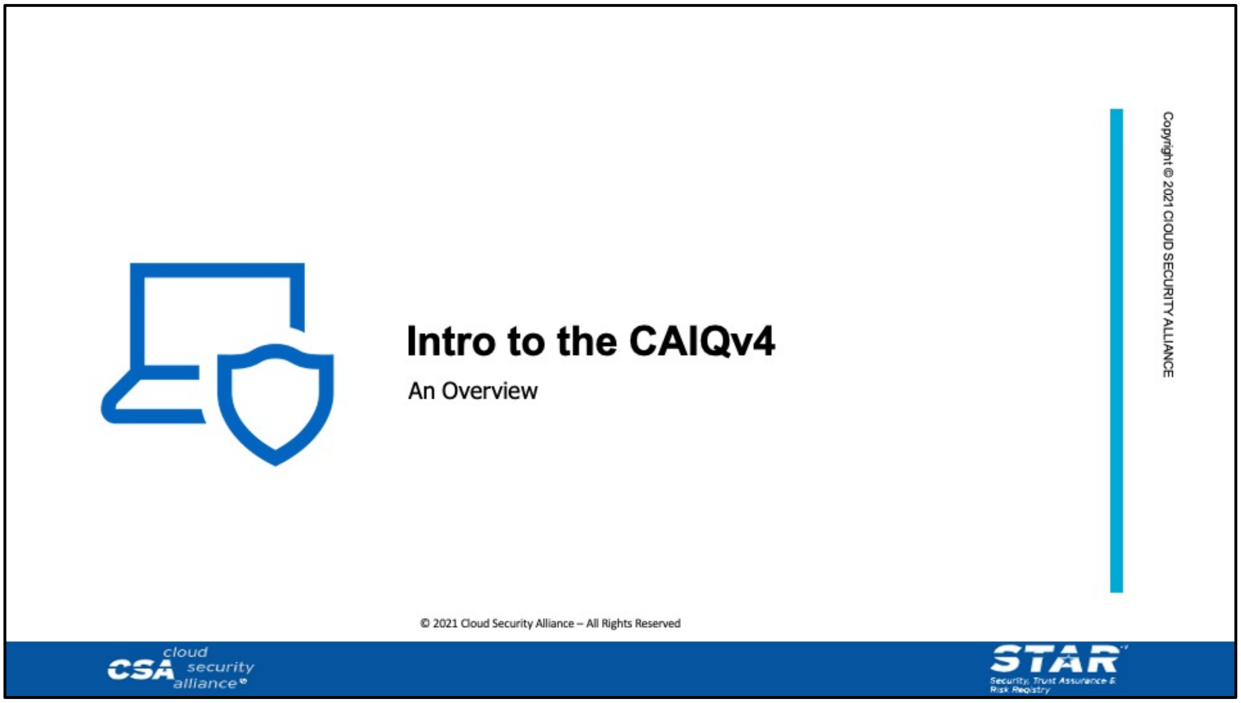
Auditing guidelines

Specifies the "how to" approach for the auditing of a control specification

SSRM

Delineates control implementation responsibility for CSPs & CSCs

				Typical Control Applicability and Ownership (CSP-Owned, CSC-Owned, Shared)		
				IaaS	PaaS	SaaS
STA-04	Delineate the shared ownership and applicability of all CSA CCM controls according to the SSRM for the cloud service offering.	Cloud service implementations involve a Shared Security Responsibility Model (SSRM) between the Cloud Service Provider (CSP) and the Cloud Service Customer (CSC) which...	*"Expected Release in November/December"*	CSP-Owned	CSP-Owned	CSP-Owned

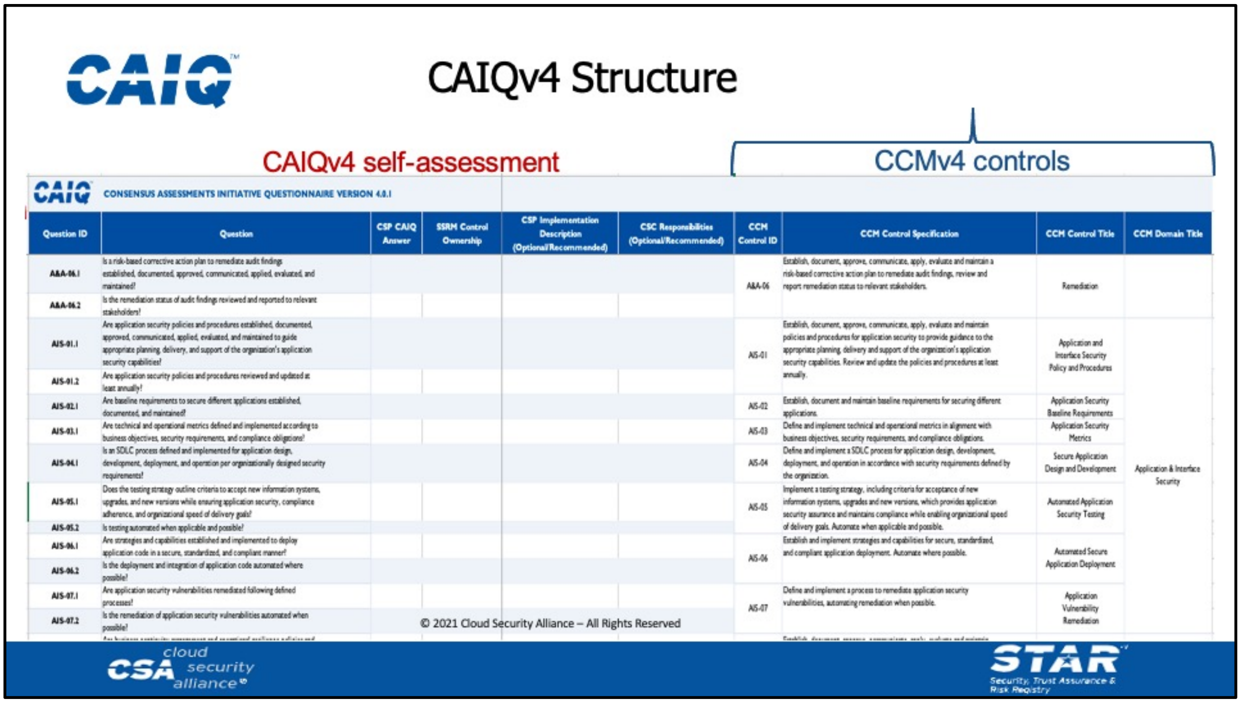


Intro to the CAIQv4

An Overview

CSA cloud security alliance®

STAR Security, Trust Assurance & Risk Registry



CAIQv4 Structure

CAIQv4 self-assessment

CCMv4 controls

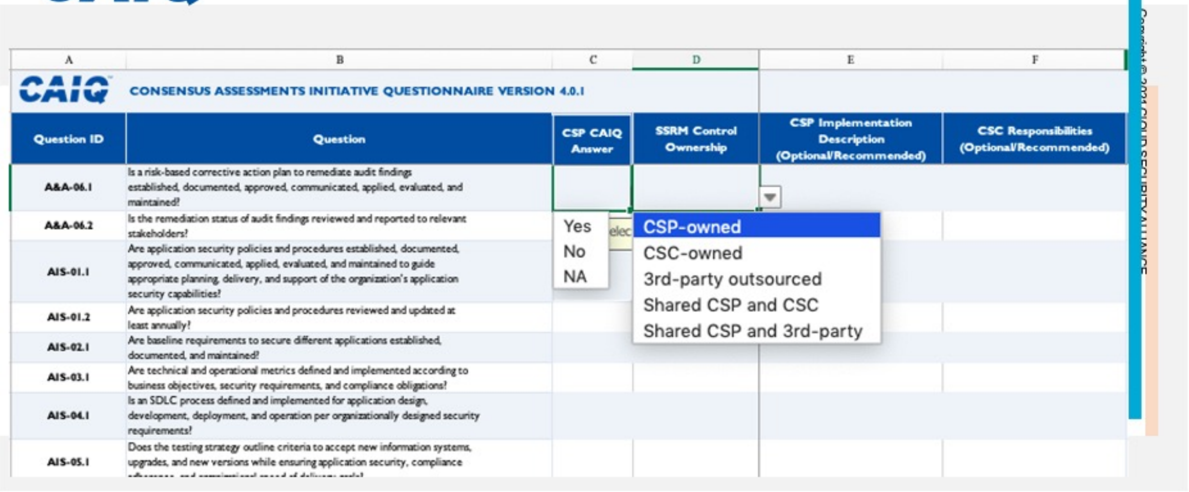
CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE VERSION 4.0.1

Question ID	Question	CSP CAIQ Answer	SSRM Control Ownership	CSP Implementation Description (Optional/Recommended)	CSC Responsibilities (Optional/Recommended)	CCM Control ID	CCM Control Specification	CCM Control Title	CCM Domain Title
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	Establish, document, approve, communicate, apply, evaluate and maintain a risk-based corrective action plan to remediate audit findings, review and report remediation status to relevant stakeholders.	Remediation	
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	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for application security to provide guidance to the appropriate planning, delivery and support of the organization's application security capabilities. Review and update the policies and procedures at least annually.	Application and Interface Security Policy and Procedures	Application & Interface Security
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-02	Establish, document and maintain baseline requirements for securing different applications.	Application Security Baseline Requirements	
AIS-03.1	Are technical and operational metrics defined and implemented according to business objectives, security requirements, and compliance obligations?					AIS-03	Define and implement technical and operational metrics in alignment with business objectives, security requirements, and compliance obligations.	Application Security Metrics	
AIS-04.1	Is an SDLC process defined and implemented for application design, development, deployment, and operation per organizationally designed security requirements?					AIS-04	Define and implement a SDLC process for application design, development, deployment, and operation in accordance with security requirements defined by the organization.	Secure Application Design and Development	
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?					AIS-05	Implement a testing strategy, including criteria for acceptance of new information systems, upgrades and new versions, which provides application security assurance and maintains compliance while enabling organizational speed of delivery goals. Automate when applicable and possible.	Automated Application Security Testing	
AIS-05.2	Is testing automated when applicable and possible?								
AIS-06.1	Are strategies and capabilities established and implemented to deploy application code in a secure, standardized, and compliant manner?					AIS-06	Establish and implement strategies and capabilities for secure, standardized, and compliant application deployment. Automate where possible.	Automated Secure Application Deployment	
AIS-06.2	Is the deployment and integration of application code automated where possible?								
AIS-07.1	Are application security vulnerabilities remediated following defined processes?					AIS-07	Define and implement a process to remediate application security vulnerabilities, automating remediation when possible.	Application Vulnerability Remediation	
AIS-07.2	Is the remediation of application security vulnerabilities automated when possible?								

© 2021 Cloud Security Alliance – All Rights Reserved

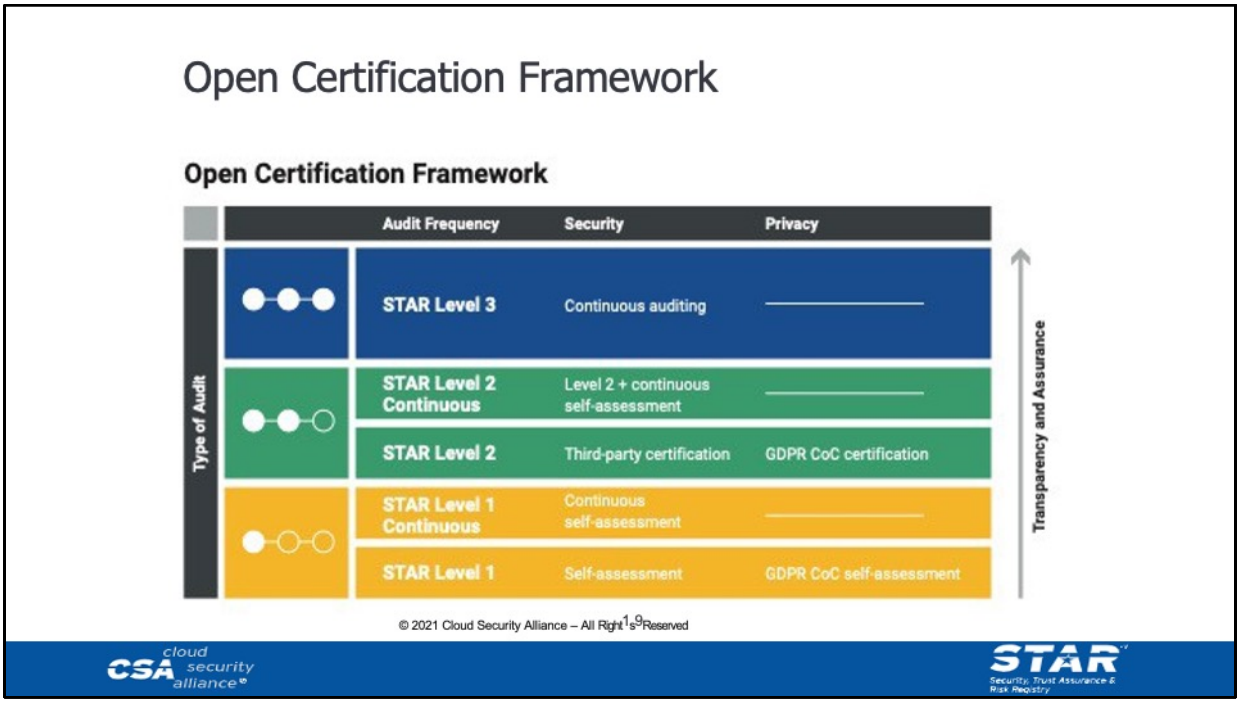
- It includes a total of 261 questions (compared to 310 of v3.1)
- It helps cloud customers/auditors gauge the security posture of CSPs and determine if their cloud services are suitably secure
- CAIQ questions are tailored to the control specifications of the CCM
- The new structure of CAIQv4 includes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

CAIQ CSP Self-Assessment Columns



CAIQ 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				



Open Certification Framework

Open Certification Framework

Type of Audit	Audit Frequency	Security	Privacy
●●●	STAR Level 3	Continuous auditing	——
●●○	STAR Level 2 Continuous	Level 2 + continuous self-assessment	——
	STAR Level 2	Third-party certification	GDPR CoC certification
●○○	STAR Level 1 Continuous	Continuous self-assessment	——
	STAR Level 1	Self-assessment	GDPR CoC self-assessment

Transparency and Assurance

© 2021 Cloud Security Alliance – All Right1s9Reserved

CSA cloud security alliance
STAR Security, Trust Assurance & Risk Registry

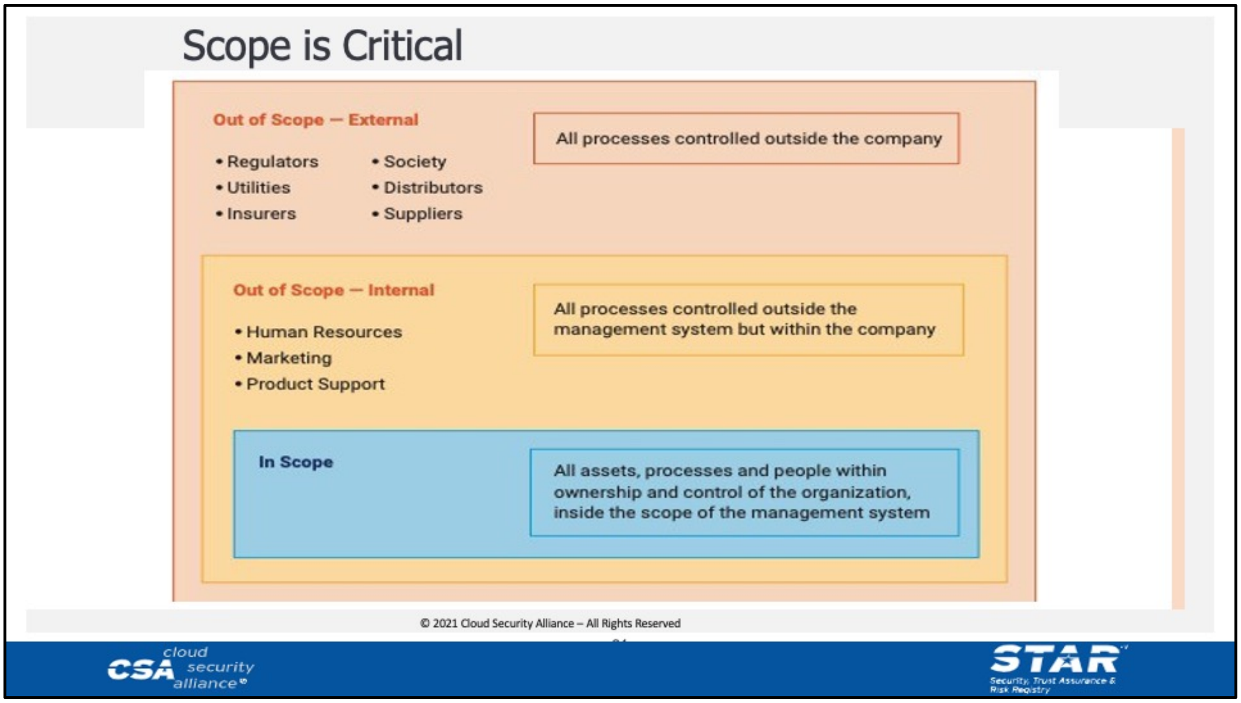
The OCF is the scheme that outlines the STAR Program and rules of engagement. Now every level has a option of continuous auditing and also GDPR Self-assessment that increases the the level of transparency, assurance and trust.

CSA STAR Attestation—CSA STAR Attestation is an auditing procedure to report on the examination of the implementation of trust service principles (TSP) and cloud-specific control objectives (CCM). CSA STAR Attestation can be considered as a SOC 2 Type 2 attestation augmented by CCM requirements.

CSA STAR Certification—The CSA STAR Certification is a third-party independent assessment of a CSP's security using the technology-neutral requirements of the ISO/IEC 27001:2013 management system standard together with the CSA Cloud Controls Matrix. STAR Certification is valid for three years and expires unless updated.

CSA C-STAR Assessment—The CSA C-STAR Assessment is another third-party independent assessment of the security of a CSP, but it is specifically designed for China-based companies based on China's national standards.

CSA GDPR COC third-party audit-based certification—The third-party certification, which is available in 2022, covers the same scope as the self-assessment, but rather than being a self-attestation, a CoC third-party assessment is obtained by having a qualified CoC auditing partner validate a CSP's adherence to the control specifications.



Scope is Critical

Out of Scope — External

- Regulators
- Utilities
- Insurers
- Society
- Distributors
- Suppliers

All processes controlled outside the company

Out of Scope — Internal

- Human Resources
- Marketing
- Product Support

All processes controlled outside the management system but within the company

In Scope

All assets, processes and people within ownership and control of the organization, inside the scope of the management system

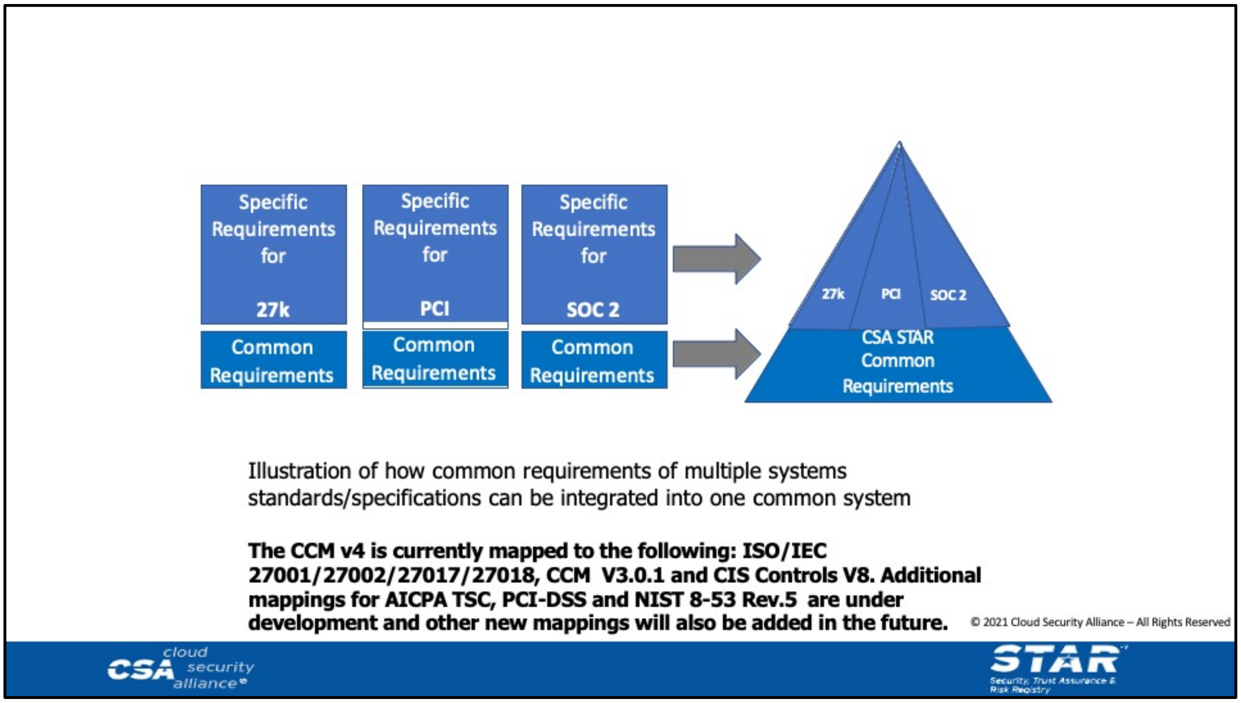
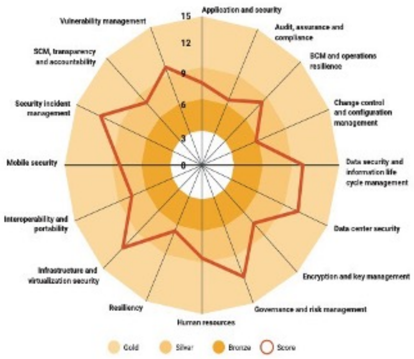

Specific Requirements for 27k
Specific Requirements for PCI
Specific Requirements for SOC 2
Common Requirements
Common Requirements
Common Requirements
27k
PCI
SOC 2
CSA STAR Common Requirements

Illustration of how common requirements of multiple systems standards/specifications can be integrated into one common system

The CCM v4 is currently mapped to the following: ISO/IEC 27001/27002/27017/27018, CCM V3.0.1 and CIS Controls V8. Additional mappings for AICPA TSC, PCI-DSS and NIST 8-53 Rev.5 are under development and other new mappings will also be added in the future.

Open Certification Framework

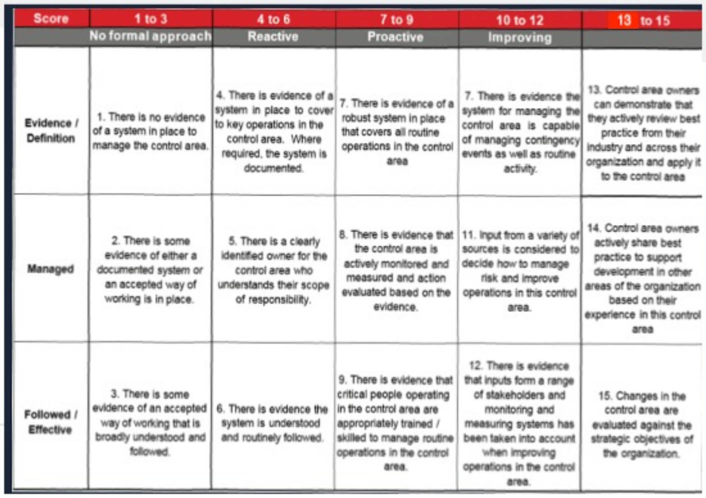


No award: 0-3

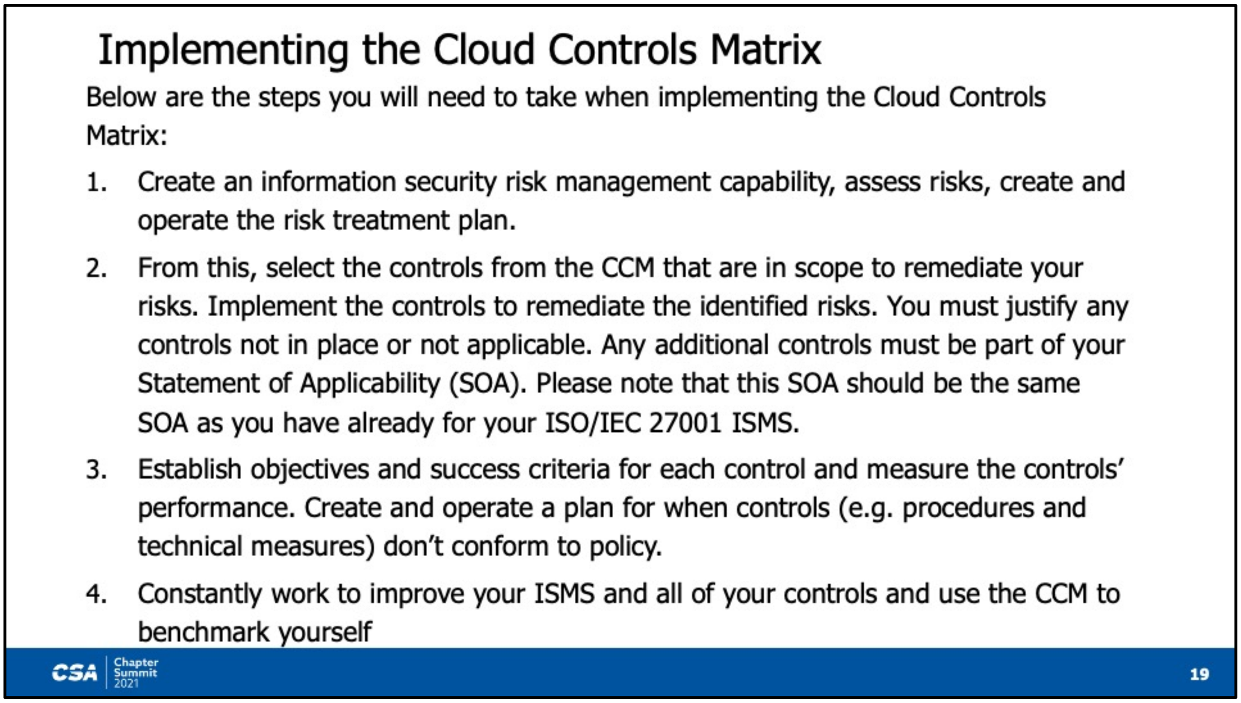
Bronze Award: 4-6

Silver Award: 7-9

Gold Award: 10-15



Score	1 to 3	4 to 6	7 to 9	10 to 12	13 to 15
	No formal approach	Reactive	Proactive	Improving	
Evidence / Definition	1. There is no evidence of a system in place to manage the control area.	4. There is evidence of a system in place to cover to key operations in the control area. Where required, the system is documented.	7. There is evidence of a robust system in place that covers all routine operations in the control area	7. There is evidence the system for managing the control area is capable of managing contingency events as well as routine activity.	13. Control area owners can demonstrate that they actively review best practice from their industry and across their organization and apply it to the control area
Managed	2. There is some evidence of either a documented system or an accepted way of working is in place.	5. There is a clearly identified owner for the control area who understands their scope of responsibility.	8. There is evidence that the control area is actively monitored and measured and action evaluated based on the evidence.	11. Input from a variety of sources is considered to decide how to manage risk and improve operations in this control area.	14. Control area owners actively share best practice to support development in other areas of the organization based on their experience in this control area
Followed / Effective	3. There is some evidence of an accepted way of working that is broadly understood and followed.	6. There is evidence the system is understood and routinely followed.	9. There is evidence that critical people operating in the control area are appropriately trained / skilled to manage routine operations in the control area.	12. There is evidence that inputs form a range of stakeholders and monitoring and measuring systems has been taken into account when improving operations in the control area.	15. Changes in the control area are evaluated against the strategic objectives of the organization.

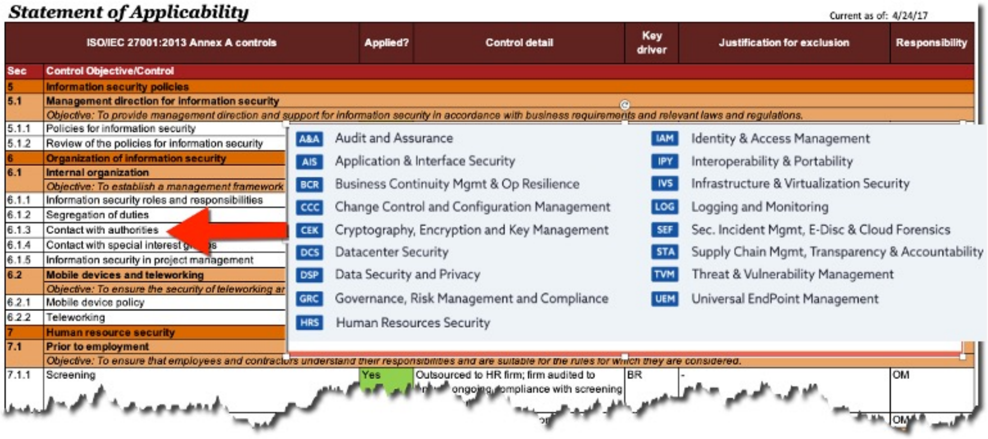


Implementing the Cloud Controls Matrix

Below are the steps you will need to take when implementing the Cloud Controls Matrix:

1. Create an information security risk management capability, assess risks, create and operate the risk treatment plan.
2. From this, select the controls from the CCM that are in scope to remediate your risks. Implement the controls to remediate the identified risks. You must justify any controls not in place or not applicable. Any additional controls must be part of your Statement of Applicability (SOA). Please note that this SOA should be the same SOA as you have already for your ISO/IEC 27001 ISMS.
3. Establish objectives and success criteria for each control and measure the controls' performance. Create and operate a plan for when controls (e.g. procedures and technical measures) don't conform to policy.
4. Constantly work to improve your ISMS and all of your controls and use the CCM to benchmark yourself

Statement Of Applicability



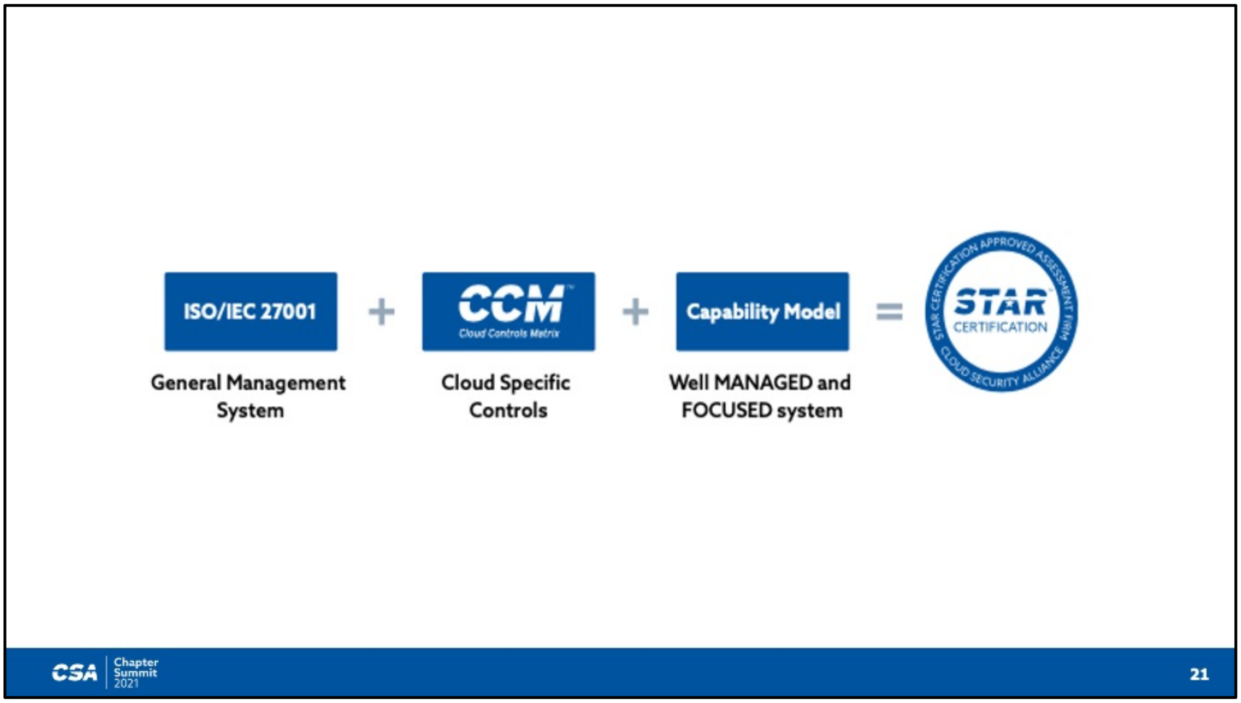
Statement of Applicability

Current as of: 4/24/17

	ISO/IEC 27001:2013 Annex A controls	Applied?	Control detail	Key driver	Justification for exclusion	Responsibility
Sec	**Control Objective/Control**					
5	**Information security policies**					
5.1	**Management direction for information security**					
	Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.					
5.1.1	Policies for information security					
5.1.2	Review of the policies for information security					
6	**Organization of information security**					
6.1	**Internal organization**					
	Objective: To establish a management framework					
6.1.1	Information security roles and responsibilities					
6.1.2	Segregation of duties					
6.1.3	Contact with authorities					
6.1.4	Contact with special interest gr s					
6.1.5	Information security in project management					
6.2	**Mobile devices and teleworking**					
	Objective: To ensure the security of teleworking ar					
6.2.1	Mobile device policy					
6.2.2	Teleworking					
7	**Human resource security**					
7.1	**Prior to employment**					
	Objective: To ensure that employees and contractors understand their responsibilities and are suitable for the rules for which they are considered.					
7.1.1	Screening	Yes	Outsourced to HR firm; firm audited to ongoing compliance with screening	BR	-	OM
						OM

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

Your Statement of Applicability (SoA) must be based on the Cloud Controls Matrix. You still can choose what is appropriate for your organization based upon both the type of service and risk to the organization.



ISO/IEC 27001 + CCM Cloud Controls Matrix + Capability Model = STAR CERTIFICATION

General Management System

Cloud Specific Controls

Well MANAGED and FOCUSED system

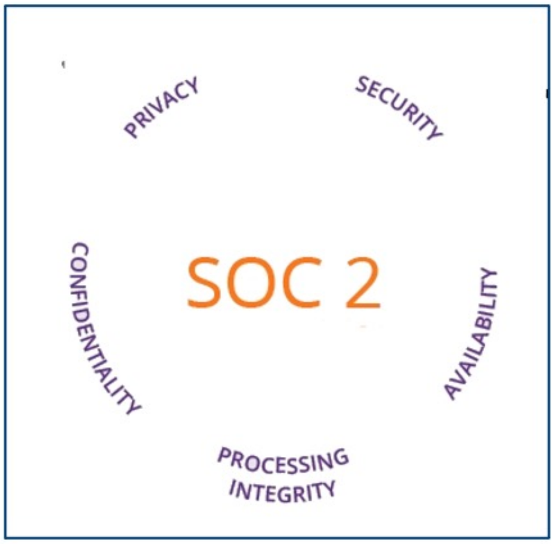
STAR Attestation

An Overview

CSA cloud security alliance
STAR
Security, Trust Assurance & Risk Registry

Trust Services Principles

The scope of the CSA STAR Attestation report is determined by the client utilizing one or more of the Trust Services Principles and Criteria and the CCM Criteria as specified by the client to determine whether the cloud services provider utilizes sufficient control activities to meet the specified criteria.

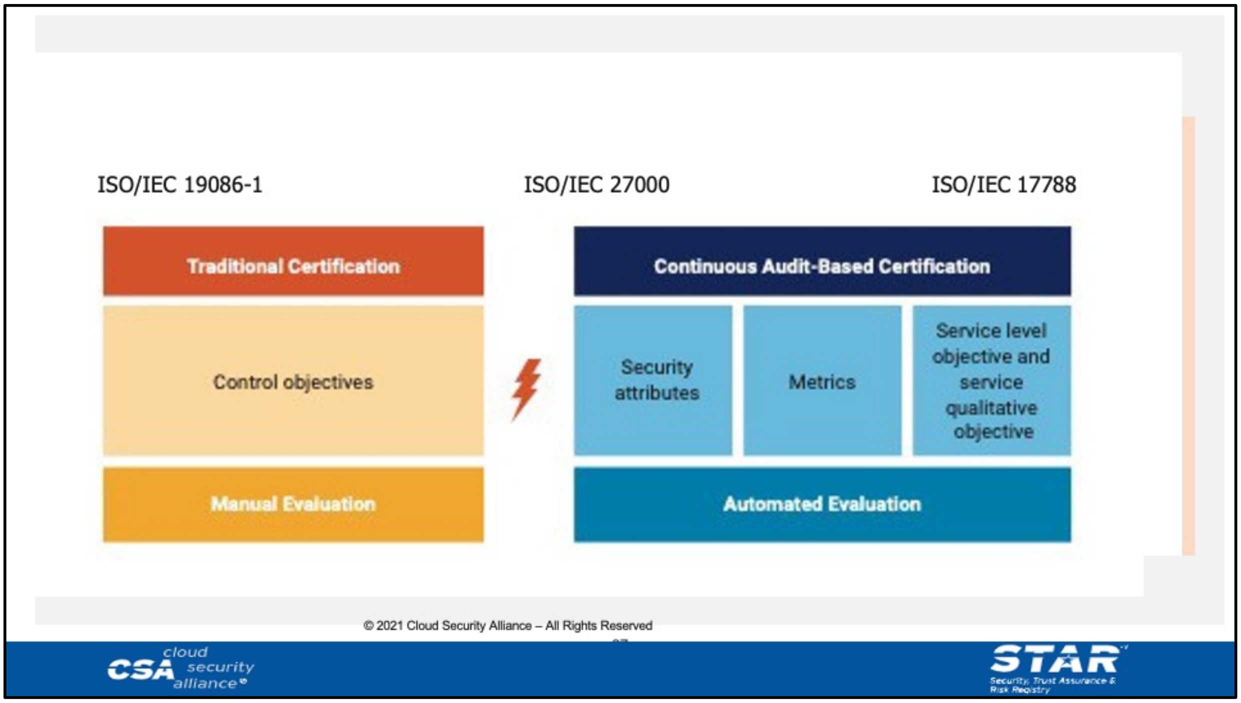


2.1 The STAR Attestation program is based on the combined requirements of the CCM and the TSC.

2.2 For a cloud system to qualify for STAR Attestation, the following must be satisfied:

- SOC 2 report scope must satisfy TSC Security category and CCM controls justified for inclusion.
- and the TSC Security category must be evaluated to ensure it includes all activities related to the reported cloud system.

Guidelines for CPAs Providing CSA STAR Attestation V.3



ISO/IEC 19086-1

ISO/IEC 27000

ISO/IEC 17788

Traditional Certification

Control objectives

Manual Evaluation

Continuous Audit-Based Certification

Security attributes

Metrics

Service level objective and service qualitative objective

Automated Evaluation

Level 3 – Continuous Auditing VS Level 3 Continuous Certification
ISO/IEC 19086-1:2016 seeks to establish a set of common cloud SLA building blocks (concepts, terms, definitions, contexts)
ISO/IEC **17788**:2014 provides an overview of cloud computing along with a set of terms and definitions. It is a terminology foundation for cloud computing ...

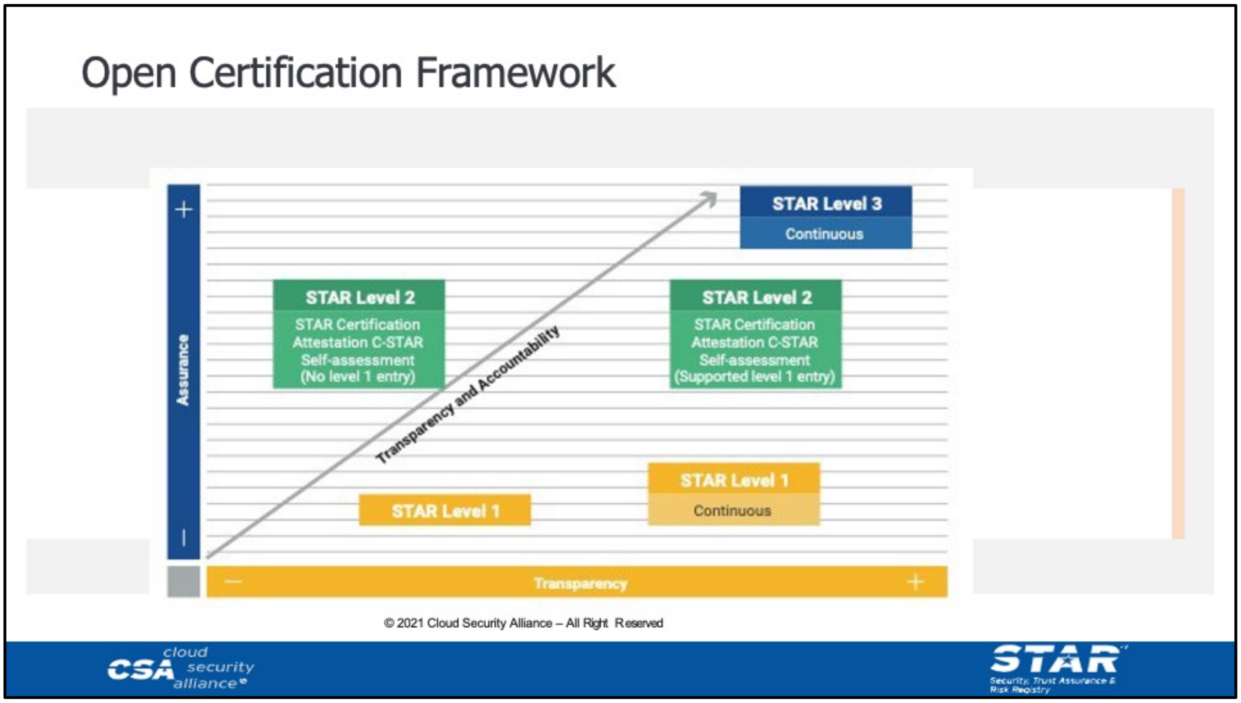
Continuous monitoring (CM) enables management to continually review business processes for adherence to and deviation from their intended levels of performance and effectiveness.
CM is an automated, ongoing process feeding through an API that enables management to continuously monitor on a frequent basis (Monthly, weekly, daily):

- Assess the effectiveness of controls and detect associated risk issues
- Improve business processes and activities while adhering to ethical and compliance standards
- Execute timelier quantitative and qualitative risk-related decisions
- Increase the cost-effectiveness of controls and monitoring through IT solutions

Value: The value of CM is that it gives management greater visibility into, and more timely information on, business processes designed to achieve strategic and operational goals. The value of CA is that it enables audit to move from sampling records and transactions to coverage of 100 percent of records and transactions (when and where desired)

Increase value through improved financial and operating controls

- Accelerate reporting to support more rapid decision making and business improvement
- Detect exceptions in real time to enable real-time responses
- Reduce — and ultimately minimize — ongoing compliance costs
- Replace manual preventative controls with automated detective controls
- Establish a more automated, risk-based control environment with lower labor costs
- Heighten competitive advantage and increase value to stakeholders through the highest level of transparency, assurance, accountability, and trust.



Open Certification Framework

STAR Level 3
Continuous

STAR Level 2
STAR Certification
Attestation C-STAR
Self-assessment
(No level 1 entry)

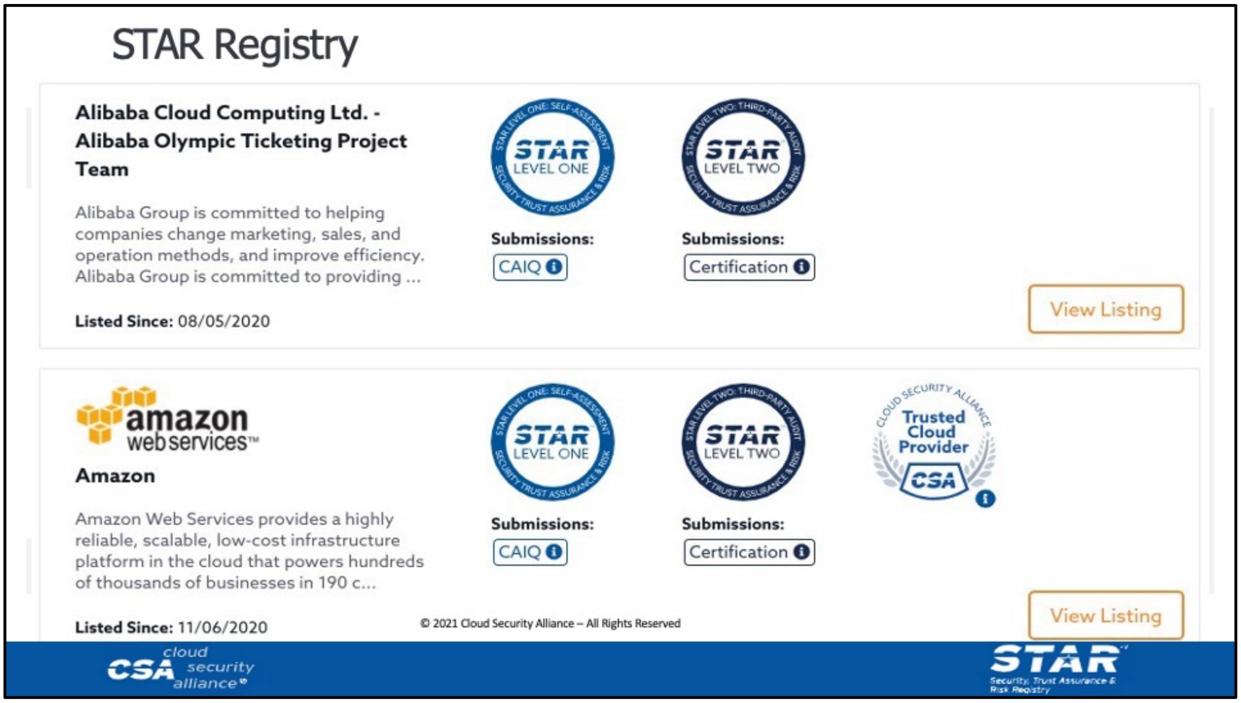
STAR Level 2
STAR Certification
Attestation C-STAR
Self-assessment
(Supported level 1 entry)

STAR Level 1

STAR Level 1
Continuous

+
Assurance
–
Transparency and Accountability
–
Transparency
+

CSA cloud security alliance®
STAR Security, Trust Assurance & Risk Registry



STAR Registry

Alibaba Cloud Computing Ltd. - Alibaba Olympic Ticketing Project Team

Alibaba Group is committed to helping companies change marketing, sales, and operation methods, and improve efficiency. Alibaba Group is committed to providing ...

Listed Since: 08/05/2020

Submissions: CAIQ

Submissions: Certification

Amazon

Amazon Web Services provides a highly reliable, scalable, low-cost infrastructure platform in the cloud that powers hundreds of thousands of businesses in 190 c...

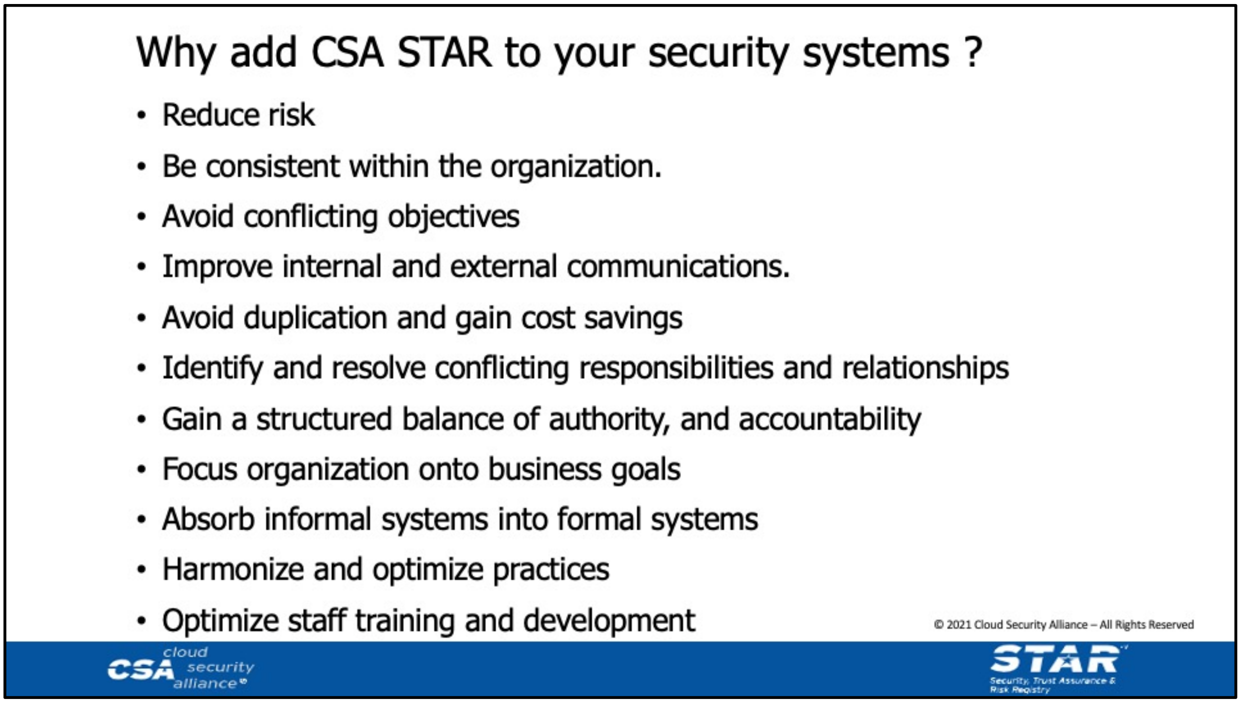
Listed Since: 11/06/2020

Submissions: CAIQ

Submissions: Certification

STAR LEVEL ONE
STAR LEVEL ONE: SELF-ASSESSMENT
SECURITY TRUST ASSURANCE & RISK
STAR LEVEL TWO
STAR LEVEL TWO: THIRD-PARTY AUDIT
View Listing
amazon web services™
Trusted Cloud Provider
CLOUD SECURITY ALLIANCE
CSA
View Listing
CSA cloud security alliance®
STAR Security, Trust Assurance & Risk Registry

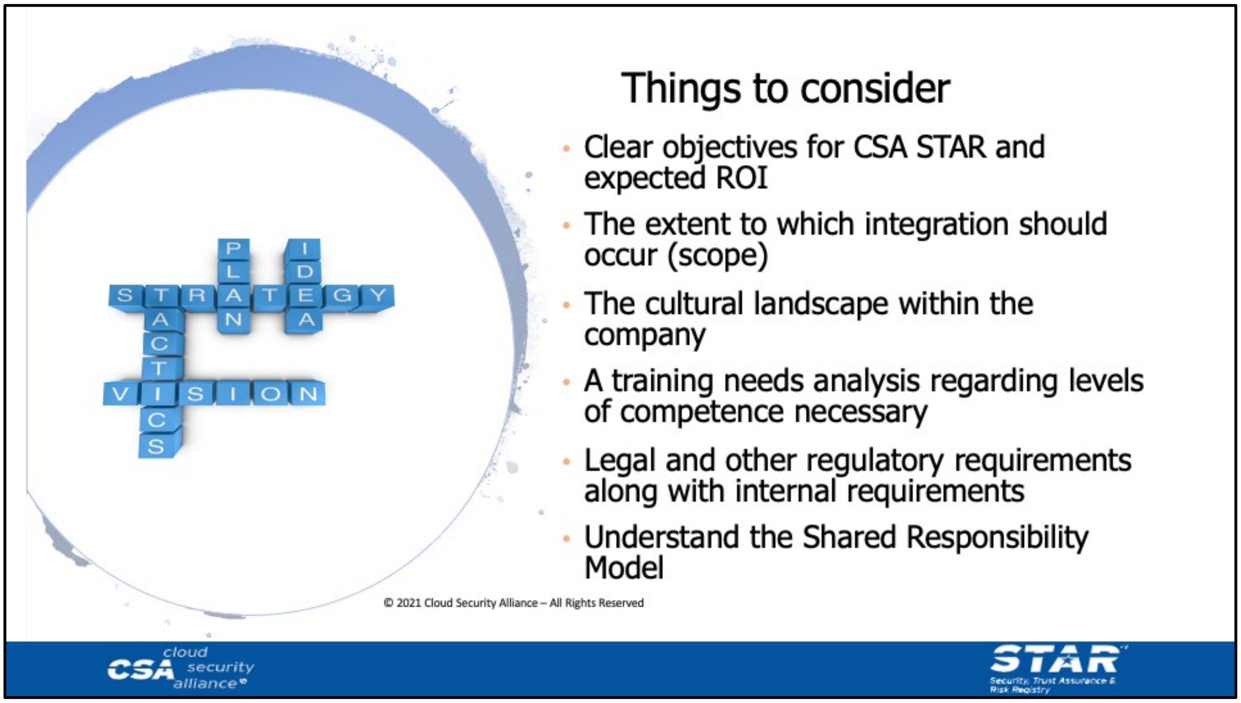
Once an organization has submitted a self-assessment or achieved Level 2 certification/attestation, it is posted on the STAR Registry adding you to the elite list of CSP leaders. As a publicly available registry, it is contentment you can share world-wide to show you are among the leaders and visionaries in the industry.



Why add CSA STAR to your security systems ?

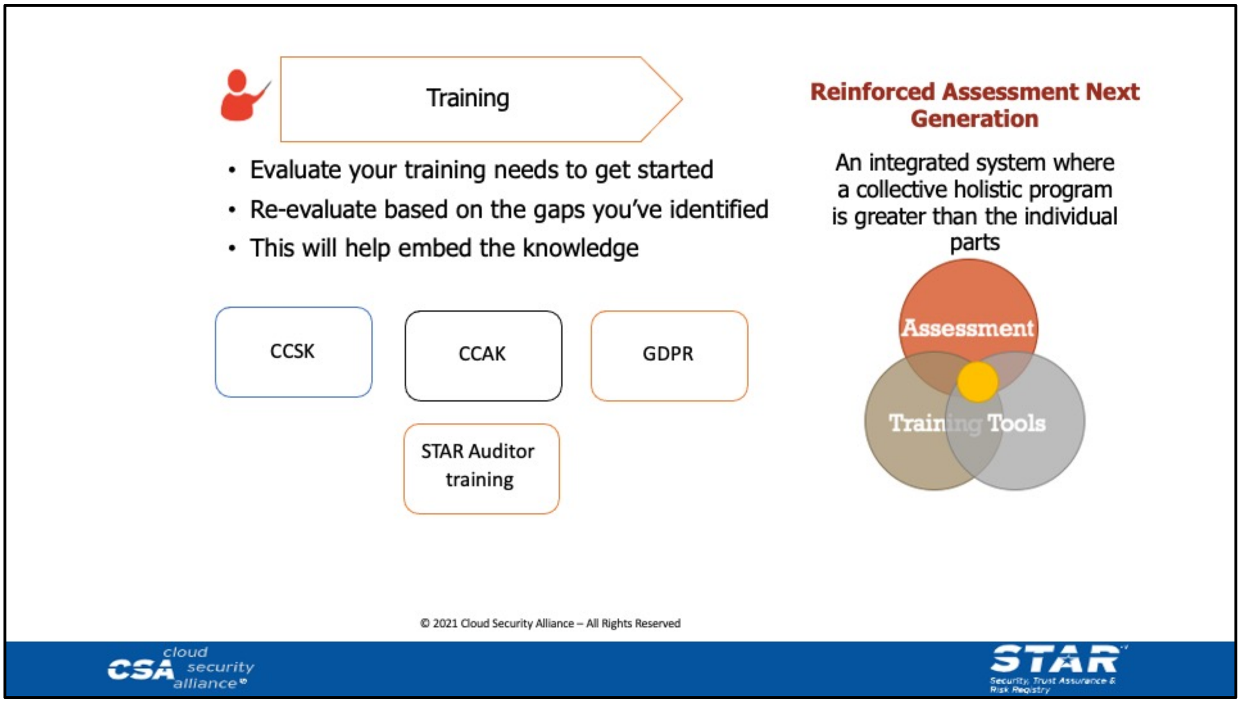
- Reduce risk
- Be consistent within the organization.
- Avoid conflicting objectives
- Improve internal and external communications.
- Avoid duplication and gain cost savings
- Identify and resolve conflicting responsibilities and relationships
- Gain a structured balance of authority, and accountability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

CSA cloud security alliance
STAR
Security, Trust Assurance & Risk Registry



Things to consider

- Clear objectives for CSA STAR and expected ROI
- The extent to which integration should occur (scope)
- The cultural landscape within the company
- A training needs analysis regarding levels of competence necessary
- Legal and other regulatory requirements along with internal requirements
- Understand the Shared Responsibility Model



Training

- Evaluate your training needs to get started
- Re-evaluate based on the gaps you've identified
- This will help embed the knowledge

CCSK

CCAK

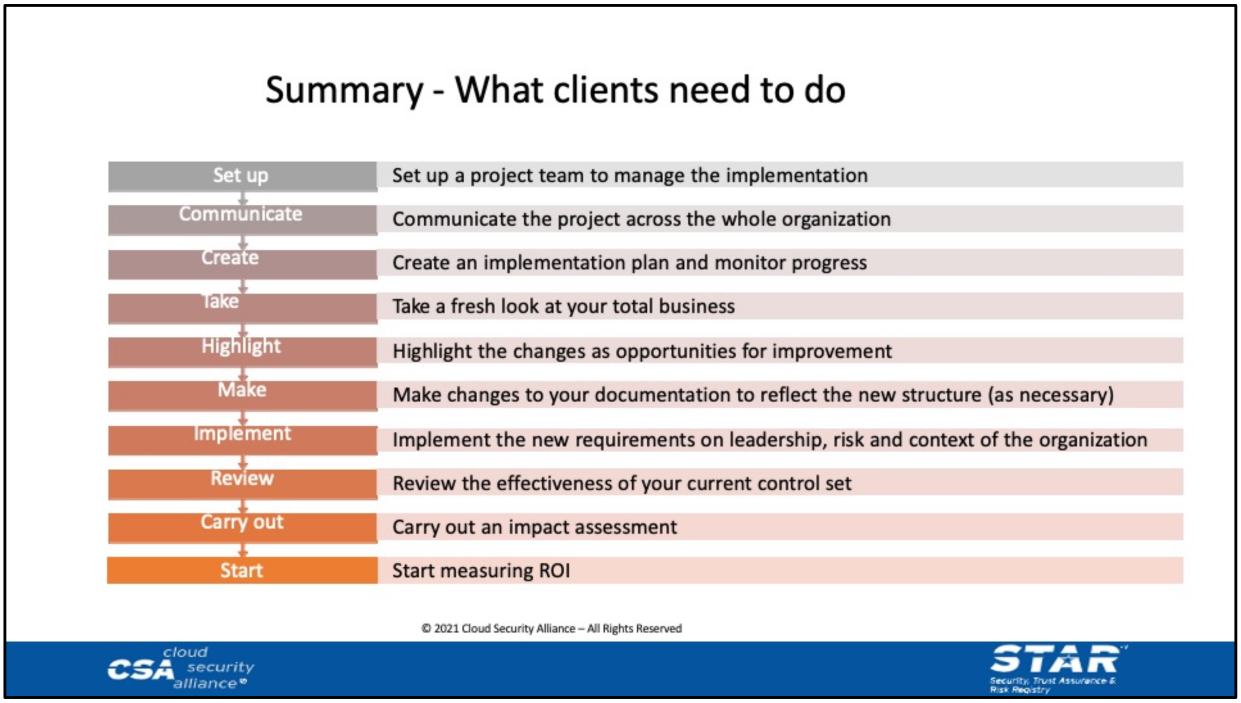
GDPR

STAR Auditor training

Reinforced Assessment Next Generation

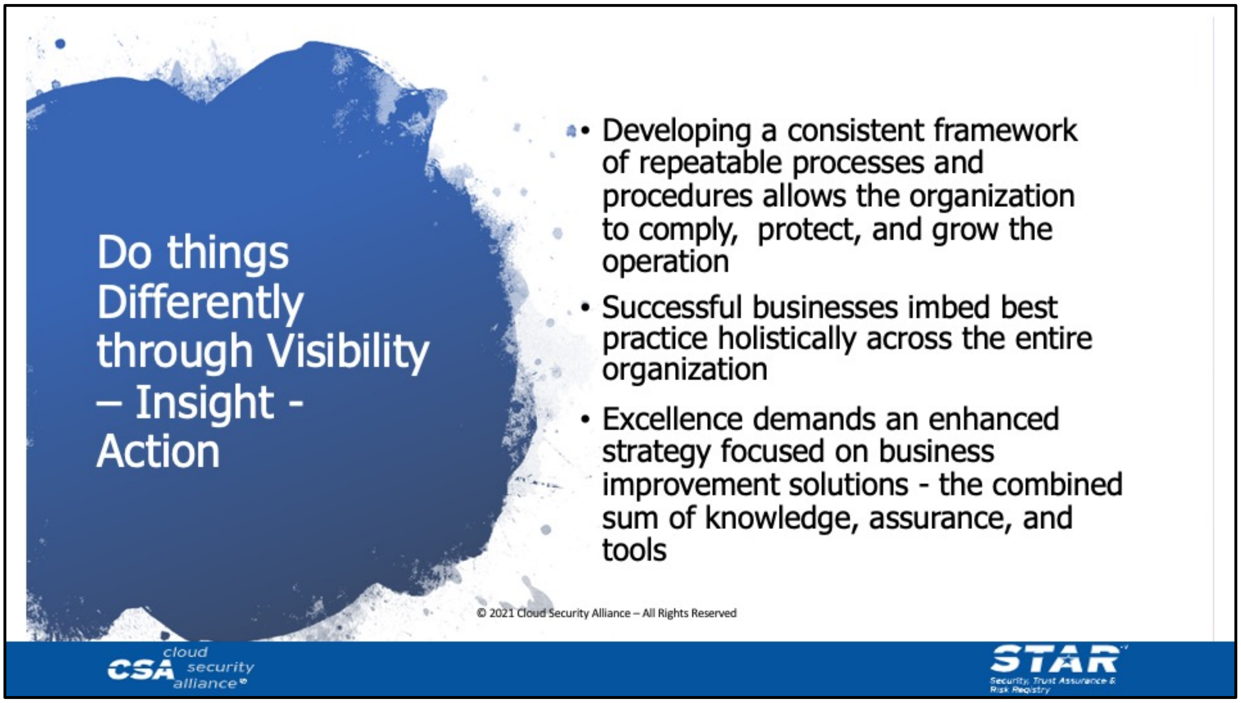
An integrated system where a collective holistic program is greater than the individual parts

Assessment
Training
Tools



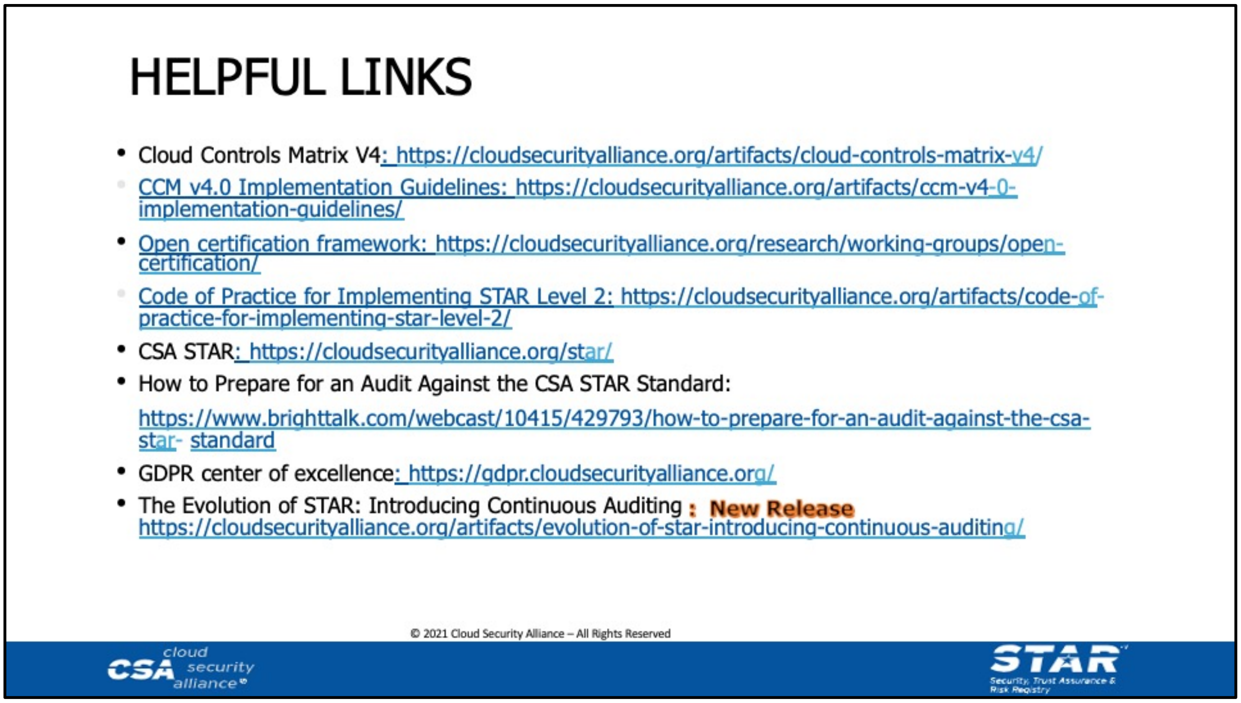
Summary - What clients need to do

Set up	Set up a project team to manage the implementation
Communicate	Communicate the project across the whole organization
Create	Create an implementation plan and monitor progress
Take	Take a fresh look at your total business
Highlight	Highlight the changes as opportunities for improvement
Make	Make changes to your documentation to reflect the new structure (as necessary)
Implement	Implement the new requirements on leadership, risk and context of the organization
Review	Review the effectiveness of your current control set
Carry out	Carry out an impact assessment
Start	Start measuring ROI



Do things Differently through Visibility – Insight - Action

- Developing a consistent framework of repeatable processes and procedures allows the organization to comply, protect, and grow the operation
- Successful businesses imbed best practice holistically across the entire organization
- Excellence demands an enhanced strategy focused on business improvement solutions - the combined sum of knowledge, assurance, and tools

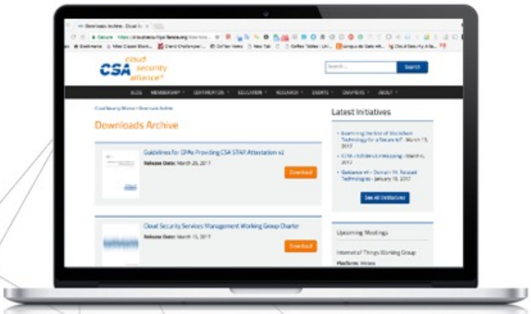


HELPFUL LINKS

- Cloud Controls Matrix V4: https://cloudsecurityalliance.org/artifacts/cloud-controls-matrix-v4/
- CCM v4.0 Implementation Guidelines: https://cloudsecurityalliance.org/artifacts/ccm-v4-0-implementation-guidelines/
- Open certification framework: https://cloudsecurityalliance.org/research/working-groups/open-certification/
- Code of Practice for Implementing STAR Level 2: https://cloudsecurityalliance.org/artifacts/code-of-practice-for-implementing-star-level-2/
- CSA STAR: https://cloudsecurityalliance.org/star/
- How to Prepare for an Audit Against the CSA STAR Standard:

  https://www.brighttalk.com/webcast/10415/429793/how-to-prepare-for-an-audit-against-the-csa-star- standard
- GDPR center of excellence: https://gdpr.cloudsecurityalliance.org/
- The Evolution of STAR: Introducing Continuous Auditing **: New Release** https://cloudsecurityalliance.org/artifacts/evolution-of-star-introducing-continuous-auditing/

Thank You!



Downloads Archive

Guidelines for CPAs Providing CSA STAR Attestation v2

Release Date: March 20, 2017

Download

Cloud Security Services Management Working Group Charter

Release Date: March 15, 2017

Download

Latest Initiatives

- Examining the Use of Blockchain Technology for a Secure IoT - March 13, 2017
- CCM - [illegible] Mapping - March 6, 2017
- Guidance v4 - Domain 14: Related Technologies - January 18, 2017

See All Initiatives

Upcoming Meetings

Internet of Things Working Group

Platform: Webex

Search
BLOG MEMBERSHIP CERTIFICATION EDUCATION RESEARCH EVENTS CHAPTERS ABOUT

Contact CSA

Email: info@cloudsecurityalliance.org

Twitter: @Cloudsa

Site: www.cloudsecurityalliance.org

Download: https://cloudsecurityalliance.org/research/artifacts/