

CSA STAR™ Level and Scheme Requirements

TABLE OF CONTENTS

STAR Introduction.....	3
STAR Levels Overview.....	4
Level 1.....	5
STAR Self-Assessment.....	6
GDPR CoC Self-Assessment (Privacy).....	6
Level 2.....	6
CSA STAR Attestation.....	6
CSA STAR Certification.....	7
CSA C-STAR Assessment.....	8
GDPR CoC Certification (Privacy).....	9
Level 3.....	10
CSA STAR-Continuous.....	10

SECURITY, TRUST, ASSURANCE AND RISK (STAR™)

CSA Security Trust, Assurance and Risk (STAR™) is the industry's most powerful program for security assurance in the cloud. STAR™ encompasses key principles of transparency, rigorous auditing, and harmonization of standards. The STAR™ program provides multiple benefits, including indications of best practices and validation of security posture of cloud offerings.

STAR™ is based on the following foundation tools:

- The [CSA Cloud Controls Matrix](#) (CCM)
- The [Consensus Assessments Initiative Questionnaire](#) (CAIQ)
- The [CSA Code of Conduct for GDPR Compliance](#)

The CCM is the only meta-framework of cloud-specific security controls, mapped to leading standards, best practices and regulations. CCM provides organizations with the needed structure, detail and clarity relating to information security tailored to cloud computing. CCM is currently considered a de-facto standard for cloud security assurance and compliance.


The CAIQ is based upon the CCM and provides a set of Yes/No questions a cloud consumer and cloud auditor may wish to ask of a cloud provider to ascertain their compliance to the Cloud Controls Matrix.

The [CSA Code of Conduct for GDPR Compliance](#) is a tool created in collaboration with industry experts and representatives from EU national data protection authorities to assist organizations in adhering to the European General Data Protection Regulation. The CSA's Code include all the necessary requirements a Cloud Service Provider has to satisfy in order to comply with the EU GDPR.

One of most essential features of the STAR™ program is its registry that documents the security and privacy controls provided by popular cloud computing offerings. This publicly accessible registry is designed for users of cloud services to assess their cloud providers, security providers and advisory and assessment services firms in order to make the best procurement decisions.

STAR™ LEVELS OVERVIEW

Open Certification Framework

	AUDIT FREQUENCY	Security	Privacy
TYPE OF AUDIT		STAR Level 3	Continuous Auditing
		STAR Level 2 Continuous	Level 2 + Continuous Self-Assessment
		STAR Level 2	3rd Party Certification
		STAR Level 1 Continuous	Continuous Self-Assessment
		STAR Level 1	Self-Assessment
			GDPR CoC Certification
			GDPR CoC Self-Assessment

TRANSPARENCY & ASSURANCE

The above image depicts three levels in the Open Certification Framework that STAR™ uses. Each of the 3 levels offers a different level of assurance:

- Level One: Self Assessment
- Level Two: Third-Party Certification
- Level Three: Continuous Monitoring

Level One: Self-Assessment

There are different options for completing each level of assurance. For level one organizations can choose to complete one or both of the security and privacy self-assessments.

Level Two: Third-Party Certification

Organizations looking for a third-party certification can choose from one or more of the options above. In some cases an organization may choose to pursue all of the certifications at this level, in other cases one will suffice. An organization's location, along with the regulations and standards it is subject to will have the greatest factor in determining which ones are appropriate to pursue.

Level 3: Continuous Monitoring

CSA STAR™ Continuous Monitoring enables automation of the current security practices of cloud providers. Providers publish their security practices according to CSA formatting and specifications, and customers and tool vendors can retrieve and present this information in a variety of contexts.

All Levels: Continuous Auditing

Each level of STAR™ has also has a continuous auditing option that allows you to increase your transparency. STAR™ Continuous can be attained by building upon the CSP's current STAR™ level.

LEVEL 1

STAR™ Self-Assessment

CSA STAR™ Self Assessment is free and open to all cloud providers and allows them to submit self assessment reports that document compliance to CSA-published best practices.

Since the initial launch at the end of 2011, CSA has seen tremendous growth in STAR™ Self Assessment, with major cloud players including Amazon Web Services, Box.com, HP, Microsoft, Ping Identity, Red Hat, Skyhigh Networks, Symantec, Terremark and many other submitting entries into the registry. These cloud providers recognized the need to provide transparency and assurance of their cloud services to corporations and end users, who are increasingly requesting visibility into the security controls provided by various cloud computing offerings. The CSA STAR™ Self Assessment is open to all cloud providers.

Cloud providers can submit two different types of reports to indicate their compliance with CSA best practices:

- The Consensus Assessments Initiative Questionnaire (CAIQ), which provides industry-accepted ways to document what security controls exist in IaaS, PaaS and SaaS offerings. The questionnaire (CAIQ) provides a set of 295 questions a cloud consumer and cloud auditor may wish to ask of a cloud provider. Providers may opt to submit a completed Consensus Assessments Initiative Questionnaire.
- The [Cloud Controls Matrix](#) (CCM), which provides a controls framework that gives a detailed understanding of security concepts and principles that are aligned to the Cloud Security Alliance guidance in 13 domains. As a framework, the CSA CCM provides organizations with the needed structure, detail and clarity relating to information security tailored to the cloud industry. Providers may choose to submit a report documenting compliance with Cloud Controls Matrix.

CSA strongly encourages all IaaS, SaaS and PaaS providers, large and small, to complete a self-assessment for publication. In doing so, they will address some of the most urgent and important security questions buyers are asking and can dramatically speed up the purchasing process for their services.

In addition to cloud provider self assessments, CSA STAR™ will also provide listings to solution providers who have integrated CAIQ, CCM and other GRC Stack components into their compliance management tools. This will help customers extend their GRC monitoring and reporting across their enterprise and in concert with multiple cloud provider relationships.

GDPR CoC Self-Assessment (Privacy)

The Code Self-Assessment consist in the voluntary publication on the STAR™ Registry of two documents:

- [Code of Conduct Statement of Adherence](#), and
- [Self-assessment results based on the PLA Code of Practice \(CoP\) Template - Annex 1](#)

The Code Self-Assessment covers the compliance to GDPR of the service(s) offered by a CSP. A company after the publication of the relevant document on the Registry will receive a Compliance Mark valid for 1 year. The Self-Assessment shall be revised every time there's a change to the company policies or practices related to the service under assessment.

LEVEL 2

CSA STAR™ Attestation

The STAR™ Attestation is positioned as STAR™ Certification at Level 2 of the Open Certification Framework and STAR™ Certification is a rigorous third party independent assessment of the security of a cloud service provider.

STAR™ Attestation is based on type 1 or type 2 SOC attestations supplemented by the criteria in the Cloud Controls Matrix (CCM). This assessment:

- Is based on a mature attest standard
- Allows for immediate adoption of the CCM as additional criteria and the flexibility to update the criteria as technology and market requirements change
- Does not require the use of any criteria that were not designed for, or readily accepted by cloud providers
- Provides for robust reporting on the service provider's description of its system and on the service provider's controls, including a description of the service auditor's tests of controls in a format very similar to the now obsolete SAS 70 reporting format and current SSAE 16 (SOC 1) reporting, thereby facilitating market acceptance

STAR™ Attestation builds on the key strengths of SOC 2 (AT 101):

- Is a mature attest standard (it serves as the standard for SOC 2 and SOC 3 reporting)
- Provides for robust reporting on the service provider's description of its system and on the service provider's controls, including a description of the service auditor's tests of controls in a format very similar to the now obsolete SAS 70 reporting format and current SSAE 18 (SOC 1) reporting, thereby facilitating market acceptance
- Evaluation over a period of time rather than a point in time
- Recognition with an AICPA Logo

CSA STAR™ Certification

The CSA STAR™ Certification is a rigorous third party independent assessment of the security of a cloud service provider. The technology-neutral certification leverages the requirements of the ISO/IEC 27001 management system standard together with the CSA Cloud Controls Matrix, a specified set of criteria that measures the capability levels of the cloud service.

Organizations that outsource services to cloud service providers have a number of concerns about the security of their data and information. By achieving the STAR™ Certification, cloud providers of every size will be able to give prospective customers a greater understanding of their levels of security controls.

The STAR™ Certification is based upon achieving ISO/IEC 27001 and the specified set of criteria outlined in the Cloud Controls Matrix.

The independent assessment by an [accredited CSA certification body](#) will assign a 'Management Capability' score to each of the CCM security domains. Each domain will be scored on a specific maturity and will be measured against five management principles.

The internal report will show organizations how mature their processes are and what areas they need to consider improving on to reach an optimum level of maturity. These levels will be designated as either "No", "Bronze", "Silver" or "Gold" awards. Certified organizations will be listed on the CSA STAR™ Registry as "STAR Certified".

STAR™ CERTIFICATION evaluates the efficiency of an organization's ISMS and ensures the scope, processes and objectives are "Fit for Purpose" and helps organizations prioritize areas for improvement and lead them towards business excellence.

It also enables effective comparison across other organizations in the applicable sector and it is focused on the strategic and operational business benefits as well as effective partnership relationships.

CSA STAR™ Certification enables the auditor to assess a company's performance, on long-term sustainability and risks, in addition to ensuring they are SLA driven, allowing senior management to quantify and measure improvement year on year.

To be consistent with international standards, the STAR™ certification scheme is designed to comply with:

- ISO/IEC 17021:2011, Conformity assessment – Requirements for bodies providing audit and certification of management systems
- ISO/IEC 27006:2011, Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems
- ISO 19011, Guidelines for auditing management systems

IMPORTANT NOTE: CSA STAR™ Certification assessments are based on either [CCM v1.4](#) and ISO/IEC 27001:2005 or [CCM v3](#) and ISO/IEC 27001:2013.

As of March 2015, all CSA STAR™ Certification assessments are based on CCM v3.x and ISO/IEC 27001:2013.

Why Certify?

Whether you use cloud services, provide cloud services, audit/certify cloud services, or secure cloud services, you have a vested interest in knowing more about cloud security from an objective, third-party source. You need the right tools to ensure that you are playing your part in securing the cloud ecosystem while supporting industry standards.

CSA C-STAR™ Assessment

The CSA C-STAR™ Assessment is a robust third party independent assessment of the security of a cloud service provider for the Greater China market that harmonizes CSA best practices with Chinese national standards. The technology-neutral assessment leverages the requirements of the GB/T 22080-2008 management system standard together with the CSA Cloud Controls Matrix, a specified set of criteria that measures the capability levels of the cloud service, plus 29 related controls selected from China's national standard GB/T 22239-2008(Information security technology — Baseline for classified protection of information system) and GB/Z 28828-2012(Information security technology – Guideline for personal information protection within information system for public and commercial services).

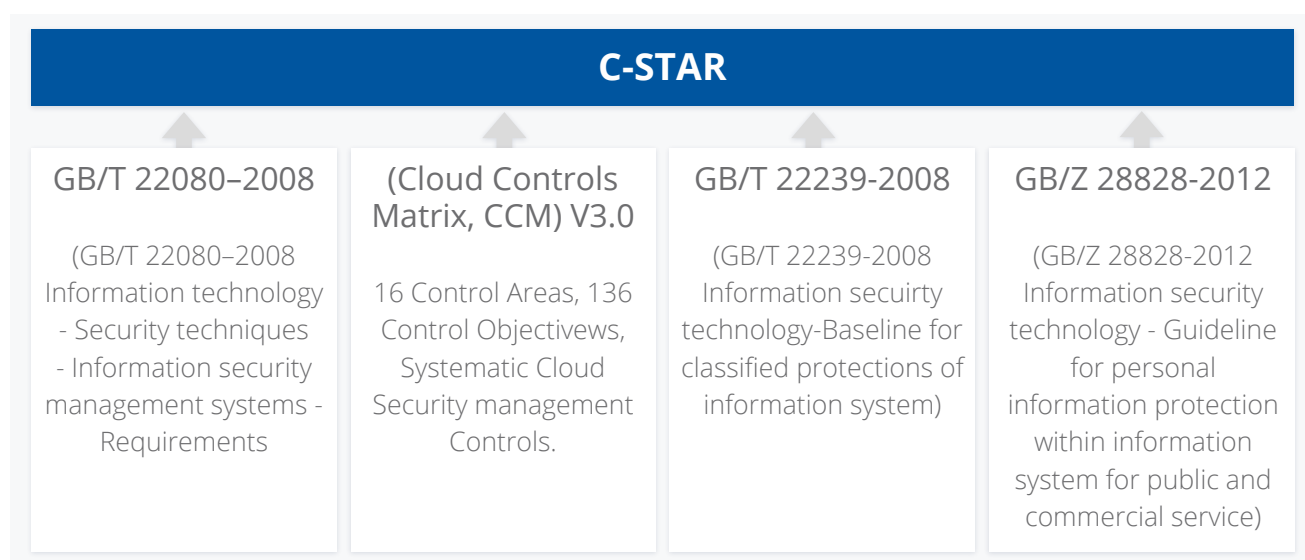


Figure 1 C-STAR Assessment Framework

Organizations that outsource services to cloud service providers have a number of concerns about the security of their data and information. By passing the C-STAR™ Assessment, cloud providers, regardless of the size of their operation, will be able to give prospective customers a greater understanding of their security management status.

The C-STAR™ Assessment is based on GB/T 22080-2008 and the specified set of criteria outlined in the Cloud Controls Matrix, plus related requirements of GB/T 22239-2008 and GB/Z 28828-2012.

The independent assessment by an accredited CSA certification body, such as CEPREI Certification Body (<http://www.ceppei.org/>), will assign a 'Management Capability' score to each of the CCM security

domains (including requirements selected from GB/T 22239-2008 and GB/Z 28828-2012). Each domain will be scored on a specific maturity and will be measured against the assessors' grid.

The assessment report will show organizations how mature their processes are and what areas they need to consider improving on to reach an optimum level of maturity. Certified organizations will be listed on the CSA STAR™ Registry as "C-STAR Assessed".

C-STAR™ Assessment enables effective comparison across other organizations in an applicable sector and it is focused on strategic and operational business benefits as well as effective partner relationships.

C-STAR™ Assessment enables the assessor to assess a company's performance in long-term sustainability and risks management, in addition to ensuring that the company is SLA-driven, allowing senior management to quantify and measure improvement year on year.

To be consistent with China national requirements, the C-STAR™ Assessment scheme is designed to comply with:

- CNAS CC01:2011 IDT ISO/IEC 17021:2011, Requirements for bodies providing audit and certification of management systems
- CNAS CC17:2012 IDT ISO/IEC 27006:2011, Requirements for Information Security Management System Certification Body
- CNAS SC18:2012, Accreditation Scheme for ISMS Certification Bodies
- GB/T 19011:2013 IDT ISO19011:2011 Management System Audit Guidance

GDPR CoC Certification (Privacy)

The CoC third-party certification is obtained via the validation by a qualified CoC auditing partner and provides increased assurance in regards to the self Statement of Adherence issued by an organization to the PLA CoP requirements. The validation process aims to verify the following:

- the correct use of the CoC (e.g., did the data controller/data processor complete all sections in the PLA CoP? Does the content included in every section provide the necessary information on data handling and processing?);
- the accuracy of information included in the Code (e.g., is the information included in the submission truthful? Are statements supported by evidence?).

A CoC third-party certification mark will be issued and will have a validity of 12 months from the day of its issuance and it will be renewed after this period.

Read the Code of Conduct here: <https://gdpr.cloudsecurityalliance.org/wp-content/uploads/sites/2/2018/08/CSA-Code-of-Conduct-for-GDPR-Compliance-Aug14-18.pdf>

LEVEL 3

CSA STAR™-Continuous

STAR™ Continuous is a continuous compliance assessment program for cloud services and an integral component of the CSA STAR™ Program. The program gives CSPs the opportunity to align their security validation capabilities with cloud security compliance and certification on an ongoing basis. STAR™ Continuous specifies the necessary activities and conditions for the continuous auditing of the cloud service over a defined set of security requirements, covering aspects from governance to infrastructure, and requiring the cloud service to define necessary processes that will be executed during the validation of controls within the scope of assessment. The program promotes trust by ensuring that a cloud service's necessary activities and conditions are continuously met by continuous auditing, such as through the operationalization of security and privacy requirements.

- A STAR™ Level 1 a CSP that uses a CAIQ to achieve Self-Assessment, a point-in-time assessment, can use a Continuous Self-Assessment to demonstrate effectiveness of controls over a period of time, to achieve STAR™ Continuous Level 1;
- A STAR™ Level 2 a CSP, who holds a third-party certification, can achieve STAR™ Level 2 Continuous by adding a Continuous Self-Assessment, which allows them to quickly inform customers of changes to their security programs, instead of communicating those until the next audit period in normal STAR™ Level 2.
- A STAR™ Level 3 a CSP is the most transparent through a continuous, automated process that ensures that security controls are monitored and validated at all times.

Benefits of CSA STAR™ Continuous

STAR™ Continuous improves on the traditional point-in-time certification in both trust and transparency. A cloud security certification is granted to a cloud service relying on trust that the security posture between audits is maintained. However, point-in-time audits often contain a considerable time gap between audits, and by adopting continuous auditing with an increased audit frequency, chances of deviation of the security posture becomes less. This empowers cloud service providers to make precise statements on compliance status of their cloud services covered by the continuous audit process, achieving an “always up-to-date” compliance status.

Implementation of CSA STAR™ Continuous

STAR™ Continuous introduces additional levels of assurance and transparency of the cloud security management system processes through more frequent testing. This provides CSPs a cost-effective way to better communicate the effectiveness of their security program and improve transparency to customers.

Learn more about CSA STAR™ Continuous

To learn more about STAR™ continuous download the [STAR Continuous Technical Guidance](#).