CSA STAR Level and Scheme Requirements
# Table of Contents

**Security, Trust, Assurance and Risk (STAR) .......................................................... 3**

Level 1: Self-Assessment .......................................................................................... 3
  - Variations of Level 1 .......................................................................................... 3
  - Security Self-Assessment .............................................................................. 3
  - GDPR Self-Assessment .................................................................................. 3

Level 2: Third-Party Audit ....................................................................................... 4
  - Variations of Level 2 ........................................................................................ 5
  - STAR Attestation: For SOC 2 .......................................................................... 5
  - STAR Certification: For ISO/IEC 27001:2013 .................................................. 5
  - C-STAR: For the Greater China Market ........................................................... 5
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.

Level 1: Self-Assessment

At level one organizations can submit one or both of the security and privacy self-assessments. For the security assessment, organizations use the Cloud Controls Matrix to evaluate and document their security controls. The privacy assessment submissions are based on the GDPR Code of Conduct.

Who should pursue level one?
Organizations should pursue this level if they are...

- Operating in a low-risk environment
- Wanting to offer increased transparency around the security controls they have in place
- Looking for a cost-effective way to improve trust and transparency

Variations of Level 1

Security Self-Assessment
CSA STAR Self-Assessment is a complimentary offering that documents the security controls provided by various cloud computing offerings, thereby helping users assess the security of cloud providers they currently use or are considering using. Cloud providers submit the Consensus Assessments Initiative Questionnaire (CAIQ) to document compliance with the Cloud Controls Matrix (CCM). This information then becomes publicly available, promoting industry transparency and providing
customer visibility into specific provider security practices. STAR Self-Assessments are updated annually.

**The CAIQ v4 has two versions:**

- **CCM + CAIQ v4:** The CAIQ v4 bundled with CCM here is intended to be used as a reference only. You cannot use the spreadsheet that contains both the CAIQ and CCM to submit to the registry.
- **STAR Level 1: Security Questionnaire (CAIQ v4):** Use this version of CAIQ v4 to fill out and submit to the STAR registry.

*Starting in July 2022 CSA will no longer be accepting CAIQ v3.1. You can learn more about the transition timeline from CAIQ v3.1 to v4 in [this blog](#).*

**GDPR Self-Assessment**

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

- **Code of Conduct Statement of Adherence**
- **PLA Code of Practice (CoP) Template - Annex 1** self-assessment results

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: Third-Party Audit**

Level 2 of STAR allows organizations to build off of other industry certifications and standards to make them specific for the cloud.

Organizations looking for a third-party audit can choose from one or more of the security and privacy audits and certifications. 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.
Which organizations should pursue level 2?
Organizations should pursue this level if they are...

- Operating in a medium to high risk environment
- Already hold or adhere to the following: ISO27001, SOC 2, GB/T 22080-2008, or GDPR
- Looking for a cost-effective way to increase assurance for cloud security and privacy

There are associated fees for STAR Level 2. CSA Corporate Members receive a price reduction on STAR Level 2 certifications and attestations.

Once you are ready to earn STAR Level 2, read the Code of Practice for Implementing STAR Level 2. This guide will explain both the practical steps as well as overall strategy you will need to implement to earn a STAR Certification or Attestation.

Variations of Level 2

STAR Attestation: For SOC 2
The CSA STAR Attestation is a collaboration between CSA and the AICPA to provide guidelines for CPAs to conduct SOC 2 engagements using criteria from the AICPA (Trust Service Principles, AT 101) and the CSA Cloud Controls Matrix. The STAR Attestation provides for rigorous third party independent assessments of cloud providers. Attestation listings will expire after one year unless updated. View approved assessment firms.

STAR Certification: For ISO/IEC 27001:2013
The CSA STAR Certification is a rigorous third-party independent assessment of the security of a cloud service provider. This technology-neutral certification leverages the requirements of the ISO/IEC 27001:2013 management system standard together with the CSA Cloud Controls Matrix. Certification certificates follow normal ISO/IEC 27001 protocol and expire after three years unless updated. View approved assessment firms.

C-STAR: For the Greater China Market
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. C-STAR leverages the requirements of the GB/T 22080-2008 management system standard together with the [CSA Cloud Controls Matrix](#), plus 29 related controls selected from GB/T 22239-2008 and GB/Z 28828-2012. Certification certificates expire after three years unless updated.

Submit to the Registry