The **CSA Security, Trust, Assurance, and Risk (STAR) program** is the largest cloud assurance program in the world that constitutes an ecosystem of the best practices, standards, technology, and auditing partners. STAR supports organizations to effectively and efficiently address how to define trust in the cloud, foster accountability, evaluate risk, measure assurance, and simplify compliance and procurement. Any organization operating or providing cloud services can benefit from completing the assessments in the STAR Assessment Portfolio.

### What is it?

The STAR Assessment Portfolio is a collection of globally-recognized cloud security and privacy assessments that can be completed by cloud service providers (CSPs). These assessments are based on the **Cloud Controls Matrix (CCM)** (the STAR program’s framework of essential cloud security policies, procedures, and technical measures), as well as the privacy requirements for GDPR compliance. The assessments fall under two levels of assurance: **STAR Level 1** (self-assessments) and **STAR Level 2** (third-party assessments).

### Why is it important?

The cloud industry consists of a vast array of service types and organizations. However, the one thing they all have in common is the need to instill trust in their customers, who are relying on these services to provide critical business functions. The STAR Assessment Portfolio provides a selection of top-tier security and privacy assessments that help instill customer trust. The Portfolio makes the process as convenient as possible for the CSP as well, who can choose which assessments to complete based on their own unique services, size, and maturity.

### How does it fit into the STAR program?

Assessments from the STAR Assessment Portfolio can be submitted to the **STAR Registry**, a publicly accessible repository of over 2,000 security and privacy assessments. Cloud customers can use the STAR Registry to find a cloud service with the right security and privacy posture for their organization.
What’s the difference between Level 1 and Level 2?

**STAR Level 1** consists of self-assessments. These are complimentary offerings that cloud providers fill out themselves to document security controls. You should pursue Level 1 if you operate in a low-risk environment and are looking for a cost-effective way to improve trust and transparency.

**STAR Level 2** consists of third-party assessments that must be conducted by certified STAR auditors. Therefore, there are associated fees for Level 2. CSA Corporate Members receive a price reduction. STAR Level 1 is a prerequisite for Level 2. You should pursue Level 2 if you operate in a medium to high-risk environment and are looking for a cost-effective way to increase assurance for cloud security and privacy.

Organizations that have completed either level may be eligible for the Trusted Cloud Provider designation if other select criteria are met.

How does it benefit me?

The STAR Assessment Portfolio benefits both CSPs and their customers by:

- Providing a simple way for CSPs to demonstrate their values of transparency, accountability, and top-tier security.
- Allowing CSPs to choose the level of assurance that will work best for them.
- Enabling customers to easily confirm the continued compliance of their CSP.
- Increasing transparency of the expected shared security responsibilities between CSPs and cloud customers.
- Eliminating the need for CSPs to complete multiple customer questionnaires.

What happens when my assessment is posted to the STAR Registry?

After you submit your assessment and it is posted to the STAR Registry, customers can download it to learn more about your security posture. Potential customers also use the Registry as a “shopping mall” of cloud services and may discover that your service meets their needs.

Learn More

Learn more about the STAR Assessment Portfolio and how to submit to the STAR Registry.