CSA cloud security alliance

CSA Security, Trust and Assurance Registry (STAR)

Whether you use cloud services, provide cloud services, or attest/certify cloud services, you have a vested interest in knowing more about cloud security practices from an objective, third-party source. You need the right tools to ensure you are playing your part in securing the cloud ecosystem—because when everyone in the cloud universe works together to ensure a secure environment, everyone wins.

Each stakeholder gains individual benefit by using CSA STAR, but perhaps the "greater good" is the combined contribution to a secure cloud ecosystem via encouragement of a more consistent level of good security practices.

cloudsecurityalliance.org/star/registry

STAR

CSA Security, Trust and Assurance Registry (STAR)

Cloud is the future of IT

In a future where computing is dominated by the cloud, no one—users, providers, assessors—can afford a cloud ecosystem that is not secure. Yet each cloud stakeholders has a different role to play in ensuring security. More and more, stakeholders are looking to the CSA STAR as their source.

What do stakeholders find in STAR?

- **Users of cloud services** get a clear view of cloud provider security practices, accelerating their due diligence and leading to higher quality procurement experiences. The searchable registry provides detailed information on the security posture of cloud providers, as measured against CSA's globally tested Cloud Controls Matrix (CCM), the only meta-framework of cloud-specific security controls, mapped to leading standards, best practices and regulations. Users can take it even one step further, and utilize these best practices for their own cloud security programs or certification.

- **Cloud service providers** find tools that can help them build a security program, assess their own security and a venue to educate potential clients on their good practices. Being able to provide assurance to clients that their valuable data will be protected is a powerful marketplace differentiator.

- **IT auditors** and firms that are in the business of providing audit, attestation or certification services gain access to guidance that enables them to build on existing reporting/standards (SOC 2, ISO/IEC 27001) with a cloud-specific overlay. The STAR's harmonized approach to cloud-specific security assurance extends a valuable competitive advantage.

What is the CSA STAR program?

CSA STAR is the industry's most powerful program for assurance in the cloud, encompassing key principles of transparency, rigorous auditing and harmonization of standards.

The searchable registry is based on two levels of assurance, consisting of three unique offerings (with a third level in development). All levels are based on CSA's succinct yet comprehensive list of cloud-centric control objectives defined in the CCM.

LEVEL ONE: CSA STAR Self-Assessment

A free offering that documents the security controls provided by cloud computing providers. This information, which is supplied by cloud providers, can be submitted in one of two formats: (1) A completed Consensus Assessments Initiative Questionnaire (CAIQ), a series of yes/no control assertion questions based on the CCM, which can be tailored to suit each unique cloud customer's evidentiary requirements, or (2) a report documenting compliance with CCM.

LEVEL TWO

Level two of the CSA STAR program comprises two offerings: attestation and certification. In each case, the STAR offering uses the CSA CCM to align with and complement an existing standard or reporting criteria. This enables the individual or firm offering the attestation/certification service to accomplish a streamlined "two-for-one" outcome: They fulfill the requirements of the existing standard or criteria, while adding cloud-specific content. Attestation and certification services can be time-consuming and costly; STAR's level two offerings help make the most of both valuable resources.

> *The European Commission, in a call for tender that aims to secure cloud services for a number of EU Institutions (European Parliament, Council and other EU institutions and agencies), makes explicit reference to the CSA STAR program and requests the candidate tenders to make use of the program to show compliance with security requirements established by the European Security Agency (ENISA).*
>
> —Directorate-General for Informatics, Call for Tender

CSA STAR Attestation

Provides guidelines for Certified Public Accountants (CPAs) to conduct SOC 2 engagements using criteria from the American Institute of Certified Public Accountants (AICPA) and the CSA CCM. Created as a collaborative effort between CSA and AIPCA, STAR Attestation couples traditional SOC 2 reporting with cloud-specific content to result in a rigorous, independent assessment of a service provider's system and controls, including a description of the service auditor's tests of controls.

CSA STAR Certification

A technology-neutral certification that leverages the requirements of ISO/IEC 27001, "Information security management," together with the CCM. The program evaluates the efficiency of an organization's information security management system (ISMS); ensures the scope, processes and objectives are fit for purpose; and helps cloud providers define and prioritize areas for improvement. It enables the auditor to assess a company's performance on long-term sustainability and risks, allowing senior management to quantify and measure improvement year on year. Certified organizations are listed on the CSA STAR Registry as "STAR Certified."

Get started with CSA STAR

Get the CSA STAR Watch SaaS App: https://cloudsecurityalliance.org/star/watch

Search the registry for current cloud provider listings: https://cloudsecurityalliance.org/star/registry

Take the first step towards Self-Assessment, Attestation or Certification: https://cloudsecurityalliance.org/star/overview

General Inquiries: star-help@cloudsecurityalliance.org

Future Developments

CSA continues to enhance the STAR program to address the varied needs of cloud trust around the world and encourage provider transparency, global harmonization of requirements and real-time cloud security assurance.

A few samples of CSA's commitment to continued enhancement include:

- CSA is a key contributor of cloud security best practices to international standards development organizations and will provide the industry's primary mechanism for incorporation of new standards into cloud assurance via CSA STAR. CSA is currently in the process of including ISO 27018, "Code of practice for protection of PII," as well as the pending ISO 27017, "Code of practice for information security controls for cloud services.

- In conjunction with the Chinese government organization CEPREI, CSA is co-developing a new level two offering to provide a cloud security certification based upon the CSA CCM and Chinese national standard GB/T 22080.

- CSA is currently developing a level three capability, which will consist of specifications for continuous monitoring that enables automation in the real-time exchange of information regarding cloud provider compliance with CSA best practices. Providers will 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. It is scheduled for release in 2015.

- Also in 2015, CSA will release CSA STAR Watch, our Software as a Service (SaaS) app to help organizations manage compliance with CSA STAR security requirements. It will present CCM and CAIQ content in a mobile-friendly way, to facilitate attestation work by using a database, rather than a spreadsheet, for such traditional activities as sharing information, delegating tasks and tracking workflow. Whether a cloud provider, consumer or auditor, CSA STAR Watch will help any organization with the means to track the security of any cloud, public or private.

About CSA

The Cloud Security Alliance is the world's leading organization dedicated to defining and raising awareness of best practices to help ensure a secure cloud computing environment. CSA harnesses the subject matter expertise of industry practitioners, associations, governments, and its corporate and individual members to offer cloud security-specific research, education, certification, events and products. CSA's activities, knowledge and extensive network benefit the entire community impacted by cloud—from providers and customers, to governments, entrepreneurs and the assurance industry—and provide a forum through which diverse parties can work together to create and maintain a trusted cloud ecosystem.

CSA Milestones

- Not-for-profit association, launched in April 2009
- Issued the first comprehensive best practices for secure cloud computing, "Security Guidance for Critical Areas of Focus for Cloud Computing"
- Created the first and only user credential for cloud security, the Certificate of Cloud Security Knowledge (CCSK), named the top cloud computing certification by CIO.com only three years after its introduction
- Created and maintains the Cloud Controls Matrix (CCM), the world's only meta-framework of cloud-specific security controls, mapped to leading standards, best practices and regulations
- Maintains a registry of cloud provider security practices, the CSA Security, Trust and Assurance Registry (STAR), and offers certification and attestation tools based on existing requirements and standards, customized to address the cloud

CSA cloud security alliance®

Cloud Security Alliance
www.cloudsecurityalliance.org
info@cloudsecurityalliance.org