

CSA STAR (CCM v4.0.1)

CSA STAR is a cloud security assurance program helping organizations assess and demonstrate cloud security and compliance.



What it is

CSA STAR (Security, Trust, Assurance, and Risk) is a cloud security assurance program that helps organizations assess and demonstrate the security and compliance posture of cloud services. The program establishes a comprehensive framework for evaluating cloud providers against a broad range of cybersecurity, risk management, and data protection controls.

Published by the Cloud Security Alliance (CSA), CSA STAR is widely used by cloud service providers, customers, and assessors to address requirements related to data security, privacy governance, operational resilience, and regulatory compliance in cloud environments. The framework works in conjunction with the CSA Cloud Controls Matrix (CCM) and aligns with industry standards such as ISO 27001 and NIST frameworks.

At a glance

PUBLISHER Cloud Security Alliance (CSA)	TYPE Certification / Assurance Program	VERSION Current CSA STAR Program
EFFECTIVE 2013	DOMAIN Cloud Security	FAMILY CSA STAR
REGION United States	INDUSTRY Cloud & Technology Providers	ADOPTION MODEL Risk Management
IMPLEMENTATION COMPLEXITY High		

Source: <https://cloudsecurityalliance.org/star>

Why it matters

- **Strengthen security governance** Establish a clear structure for managing responsibilities, monitoring security controls, and ensuring continuous improvement in cloud environments.
- **Enhance regulatory alignment** Map controls to industry standards and regulations, supporting compliance with local, international, and industry-specific requirements.
- **Increase audit transparency** Facilitate self-assessments and third-party validations, enabling organizations to share verified security information with customers and stakeholders.
- **Improve risk management capabilities** Identify, assess, and mitigate risks associated with cloud usage, supporting informed decision-making and prioritization of security investments.

How SmartSuite supports CSA STAR

CCM-to-STAR Mapping Structure

Map CCM controls to STAR requirements with clear ownership and evidence.

Provider Assurance Artifact Repository

Centralize policies, reports, and technical proof used for STAR submissions.

Customer Questionnaire Response Workflow

Standardize responses and attach reusable evidence to reduce repeat work.

Findings and Remediation Tracking

Manage gaps, corrective actions, and closure evidence to strengthen assurance.

Renewal Cadence and Continuous Improvement

Track renewals, recurring reviews, and program improvements over time.

Submission Readiness Reporting

Report submission readiness, open issues, and evidence coverage for stakeholders.

Common framework mappings

- ISO 27001:2022
- ISO 27017
- ISO 27018
- ISO 27701
- NIST CSF 2.0
- NIST 800-53 Rev.5
- SOC 2

Official resources

CSA STAR Self-Assessment

Provides a structured format for cloud providers to document security controls implementation.

cloudsecurityalliance.org/star/self-assessment

CSA STAR Certification

Outlines the third-party certification process for evaluating cloud service providers.

cloudsecurityalliance.org/star/certification

CSA Cloud Controls Matrix (CCM)

Defines a controls framework aligned with CSA STAR requirements and standards.

cloudsecurityalliance.org/research/cloud-controls-matrix

CSA STAR Program Overview

Describes the structure and benefits of participating in the CSA STAR assurance program.

cloudsecurityalliance.org/star

Frequently asked questions

What is CSA STAR used for?

CSA STAR is used to assess, validate, and demonstrate the security and compliance posture of cloud service providers. It provides a structured methodology for evaluating cloud controls and facilitating trust between providers, customers, and third-party assessors.

Is CSA STAR certification mandatory?

CSA STAR certification is not mandatory but is increasingly requested by customers and regulators as part of supplier due diligence and cloud risk management. Organizations may choose between self-assessment and independent third-party certification depending on their compliance needs and market demands.

What is the scope of CSA STAR and who should use it?

CSA STAR applies to cloud service providers and organizations seeking to evaluate or assure cloud security practices. It covers a broad range of security domains including data protection, privacy, governance, and operational resilience across all cloud deployment models.

What are the key components or artifacts of CSA STAR?

Key artifacts include the Cloud Controls Matrix (CCM), which lists required controls, the Consensus Assessments Initiative Questionnaire (CAIQ) for self-assessment, and entries within the CSA STAR Registry. These facilitate structured assessment and transparent reporting of cloud security practices.

How does CSA STAR implementation work in practice?

Organizations implement CSA STAR by mapping their cloud security controls to the CCM, completing the CAIQ for self-assessment, and pursuing third-party audits if seeking higher assurance levels. Continuous control monitoring, regular risk assessments, and evidence collection are integral to ongoing program maintenance.

How does CSA STAR relate to other frameworks like ISO 27001 or NIST?

CSA STAR is designed to align with industry standards such as ISO 27001 and NIST by mapping CCM controls to these frameworks. This approach allows organizations to leverage their existing compliance efforts and streamline cloud-specific reporting and assessments.

What are the ongoing compliance requirements for CSA STAR?

Ongoing compliance involves periodically reviewing control effectiveness, updating risk assessments, maintaining accurate CAIQ documentation, and addressing identified gaps. Third-party certifications typically require annual surveillance or recertification to ensure continual adherence to evolving standards.

How would SmartSuite support CSA STAR?

SmartSuite supports CSA STAR by providing control libraries mapped to CCM, risk register management, and automated evidence collection processes. The platform facilitates CAIQ completion, tracks audit artifacts, and enables remediation workflows, audit readiness, and real-time compliance reporting for regulatory and executive oversight.

License included / downloadable: Yes CSA STAR program documentation and registry information are publicly available through the Cloud Security Alliance.

Full framework page and mappings: smartsuite.com/frameworks/csa-star-security-trust-assurance-risk-program