cloud security alliance℠

Cloud Security Alliance (CSA) STAR Attestation

Azure and Intune were awarded the Cloud Security Alliance STAR Attestation based on an independent audit.

Microsoft and CSA STAR Attestation

Microsoft Azure, Microsoft Azure Government, and Microsoft Intune have been awarded CSA STAR Attestation. The STAR Attestation provides an auditor's findings on the design suitability and operating effectiveness of SOC 2 controls in Microsoft cloud services.

Microsoft in-scope cloud services

- Azure and Azure Government
  Learn more
- Intune

Audits, reports, and certificates

- Azure CSA STAR Attestation

How to implement

- **Azure responses to the CSA CAIQ**
  Get an understanding of how Azure meets the requirements set forth by the CSA.
  Learn more

About CSA STAR Attestation

The Cloud Security Alliance (CSA) maintains the CSA Security, Trust & Assurance Registry (STAR), a free, publicly accessible registry where cloud service providers (CSPs) can publish their CSA-related assessments. STAR consists of three levels of assurance aligned with control objectives in the CSA Cloud Controls Matrix (CCM). (The CCM covers fundamental security principles across 16 domains to help cloud customers assess the overall security risk of a cloud service.)

- Level 1: STAR Self-Assessment
- Level 2: STAR Attestation, STAR Certification, and C-STAR Assessment (which are based on audits by third parties)
- Level 3: STAR Continuous Monitoring (program requirements are still under development by CSA)

STAR Attestation involves a rigorous independent audit of a cloud provider's security posture based on a SOC 2 Type 2 audit in combination with CCM criteria. The independent auditor that evaluates a cloud provider's offerings for STAR Attestation must be a certified public accountant (CPA) and is required to have the CSA Certificate in Cloud Security Knowledge (CCSK).

A SOC 2 Type 2 audit is based on American Institute of Certified Public Accountants (AICPA) Trust Services Principles and Criteria, including security, availability, confidentiality, and processing integrity, and the requirements set forth in the CCM.

Frequently asked questions

Which industry standards does the CSA CCM align with?

The CCM corresponds to industry-accepted security standards, regulations, and control frameworks such as ISO/IEC 27001, PCI DSS, HIPAA, AICPA SOC 2, NERC CIP, FedRAMP, NIST, and many more. To get the current list, go to the Cloud Controls Matrix Working Group page, and click **Cloud Control Matrix v3.0.1.**

Which CSA STAR levels of assurance have Microsoft business cloud services attained?

- Level 1: CSA STAR Self-Assessment: Azure, Dynamics 365, and Office 365.
  The Self-Assessment is a complimentary offering from cloud service providers to document their security controls to help customers assess the security of the service.
- Level 2: CSA STAR Certification: includes Azure, Cloud App Security, Intune, and Power BI.
  STAR Certification is based on achieving ISO/IEC 27001 certification and meeting criteria specified in the CCM. It is awarded after a rigorous third-party assessment of the security controls and practices of a cloud service provider.
- Level 2: CSA STAR Attestation: Azure, Azure Government, and Intune.
  CSA and the American Institute of Certified Public Accountants (AICPA) has collaborated to provide guidelines for CPAs to use in conducting SOC 2 engagements, using criteria from the AICPA (Trust Service Principles, AT 101) and the CSA CCM. STAR Attestation is based on these guidelines and is awarded after rigorous independent assessments of cloud providers.

Additional resources

- Azure standard response for request for information
- Microsoft and SOC 1, 2, and 3 Reports