

CSA Cloud Controls Matrix (CCM) v4

The CSA Cloud Controls Matrix v4 is a cloud security control framework of 17 domains, mapped to ISO/IEC 27001, NIST SP 800-53, PCI DSS, CIS Controls, and SOC 2.



What it is

The CSA Cloud Controls Matrix (CCM) v4 is a cybersecurity control framework built specifically for cloud computing. Its current release, CCM v4.1, defines control objectives across 17 security domains and pairs each control with implementation guidance, auditing guidance, a shared-responsibility view for IaaS, PaaS, and SaaS, and a companion questionnaire, the Consensus Assessments Initiative Questionnaire (CAIQ).

The Cloud Security Alliance (CSA), a nonprofit industry association, publishes and maintains the CCM through its CCM Working Group. The framework is voluntary: cloud service providers use it to document their security posture, and cloud customers, auditors, and procurement teams use it to evaluate providers. It is also the control basis for the CSA STAR assurance program, where CAIQ submissions and third-party certifications are published in the STAR Registry.

At a glance

PUBLISHER Cloud Security Alliance (CSA)	TYPE Control Framework	VERSION 4.1
EFFECTIVE January 27, 2026	DOMAIN Cloud Security	FAMILY CSA STAR
REGION International	INDUSTRY Cloud & Technology Providers	ADOPTION MODEL Voluntary
IMPLEMENTATION COMPLEXITY Medium		

Source: <https://cloudsecurityalliance.org/research/cloud-controls-matrix>

Why it matters

- **Cloud-specific control coverage** Addresses cloud concerns such as virtualization, container security, key management, interoperability, and supply chain that generic catalogs treat only indirectly.
- **Clear shared responsibility** Each control indicates whether the cloud provider, the customer, or both are responsible, so ownership is settled before an assessment begins.
- **Reduced compliance fatigue** CSA publishes mappings to ISO/IEC 27001, NIST SP 800-53, PCI DSS, CIS Controls, AICPA TSC, and the NIST Cybersecurity Framework, letting one set of evidence serve many obligations.
- **Recognized assurance path** The CCM is the control basis for CSA STAR, so implementing it prepares a provider for a STAR Level 1 self-assessment or a STAR Level 2 certification or attestation.

How SmartSuite supports CSA CCM v4

CCM Control Library

Load the 17 CCM domains and their controls with implementation and auditing guidance attached to each record.

Ownership, Cadence, and Accountability

Assign a control owner and review schedule for every control and flag shared-responsibility items that depend on the cloud provider.

Evidence Collection and Audit Trail

Store evidence against each control with timestamps and reviewers so CAIQ answers and STAR submissions are backed by records.

Control Testing and Metrics

Plan tests against the CCM auditing guidelines and track continuous auditing metrics over time.

Cross-Framework Mapping

Link each CCM control to its ISO/IEC 27001, NIST SP 800-53, PCI DSS, and SOC 2 equivalents so one piece of evidence satisfies several frameworks.

STAR-Ready Reporting

Report CAIQ completeness, open gaps, and remediation status for customers, auditors, and leadership.

Common framework mappings

ISO 27001:2022

ISO 27002:2022

ISO 27017

ISO 27018

NIST 800-53 Rev.5

NIST CSF 2.0

PCI DSS 4.0.1

SOC 2 (AICPA TSC 2017)

CIS Controls v8.1

CSA STAR

Official resources

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

CSA CCM and CAIQ v4.1 Download

Official CSA artifact page for the CCM v4.1 bundle: controls, CAIQ, implementation and auditing guidelines, and metrics catalog.

cloudsecurityalliance.org/artifacts/cloud-controls-matrix-v4-1

CSA CCM Machine-Readable Bundle

JSON, YAML, and OSCAL editions of the Cloud Controls Matrix for loading into compliance tooling.

cloudsecurityalliance.org/artifacts/ccm-machine-readable-bundle-json-yaml-oscal

Frequently asked questions

What is the CSA Cloud Controls Matrix (CCM)?

The CSA Cloud Controls Matrix is a cybersecurity control framework for cloud computing published by the Cloud Security Alliance. Version 4 organizes control objectives into 17 security domains and pairs each control with implementation guidelines, auditing guidelines, and a shared-responsibility view for IaaS, PaaS, and SaaS. It is the control basis for the CSA STAR assurance program.

What is new in CCM v4.1?

CCM v4.1, released on January 27, 2026, combines the CCM and the CAIQ into a single bundle and refines the control set within the same 17 domains. The release adds a continuous auditing metrics catalog, a code of practice for implementing and maintaining key metrics, introductory guidance on the Shared Security Responsibility Model, and a change analysis against v4.0.3.

How does the CCM relate to the CAIQ and CSA STAR?

The Consensus Assessments Initiative Questionnaire restates every CCM control as yes/no questions that a cloud provider answers to document its security posture. A completed CAIQ is the basis of a CSA STAR Level 1 self-assessment, and STAR Level 2 certification or attestation is a third-party audit against the CCM combined with ISO/IEC 27001 or SOC 2. Results are published in the public STAR Registry.

Which frameworks does CCM v4 map to?

The Cloud Security Alliance publishes mappings from CCM v4 to ISO/IEC 27001, 27002, 27017, and 27018, NIST SP 800-53 Rev. 5, the NIST Cybersecurity Framework, PCI DSS, CIS Controls v8, the AICPA Trust Services Criteria used in SOC 2, the ISF Standard of Good Practice, and CCM v3.0.1. These mappings let organizations reuse evidence across frameworks and reduce duplicate assessment work.

Is the CSA CCM free to use?

Yes for internal use. The CCM and CAIQ v4.1 bundle, including the implementation and auditing guidelines and the machine-readable JSON, YAML, and OSCAL editions, can be downloaded from the Cloud Security Alliance at no cost. Organizations that want to customize the CCM, embed it in a product, or use it in consulting services need a commercial license from CSA.

Who should use the Cloud Controls Matrix?

Cloud service providers use the CCM to structure and assure their security programs, cloud customers use it to evaluate providers and define their own responsibilities, and auditors and consultants use it as an assessment baseline. Because it is sector-neutral and mapped to major standards, it suits any organization that provides, procures, or governs cloud services.

How would SmartSuite support CSA CCM v4?

SmartSuite lets teams load the 17 CCM domains as a control library, assign owners and review cadences, and attach evidence and test results to each control. Cross-framework mappings link CCM controls to their ISO/IEC 27001, NIST SP 800-53, PCI DSS, and SOC 2 equivalents, and dashboards track CAIQ completeness and open gaps ahead of a STAR submission.

License included / downloadable: Yes The CCM v4.1 bundle, including the CAIQ, implementation guidelines, auditing guidelines, and mappings, is downloadable free of charge from the Cloud Security Alliance for internal use; commercial use requires a CSA license, and the text is not bundled with the platform.

Full framework page and mappings: smartsuite.com/frameworks/csa-cloud-controls-matrix-ccm-v4