

# Guide to the CCM and CAIQ

## Understanding the Key Components and their Applications

The [Cloud Controls Matrix \(CCM\) and CAIQ v4](#) is your comprehensive resource for implementing and assessing cloud security. This guide explains the components in the download file, their purpose, and how to use them. Whether you're new to the CCM and CAIQ or looking to maximize its potential, this guide will help you navigate and utilize these critical resources.

### What's included in the download?

The CCM and CAIQ v4 download includes eight key components:

- [CCM v4 Controls](#)
- [Mappings](#)
- [CAIQ v4](#)
- [Implementation Guidelines](#)
- [Auditing Guidelines](#)
- [CCM Metrics](#)
- [STAR Level 1: Security Questionnaire \(CAIQ v4\)](#)

Explore the purpose, use cases, and practical applications of each component:

## CCM v4 Controls

The CCM is a comprehensive cybersecurity control framework developed to provide a set of structured and standardized controls that address security and privacy concerns associated with cloud computing. It helps organizations assess and manage risks related to the adoption of cloud services.

It is composed of 197 control objectives that are structured in 17 domains covering all key aspects of cloud technology. It can be used as a tool for the systematic assessment of a cloud implementation, and provides guidance on which security controls should be implemented by which actor within the cloud supply chain. The controls framework is aligned to the [CSA Security Guidance for Cloud Computing](#), and is considered a de-facto standard for cloud security assurance and compliance.

## Mappings

Mappings serve to identify the equivalence, gaps, and misalignment between the control specifications of the CCM V4 and other standards, allowing for more streamlined compliance. Cloud organizations can leverage this mapping to derive numerous [key benefits](#), enhancing their cloud security and compliance programs.

Mappings of CCM v4 to other standards currently available include but are not limited to: ISO/IEC 27001/27002/27017/27018, AICPA TSC , CIS Controls, NIST CSF, NIST 800-53, PCI DSS and others.

## CAIQ v4

The Consensus Assessment Initiative Questionnaire (CAIQ) provides cloud customers and auditors with questions for CSPs about security posture, adherence to CSA best practices (CCM and the CSA Security Guidance) and customer SSRM responsibilities. While the CCM defines the control specification and implementation guidelines, the CAIQ defines questions to evaluate and inform implementation.

This version cannot be used to submit to STAR and is just for reference.

## Implementation Guidelines

This document will help you understand how to navigate the [Cloud Controls Matrix v4](#), use it effectively and interpret and implement the CCM control specifications. The document's main goal is to support the implementation of CCM controls and provide recommendations on how that can be properly achieved per CCM control specification.

The CCM Implementation guidelines are a collaborative product created from volunteering subject matter experts within the [CCM Working Group](#). It is based on the shared experiences of both cloud providers and cloud customers in implementing and securing cloud services when leveraging the CCM controls in alignment with the Shared Security Responsibility Model.

The guidelines are also available in a [spreadsheet format](#), where they can be leveraged alongside the rest of the CCMv4 components.

## Auditing Guidelines

The auditing guidelines aim to facilitate and guide a CCM audit. Auditors are provided with a set of assessment guidelines per CCM v4.0 control specification with an objective to improve the controls' auditability and help organizations to more efficiently meet compliance (by conducting either internal or external 3rd party cloud security audits).

### Key Takeaways:

- What the different CCM audit areas are
- How to perform a CCM-related audit and assessment of organizations of any size, business, cloud deployment complexity, or maturity

The auditing guidelines are not exhaustive or prescriptive by nature. Rather, they represent a generic guide through recommendations for assessment. Auditors must customize the descriptions, procedures, risks, controls, and documentation. These elements must conform to organizational- specific audit work programs and service(s) in the scope of the assessment to address the specific audit objectives.

## CCM Metrics

A metric is a standard for measurement that defines the rules for performing the measurement and understanding the results of a measurement (ISO/IEC 19086-1). In the context of cloud computing, there is a growing interest in defining metrics that can be used to evaluate the security of an information system, potentially in real-time.

The [Continuous Audit Metrics Catalog](#) is the product of the work conducted by industry experts in the CSA [Continuous Audit Metrics Working Group](#). The catalog does not aim to be exhaustive or complete; this release aims to offer support for those organizations seeking for a more systematic evaluation of the efficiency and effectiveness of the CCM controls implementation.

The proposed metrics aim to support internal CSP governance, risk, and compliance (GRC) activities and provide a helpful baseline for service-level agreement transparency. Additionally, these metrics might be integrated within the STAR Program in the future, providing a foundation for continuous certification.

## STAR Level 1: Security Questionnaire (CAIQ v4)

The STAR Level 1: Security Questionnaire (CAIQ v4) offers an industry-accepted way to document what security controls exist in IaaS, PaaS, and SaaS services, providing security control transparency. It provides a set of Yes/No questions a cloud consumer and cloud auditor may wish to ask of a cloud provider to ascertain their compliance to the Cloud Controls Matrix (CCM). Therefore, it helps cloud customers to gauge the security posture of prospective cloud service providers and determine if their cloud services are suitably secure.

The STAR Level 1: Security Questionnaire (CAIQ v4) is what individuals will need to use to submit to the [STAR Registry](#), and includes all the necessary features of CAIQ v4. You can read more about the updates made to CAIQ v4 in [this blog](#).

CSA also offers Valid-AI-ted, an optional, AI-powered enhancement to STAR Level 1. The service automatically evaluates CAIQ v4 submissions, delivering objective scoring, detailed feedback, and faster time to listing. Organizations who pass receive a Valid-AI-ted badge on the STAR Registry. Learn more about Valid-AI-ted [here](#).

---

## Related Resources

### Valid-AI-ted: AI-Powered STAR Level 1 Validation

- An optional service that uses AI to validate STAR Level 1 CAIQ v4 submissions. Organizations receive near-instant feedback and guidance—plus a Valid-AI-ted badge on the [STAR Registry](#) upon passing. Learn more about Valid-AI-ted [here](#).

### Download the CCM Machine Readable (JSON/YAML/OSCAL) Format

- CSA provides a [machine-readable format](#) of the CCM Controls, CAIQ Security Questionnaire, Implementation Guidelines (both JSON/YAML and OSCAL) and Mappings (JSON/YAML) to support organizations that would like to foster CCM automation.

### Get Listed in the STAR Registry

- Showcase your organization's commitment to cloud security by [getting listed in the CSA STAR Registry](#). Build trust and transparency with your customers by demonstrating your alignment with the CCM.

### CCM Deep Dive Video Series

- Gain expert insights into each of the 17 CCM v4 domains with our comprehensive video series. Explore practical guidance to strengthen your cloud security implementation and access the [free videos here](#).

---

**Your input on the CCM is important to use—share your feedback by completing [this form](#). For any questions regarding the CSA STAR Program, please reach out to us [here](#).**