Consensus Assessments Initiative Questionnaire v3.0.1

Info Sheet

CAIQv3.0.1™

https://cloudsecurityalliance.org/research/cai/

Welcome to the Latest Version of the Consensus Assessments Initiative Questionnaire, CAIQ v3.0.1!

ABOUT THE CSA CLOUD QUESTIONNAIRE

The Consensus Assessments Initiative Questionnaire (CAIQ) is a set of questions a cloud consumer and cloud auditor may wish to ask of a cloud provider. It provides a series of "yes or no" control assertion questions which can then be tailored to suit each unique cloud customer's evidentiary requirements. The questions are based off of security controls found in the CSA Cloud Controls Matrix (CCM), a code of practice focused on providing industry-accepted ways to document what security controls exist in IaaS, PaaS, and SaaS offerings and providing security control transparency around them. CAIQ, by design, is a questionnaire integrated with and to support other projects from our research partners.

The CAIQ is meant to be a companion to the CSA Guidance and the CSA Cloud Controls Matrix (CCM), and these documents should be used together. The question set is a simplified distillation of the issues, best practices, and control specifications from our Guidance and CCM, intended to help organizations build the necessary assessment processes for engaging with cloud providers. The Consensus Assessments Initiative is part of the CSA GRC Stack.

- A simplified distillation of the issues, best practices, and control specifications
- Companion to the CSA Guidance and CSA Cloud Controls Matrix (CCM) v3.0.1
- Helps organizations build the necessary assessment processes for engaging with cloud providers
- Helps cloud providers assess their own security posture
- Part of the CSA GRC Stack

WHAT'S NEW IN THIS VERSION!

- Realigns the CAIQ questions to CCM v3.0.1 control domains and the Cloud Security Alliance "Security Guidance for Critical Areas of Focus in Cloud Computing V3.0"
- Maps the CAIQ questions to the latest compliance regulations found in the CCM v3.0.1
- Updated questions for clarity of intent, STAR enablement, and SDO alignment

Consensus Assessments Initiative Questionnaire v3.0.1

Quick Stats

FOR MORE INFORMATION:
https://cloudsecurityalliance.org/research/cai
cai-leadership@cloudsecurityalliance.org

Now in its third version, the **Cloud Assessments Initiative (CAI) Questionnaire** was developed by the Consensus Assessments Initiative Working Group with contributions from over 50 security professionals and industry experts. An additional open review period helped further build these necessary assessment processes for engaging with cloud providers.

CAIQ v3.0.1, available in spreadsheet form, is now color coded to match the CCM v3.0.1 domains for easy review.

CONTROL SPECIFICATION NUMBERING UPDATES

- **BCR-10** (Business Continuity Management & Operational - *Resilience Management Program*) has been removed and consolidated in **BCR-01**.
- **BCR-11** (Business Continuity Management & Operational - *Resilience Policy*) has been moved to the **BCR-10** Control Domain.
- **BCR-12** (Business Continuity Management & Operational - *Resilience Retention Policy*) has been moved to the **BCR-11** Control Domain.
- **DSI-05** (Data Security & Information Lifecycle Management - *Information Leakage*) has been removed since data loss/leakage is covered in other contols such as **GRM-02**, **GRM-04**, and **DCS-08**.
- **DSI-06** (Data Security & Information Lifecycle Management - *Non-Production Data*) has been moved to the **DSI-05** Control Domain.
- **DSI-07** (Data Security & Information Lifecycle Management - *Ownership / Stewardship*) has been moved to the **DSI-06** Control Domain.
- **DSI-08** (Data Security & Information Lifecycle Management - *Secure Disposal*) has been moved to the **DSI-07** Control Domain.
- **GRM-12** (Governance and Risk Management - *Risk Management Framework*) has been removed, as it was addressed in **GRM-11**.
- **HRS-05** (Human Resources - *Industry Knowledge / Benchmarking*) has been removed and assumed as regular practices.
- **HRS-06** (Human Resources - *Mobile Device Management*) has been moved to the **HRS-05** Control Domain.
- **HRS-07** (Human Resources - *Non-Disclosure Agreements*) has been moved to the **HRS-06** Control Domain.
- **HRS-08** (Human Resources - *Roles / Responsibilities*) has been moved to the **HRS-07** Control Domain.
- **HRS-09** (Human Resources - *Technology Acceptable Use*) has been moved to the **HRS-08** Control Domain.
- **HRS-10** (Human Resources - *Training / Awareness*) has been moved to the **HRS-09** Control Domain.
- **HRS-11** (Human Resources - *User Responsibility*) has been moved to the **HRS-10** Control Domain.
- **HRS-12** (Human Resources - *Workspace*) has been moved to the **HRS-11** Control Domain.
- **IVS-13** (Infrastructure & Virtualization Security - *Network Architecture*) has been added. This domain has been split off from the **IVS-06** Control Domain.