CAIQ™ CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v4.0.2

Introduction

Consensus Assessments Initiative Questionnaire (CAIQ):

This tab includes the questionnaire associated with the Cloud Control Matrix (CCM) controls, commonly known as the CAIQ.

The Consensus Assessments Initiative Questionnaire version 4 (or CAIQv4.0.2) aligns with the CCMv4.0.2 control specifications. The CAIQv4.0.2's purpose is to help organizations conduct self-assessments to test their compliance against the CCM V4. It is developed under CSA's STAR-Level 1 program umbrella, allowing organizations to complete and submit self-assessments to CSA's STAR Registry.

The CAIQv4.0.2 features 261 questions structured and formulated based on the 17 domains and underlying control specifications of the CCM.

Each question is described using the following attributes:

Question ID

The question identifiers.

Assessment Question

The description of the question.

In addition, this tab includes the following sections (groups of columns).

CSP CAIQ Answer

The Cloud Service Provider (CSP) must respond with "Yes"/ "No"/ "NA" next to the corresponding assessment question, and for the portion(s) of the CCM control specification they are responsible and accountable for implementing.

Meaning of possible replies:

• "Yes": The portion(s) of the CCM control requirement corresponding to the assessment question is met.

• "No": The portion(s) of the CCM control requirement corresponding to the assessment question is not met.

• "N/A": The question is not in scope and does not apply to the cloud service under assessment.

NOTES:

A "Yes" answer indicates that the portion of the control in question is implemented. The CSP indicates the responsible and accountable parties (SSRM control ownership), and optionally elaborates on the implementation "how-to" per relevant party CSP and/or CSC.

A "No" answer indicates that the portion of the control in question is not implemented, while in scope of the assessment. The CSP has to assign the implementation responsibility of the control to the relevant party under column "SSRM control ownership", and optionally elaborate on the "why" (has not been implemented), and "what" has to be done for its implementation by that party.

A "N/A" answer indicates that the portion of the control in question is out of scope of the assessment. The "SSRM control ownership" column is to be left blank (e.g., greyed out), and optionally the CSP may explain why it is the case ("CSP Implementation Description").

Shared Security Responsibility Model (SSRM) control ownership

The CSP control responses shall identify control applicability and ownership for their specific service.

• CSP-owned: The CSP is entirely responsible and accountable for the CCM control implementation.

• CSC-owned: The Cloud Service Customer (CSC) is entirely responsible and accountable for the CCM control implementation.

• Third-party outsourced: The third-party CSP in the supply chain (e.g., an IaaS provider) is responsible for CCM control implementation, while the CSP is fully accountable.

• Shared CSP and CSC: Both the CSP and CSC share CCM control implementation responsibility and accountability.

• Shared CSP and third party: Any CCM control implementation responsibility is shared between CSP and the third party, but the CSP remains fully accountable.

Note: The CAIQv4 SSRM schema is tailored to CCMv4's Supply Chain Management, Transparency, and Accountability (STA) domain, controls 1-6, and their corresponding implementation guidelines.

CSP implementation description (optional/recommended)

A description (with references) of how the cloud service provider meets (or does not meet) the portion(s) of the SSRM control they are responsible for. If "NA," explain why.

CSC responsibilities (optional/recommended)

A summary description of the cloud service customer security responsibilities for the portion(s) of the SSRM control that is responsible for, with corresponding guidance and references.

End of Introduction

© Copyright 2021-2022 Cloud Security Alliance - All rights reserved. You may download, store, display on your computer, view, print, and link to the Cloud Security Alliance "Consensus Assessments Initiative Questionnaire (CAIQ) Version 4.0.2" at http://www.cloudsecurityalliance.org subject to the following: (a) the Consensus Assessments Initiative Questionnaire v4.0.2 may be used solely for your personal, informational, non-commercial use; (b) the Consensus Assessments Initiative Questionnaire v4.0.2 may not be modified or altered in any way; (c) the Consensus Assessments Initiative Questionnaire v4.0.2 may not be redistributed; and (d) the trademark, copyright or other notices may not be removed. You may quote portions of the Consensus Assessments Initiative Questionnaire v4.0.2 as permitted by the Fair Use provisions of the United States Copyright Act, provided that you attribute the portions to the Cloud Security Alliance Consensus Assessments Initiative Questionnaire Version 4.0.2. If you are interested in obtaining a license to this #material for other usages not addresses in the copyright notice, please contact info@cloudsecurityalliance.org.