CAIQ-Lite: A New Framework For Cloud Vendor Assessment

Developed To Meet The Demands Of An Increasingly Fast-Paced Cybersecurity Environment

A Cloud Security Alliance and
Whistic Whitepaper

The Need for More Streamlined Vendor Security Assessments

Cloud providers are investing significantly more time and resources in communicating and validating security information in order to satisfy the demands of customers, as cloud vendor security continues to gain increased attention in all levels of corporations throughout the world. In this environment, organizations that leverage the cloud must either launch or mature a robust cloud vendor security assessment program in order to protect against the threat of a data breach.

However, the vast majority of vendor security assessments are still conducted using inefficient processes and are frequently reliant on proprietary, in-house questionnaires instead of widely adopted standards. As highlighted in a recent White Paper by CSA and NTSC:

> “Vendor security assessments generally consume a lot of time and cost while resulting in a limited understanding of a vendor’s risk profile. These inefficient assessments have trouble keeping up with the growing ecosystem of technology vendors—and especially the increased reliance on cloud security vendors.
>
> As a critical step toward securing the digital foundation of our economy, we recommend that businesses reduce their reliance on proprietary, in-house security assessment programs related to cloud computing...We believe [an] emphasis on consistent, uniform cloud security standards will increase the security baseline for all participants in our economy.”

While increasing the security baseline is one of the most important shared goals of our community, an often overlooked aspect of this standards-based approached is the potential risk of overburdening cloud vendors with a disproportionate level of assessment questions that are not commensurate with the level of risk or the potential use-case for the cloud vendor. In some cases, cloud vendors who are not critical to the business operations of an organization or that represent a low inherent risk level based on the type of data that they process, may be required to complete the same extensive vendor security assessment questions and provide the same level of documentation as a non-comparable vendor.

When observed from the vendor's point of view, this often leads to a poor assessment experience and creates unnecessary burden on the vendor to explain why answers to non-applicable questions were omitted. It also places an extra burden on the assessor in sifting through these omitted questions and makes it more difficult to compare vendors across an entire portfolio while maintaining a focus on what matters most. For this reason, an increasing number of companies are opting for lighter-weight assessment questionnaires and making program-level decisions based on ease-of-use, in addition to other considerations.

A new, lighter-weight assessment questionnaire is needed in order to accommodate the shift to cloud procurement models and to enable cybersecurity professionals to more easily engage with cloud vendors. The purpose of this white paper is to introduce a new questionnaire developed jointly by Cloud Security Alliance and Whistic to meet the demands of an increasingly fast-paced cybersecurity environment in which the ease of adoption is becoming one of the more important factors in selecting a vendor security questionnaire.

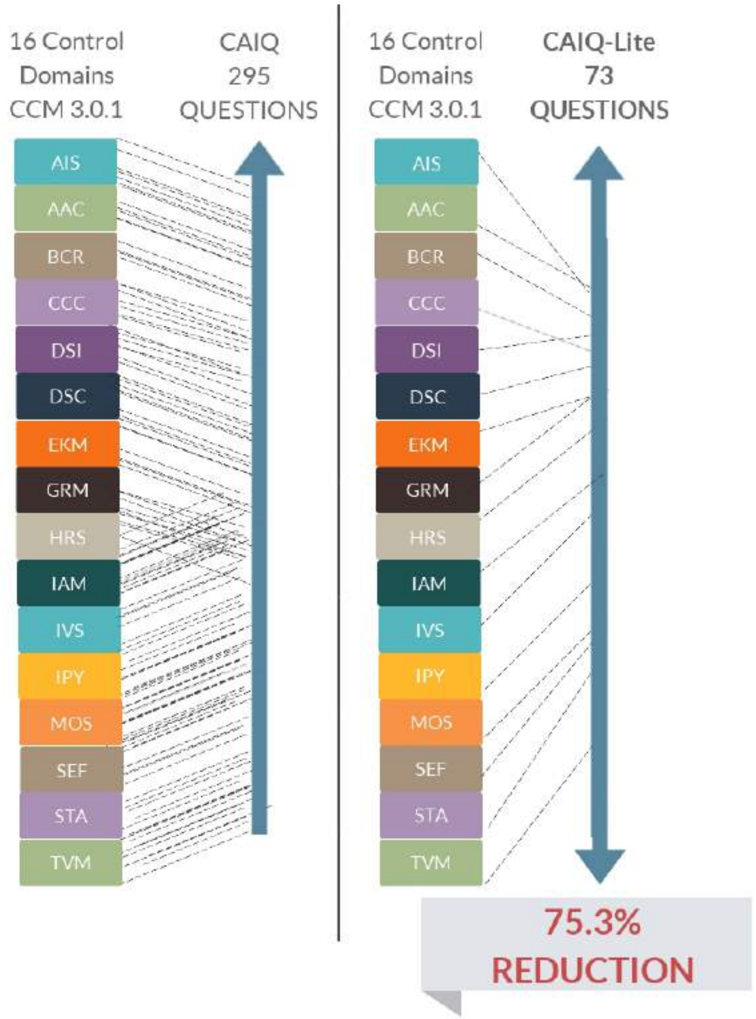
Overview of CSA Assurance Tools

- The CSA Cloud Controls Matrix (CCM) provides both cloud providers and customers with needed structure, detail, and clarity relating to information security. The CCM provides fundamental cloud control objectives around key cloud areas and is mapped to other popular standards such as ISO/IEC 27001, 27017 and 27018, AICPA TSC, NIST 800-53 ,German BSI C5 and COBIT between others
- The Consensus Assessments Initiative Questionnaire (CAIQ) was based upon the CCM, and provides a set of Yes/No/NA questions that a cloud consumer and cloud auditor may wish to ask of a cloud provider to ascertain compliance to the CCM and CSA best practices. The latest version of CAIQ is v3.0.1 and was updated on September 1, 2017

Introducing a Streamlined Version of CAIQ

A new, streamlined version of CAIQ was developed by CSA in conjunction with Whistic and combines data from an independent research panel of hundreds of Information Security professionals, CSA member feedback, and Whistic customer feedback. The project has been multiple years in the making and will allow companies throughout the world to more easily leverage CSA's industry-leading thought leadership in their cloud vendor security assessments.

The initial draft of CAIQ-Lite (BETA) released in conjunction with this white paper is 73 questions compared to the 295 found in the latest version of CAIQ. Every security control domain from the original questionnaire remains represented in the new, streamlined format. The research was focused on delivering accessibility and ease of use for both cloud vendors and the enterprises performing vendor security assessments.



The primary driving influence in forming the CAIQ-Lite centered on increasing adoption and utilization to help address the challenges discussed above. With the current CAIQ framework containing 295 questions, developing a solution that still leveraged the industry-leading research and best practices behind the Cloud Controls Matrix (CCM) and Consensus Assessments Initiative Questionnaire (CAIQ), with a more manageable scope, was the primary objective.

We collectively invite CSA members and the broader cybersecurity community to share their feedback regarding the initial release of CAIQ-Lite by emailing caiqlite@whistic.com. We look forward to gaining insights from the community regarding the actual implementation of this framework in a cloud vendor security assessment setting, and will incorporate this feedback in subsequent releases.

Research Methodology Utilized

Research that contributed to the creation of CAIQ-Lite is comprised of two different categories:

1. Empirically-driven statistical research that leverages a proprietary scoring algorithm developed by Whistic
2. Practically-driven qualitative feedback from expert teams of cloud security assessors

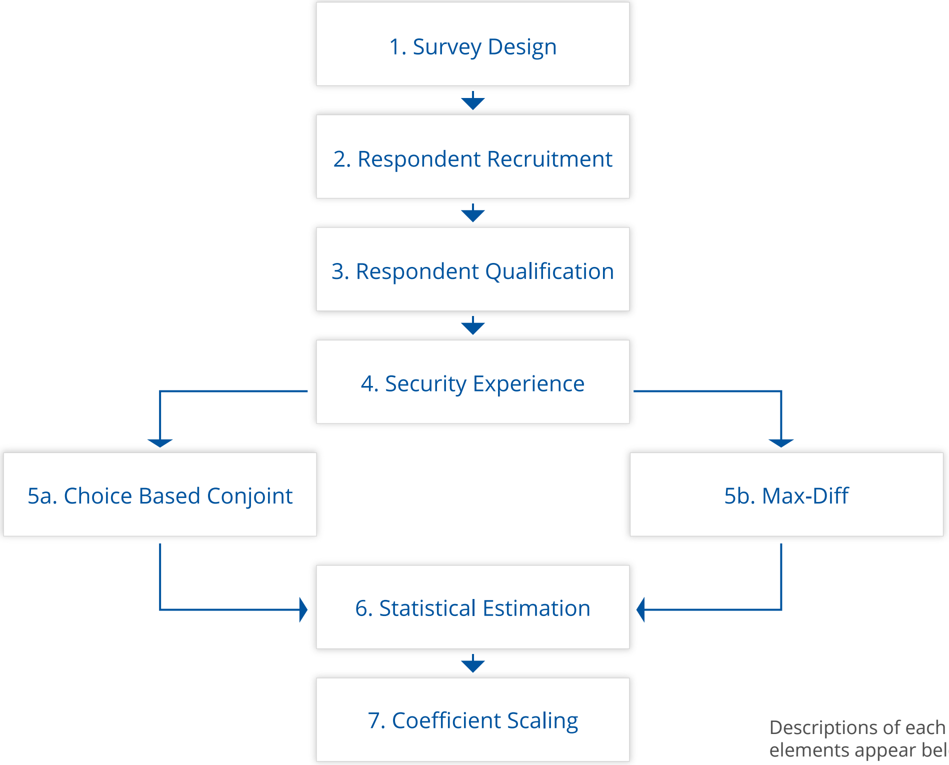
The resulting data from each category was layered and analyzed across categories with the primary objective of finding the question set that best represented the entire research body's short-list of questions. A few of the summary findings are listed below:

Finding	Result
# of questions retained in CAIQ-Lite	73
# of unique control IDs retained	53
# of unique control IDs eliminated	80
# of control domains completely eliminated	0
# of questions not kept by any data set	130

Empirically-Driven Methodology and Scoring Algorithm

The proprietary scoring algorithm leveraged in the CAIQ-Lite selection process is the same algorithm that powers Whistic's CrowdConfidence™ Score (for determining the relative risk of vendors assessed in the Whistic Platform). This methodology was used to assign an importance level to each question within the 16 control domains of CAIQ, and a subsequent weighting was derived to assist in the selection process for the CAIQ-Lite.

This methodology was architected to harness the collective wisdom of hundreds of IT security professionals in order to understand how each of the 295 questions in the Consensus Assessments Initiative Questionnaire (CAIQ) relate to a firm's trust in a cloud vendor. To accomplish this, IT security professional completed a 3-stage question set using 2 distinct modalities of preference elicitation questions. Data collected through this process was then fed into a statistical model that used Hierarchical Bayesian methods to estimate a ratio-scaled coefficient for each of the 295 items in the CAIQ. These parameter estimates then form the relative importance of each item as it relates to a firm's ability to trust an IT vendor. To deliver the CrowdConfidence™ Score, the estimated parameters are then rescaled so that the computed risk score will lie on the interval of 300-850. Figure 1 illustrates the flow of the survey design, collection, estimation, and scaling processes.


1. Survey Design
2. Respondent Recruitment
3. Respondent Qualification
4. Security Experience
5a. Choice Based Conjoint
5b. Max-Diff
6. Statistical Estimation
7. Coefficient Scaling

Descriptions of each of the illustrated elements appear below.

1. The CrowdConfidence™ question set included three major components:

    a. A set of screener questions to determine if respondents are IT security professionals and if they qualified to complete the study.

    b. A collection of questions used to determine industry affiliation, education level, years of experience, and other meaningful characteristics of the respondent.

    c. A set of either MaxDiff or Choice-Based Conjoint questions used to elicit the relative importance of items in the CAIQ. Illustrations of these types of questions appear in Figure 2 (Choice-Based Conjoint) and Figure 3 (MaxDiff). In both cases, fractional-factorial experimental design methods are used to reduce the complexity of the design space (i.e., it is not feasible to show respondents all 295 items).

2. Respondents for the initial calibration sample were recruited from a variety of sources including LinkedIn groups related to IT Security, as well as commercial panels of IT Security professionals maintained by SSI and Qualtrics.

3. In order to qualify for participation in the study respondents must work in the field of IT Security and must be familiar with the IT Security risk assessment process.

4. Once qualified, respondents completed a variety of questions to assess their demographic and professional backgrounds, as well as the nature of the IT Security Assessment process at their current place of employment.

5. At this stage in the questionnaire, respondents were randomly divided (50/50 split) into 1 of 2 possible paths: Choice Based Conjoint or MaxDiff. Both paths involve methods used to elicit a relative rank ordering over items in the CAIQ, but use a different approach to do so.

    5a. Respondents branched into the Choice Based Conjoint questions were shown a collection of 4 prospective firms that differ with respect to the presence or absence of 5 security characteristics (see Figure 2). They are asked to pick the firm that they would trust the most as a prospective vendor. The process is repeated 8 times with a new set of statements and characteristics.

5b. In the MaxDiff condition, respondents are shown a collection of 5 security protocols and are asked to pick the most and least important protocol from the list. This process was also repeated 8 times for each respondent.

6. Data collected through both the MaxDiff and Choice Based Conjoint tasks was pooled together (with the corresponding design matrix) and was used to estimate a model where the probability of each discrete choice, i, is made according to the following formula:

$$prob(y_i = j) = \frac{e^{x'_j\beta}}{\sum_k e^{x'_k\beta}}$$

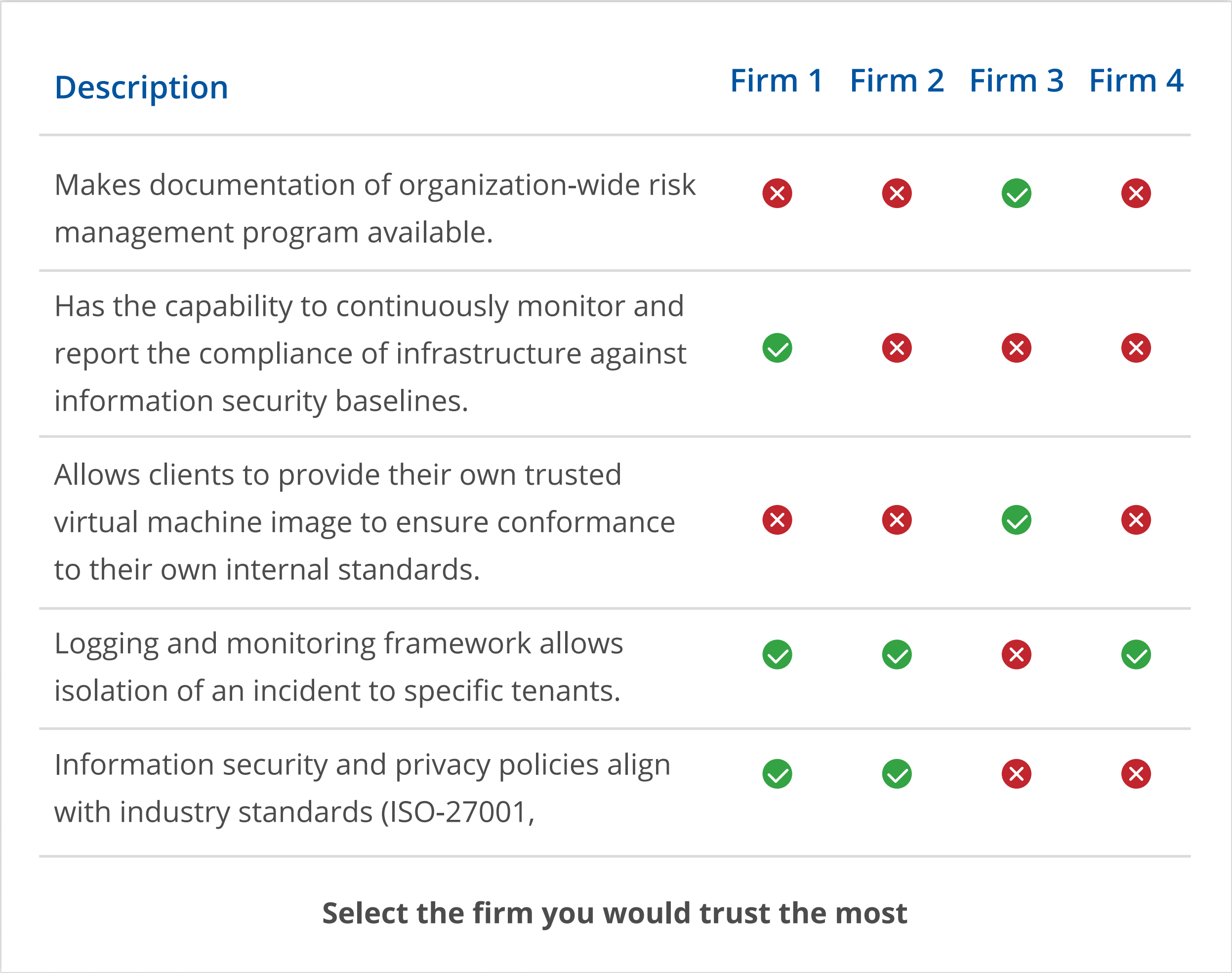
Where yi denotes the choice made by the respondent and beta (in vector notation) is the set of weights for the questions. Given the expression above, we derived a likelihood for data and can then use Bayesian statistical methods to estimate the model parameters.

7. The estimated collection of coefficients were then scaled according to the following formula to lie on the 300 to 850 interval according to the following formula. The result is the Crowd Confidence™ score.

$$300 + \sum_{i=1}^{295} 550 * (\beta_i / \sum_i \beta_i) * I(q_i = 1)$$

Figure 2: Example of a Choice Based Conjoint Task

Imagine that you are screening potential vendors for your organizatio. Which of these firms would you **trust the most?**

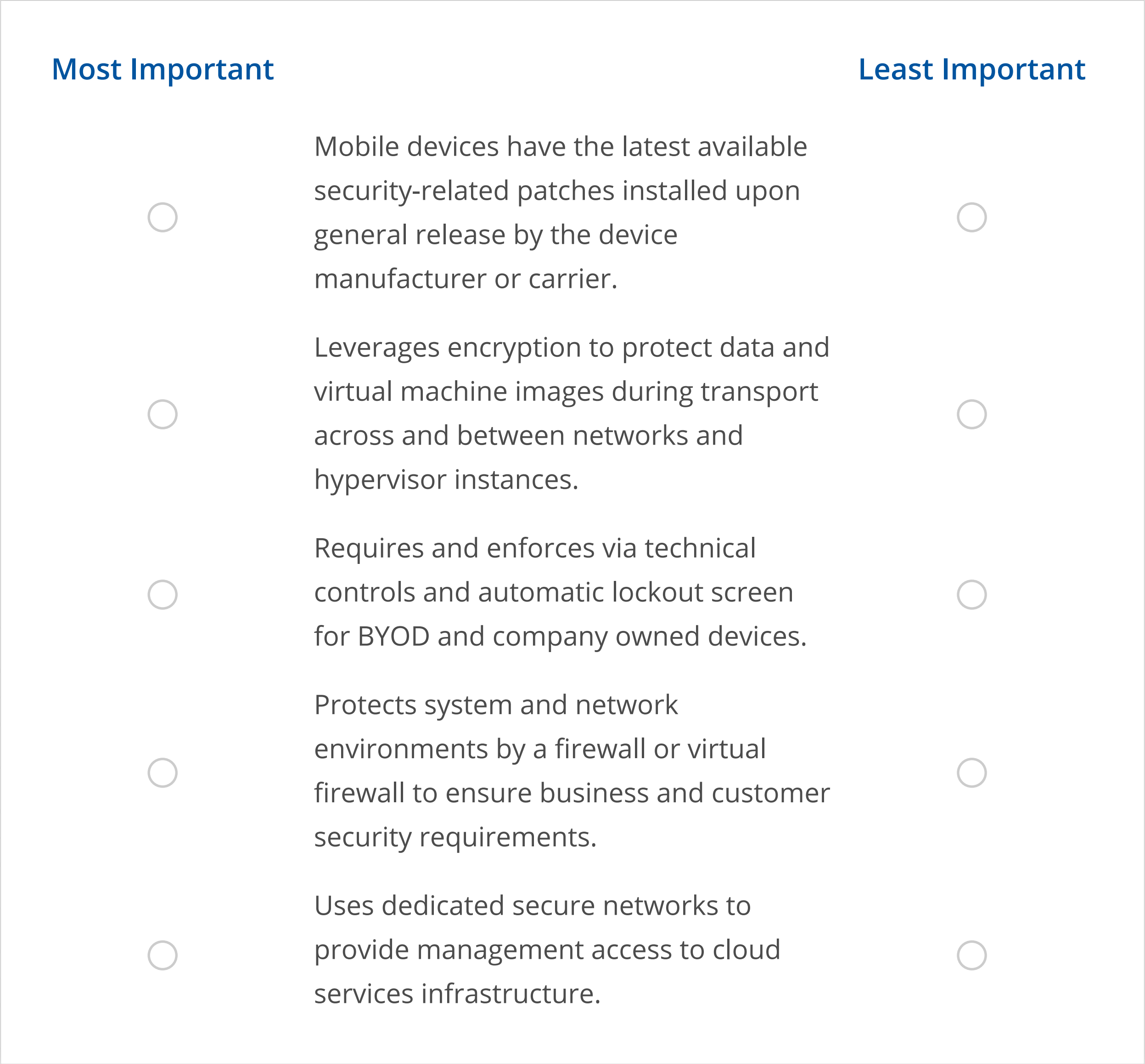


Description	Firm 1	Firm 2	Firm 3	Firm 4
Makes documentation of organization-wide risk management program available.	✗	✗	✓	✗
Has the capability to continuously monitor and report the compliance of infrastructure against information security baselines.	✓	✗	✗	✗
Allows clients to provide their own trusted virtual machine image to ensure conformance to their own internal standards.	✗	✗	✓	✗
Logging and monitoring framework allows isolation of an incident to specific tenants.	✓	✓	✗	✓
Information security and privacy policies align with industry standards (ISO-27001,	✓	✓	✗	✗

Select the firm you would trust the most

Figure 3: Example of a MaxDiff Task

Which of these controls are **most** and **least** important?



Most Important		Least Important
○	Mobile devices have the latest available security-related patches installed upon general release by the device manufacturer or carrier.	○
○	Leverages encryption to protect data and virtual machine images during transport across and between networks and hypervisor instances.	○
○	Requires and enforces via technical controls and automatic lockout screen for BYOD and company owned devices.	○
○	Protects system and network environments by a firewall or virtual firewall to ensure business and customer security requirements.	○
○	Uses dedicated secure networks to provide management access to cloud services infrastructure.	○

Practically-driven qualitative feedback from expert teams of cloud security assessors

Since the initial release of CAIQ by CSA years ago, individual CSA Members have developed, tested, and leveraged various condensed versions of CAIQ for their own purposes. Some of these members, comprising both cloud service providers and global enterprises, have proactively shared this feedback with CSA in order to help inform future thinking around a lighter-weight question set. While this feedback was not research-driven and was focused on the practical application of CAIQ in a condensed version, hundreds of cloud vendor assessments have been conducted over the course of several years using these custom CAIQ's. This feedback and research was leveraged to help inform the selection of the final question set for CAIQ-Lite.

Likewise, Whistic engaged experienced vendor assessment professionals from among its customer base to in order to garner feedback for inclusion in the CAIQ-Lite selection process. These professionals spent time reviewing CAIQ and proposing what their final set of questions would look like if they had a cap of 100 total questions.

Data from each of these groups was segmented and analyzed, in combination with the empirical scoring data, and both frequency of questions appearing across data sets as well as empirical score weights were combined to determine the optimal set of questions for the initial CAIQ-Lite release.

Tips/FAQ

Why/When would one potentially utilize CAIQ-Lite vs. CAIQ?

- CAIQ-Lite could be utilized to assess lower-risk cloud service providers.
- CAIQ-Lite could be utilized to assess vendors that have access to less-sensitive data
- CAIQ-Lite could be utilized to assess vendors that are less-critical to business operations
- CAIQ-Lite could be utilized as a two-step assessment model to fit your desired sales and procurement timetable; with the full CAIQ as the second step.
- CAIQ-Lite could be utilized by cloud vendors for self-assessment and sharing with potential customers to streamline the security review process

Should Cloud Providers self assess against CAIQ-Lite?:

- Yes, it is advisable for Cloud Providers to self-assess using the newly created CAIQ-Lite framework. This can also serve as a useful addition to any businesses' security posture.

If I am a Whistic customer or a vendor with a CAIQ that has a CrowdConfidence score in the Whistic Platform, how should I interpret comparative CrowdConfidence™ Score differences between CAIQ & CAIQ-Lite?

- While the importance level of CAIQ questions remains the same, the weighting is inherently different due to the selected reduction in questions. It's natural to experience a difference in scoring as the questions within each Control Area are therefore amplified within CAIQ-Lite. The CrowdConfidence™ Score serves as an intelligent starting point to further delve into any vendors overall security postures, procedures, and policies.

About CSA

The Cloud Security Alliance (CSA) is the world's leading organization dedicated to defining and raising awareness of best practices to help ensure a secure cloud computing environment. CSA harnesses the subject matter expertise of industry practitioners, associations, governments, and its corporate and individual members to offer cloud security-specific research, education, certification, events and products. CSA's activities, knowledge and extensive network benefit the entire community impacted by cloud — from providers and customers, to governments, entrepreneurs and the assurance industry — and provide a forum through which diverse parties can work together to create and maintain a trusted cloud ecosystem. For further information, visit us at www.cloudsecurityalliance.org, and follow us on Twitter @cloudsa.

About Whistic

Whistic enables companies to conduct and respond to vendor security reviews on a single platform. Software vendors and other companies that store or process sensitive data are undergoing an increasing amount of scrutiny from their prospects, customers and partners as it relates to information security and compliance. Whistic reduces friction by automating and streamlining security reviews, enabling InfoSec and compliance teams to more efficiently understand the security and compliance posture of a given company and empowering sales teams to standardize their responses to security questionnaires. Whistic is currently located in the heart of the Silicon Slopes in Utah. Our award winning platform is now backed by incredible investors and used by top security teams throughout the world, and is The Complete Vendor Security solution for both sides of the supply chain. For further information, visit us at www.whistic.com and follow us on Twitter @Whistic_Inc

How To Access CAIQ-Lite

CAIQ-Lite can be accessed by CSA members for free on both Whistic and CSA websites:

https://resources.whistic.com/CAIQ-Lite

https://cloudsecurityalliance.org/star/#_caiq-lite

Also, any members that already have a CAIQ on The CSA STAR Program will automatically have a CAIQ-Lite generated for them on the Whistic Platform.