Worked Example: a security questionnaire, completed

Five questions from a CAIQ v4.1.0, completed for a sample MSP from its own security documents.

This is how a finished questionnaire comes back: every answer is drawn only from your documents, the source is cited, and any gap is flagged for your sign-off rather than guessed. A confident wrong answer is what gets an MSP caught in a security review, so the engine never invents a control you do not have.

A&A-01.1; Are audit and assurance policies, procedures and standards established, documented, approved, communicated, applied, evaluated and maintained?

Yes [Company] maintains an ISMS aligned to ISO 27001:2022. Information security policies, including audit and assurance provisions, are documented, approved by management, communicated to staff and reviewed at least annually. Internal ISMS audits are conducted annually.

Basis: Information Security Policy (ISMS / internal audit clauses); ISO 27001:2022 certificate.

A&A-02.1; Are independent audit and assurance assessments conducted according to relevant standards at least annually?

Yes [Company] holds ISO/IEC 27001:2022 certification, involving annual independent surveillance audits by a UKAS-accredited body, and Cyber Essentials, renewed annually.

Basis: ISO 27001:2022 certificate; Cyber Essentials certificate.

A&A-03.1; Are independent assessments performed according to risk-based plans and in response to significant changes or emerging risks?

Partial Certification implies risk-based audit planning, and policies are reviewed on significant change. The documents do not confirm that independent assessments (as distinct from policy reviews) are triggered by significant changes or emerging risks.

Basis: ISO 27001 certificate; Information Security Policy.

Flag: confirm whether independent assessments are triggered by significant changes.

A&A-04.1; Is compliance verified against all relevant standards, regulations and legal/contractual requirements applicable to the audit?

Confirm Not evidenced in the provided documents. No compliance obligations register or evidence of legal and contractual compliance verification was supplied.

Basis: Not found in provided documents.

Flag: provide a compliance obligations register / evidence of legal and contractual compliance verification.

A&A-05.1; Is an audit management process defined and implemented (planning, risk analysis, control assessment, remediation schedules, reporting, review of past reports)?

Partial Annual internal audits, recorded nonconformities, corrective actions tracked to closure and an annual management review are evidenced. A fully defined audit management process is not.

Basis: Information Security Policy (internal audit, nonconformity, management review).

Flag: provide the documented internal audit procedure.

What this shows

- Confident answers only where your documents support them.
- Honest *Partial* and flags everywhere they do not, so nothing overstated gets you caught in review.
- Every answer sourced, ready for your sign-off.

Your next questionnaire, completed and submission-ready in 3 working days.

You spend about 15 minutes. £349 per questionnaire, and you only pay once you are happy. [your name] · [email]

Illustrative sample using fictional company data. CAIQ is a standard of the Cloud Security Alliance.