FREE GUIDE

A Customer Sent You a Security Questionnaire. Now What?

A plain-English survival guide to your first vendor security questionnaire: what they're asking, why, and how to answer honestly without losing the deal.

A security questionnaire means a bigger customer is seriously considering buying from you. It's the toll booth between a small vendor and a big deal. It is also, for most founders, the first time anyone has formally asked "so how do you actually handle security?" That is why it feels like an exam you didn't study for. You can pass it honestly. Here's how to think about it.

A free guide from Sylvan Assurance — plain-English security, without us ever seeing your data.

First: this is good news, mostly

A security questionnaire means a bigger customer is seriously considering buying from you. It's the toll booth between a small vendor and a big deal. It is also, for most founders, the first time anyone has formally asked "so how do you actually handle security?" That is why it feels like an exam you didn't study for. You can pass it honestly. Here's how to think about it.

What you've actually been sent

Most questionnaires are one of a few standard forms, or a homegrown copy of one. **SIG** (Standardized Information Gathering) and **CAIQ** (the Consensus Assessments Initiative Questionnaire) are the two you'll meet most. They run from dozens to hundreds of questions, but they circle the same handful of topics: who can access what, how you sign in, how your devices are protected, whether you keep backups, what you'd do in a breach, and how you handle the customer's data.

The reviewer on the other end usually isn't trying to fail you. They're trying to document that they checked. Clear, honest, complete answers (even ones that admit gaps) make their job easy. Evasive or inflated answers make it hard, and hard is what gets a small vendor rejected.

The six things they almost always ask about

- **Sign-in security**: do you require two-step login, especially on email and admin accounts?
- **Access**: does each person have their own account, with only the access their job needs? What happens when someone leaves?
- **Devices**: are laptops encrypted and kept up to date? Is there protection against malicious software?
- **Backups**: do they exist, are they separate from your main systems, and have you tested a restore?
- **When something goes wrong**: do you have a written plan, and would you tell the customer if their data were involved?
- **Data handling**: where does customer data live, who can see it, and when is it deleted?

If you can answer those six topics truthfully and specifically, you can answer most of any questionnaire. The hundreds of questions are mostly these six wearing different clothes.

The golden rule: never inflate

It is tempting to answer "yes" to everything. Don't. Reviewers read hundreds of these; confident vagueness and too-perfect answers stand out. Worse, your answers often get attached to the contract. An inflated "yes" can become a legal problem later.

The honest alternative that still wins deals is the **"in progress" answer**: state what's true today, and what's planned. "Laptops are encrypted; a formal written policy is planned for this quarter" is a strong answer. It signals exactly what a reviewer wants to see: a vendor who knows where they stand.

What "evidence" means

Many questionnaires ask you to attach proof: a security policy, an incident-response plan, an access-control policy. For a small business these don't need to be long: a page or two each, stating what you actually do. What matters is that they exist, they're dated, and they match your answers. A reviewer who sees a short, honest policy that matches the questionnaire believes everything else you wrote.

Reuse everything

Here's the secret that makes the second questionnaire painless: they're all mostly the same. Keep every answer you write in one document (your answer bank) and the next questionnaire becomes an afternoon of copy-and-adapt instead of a week of dread. Vendors who get ahead of this go one step further and publish a short security overview page, which answers the common questions before anyone sends a form at all.

The honest summary

Answer the six core topics truthfully, use "in progress" instead of inflation, back your answers with short real documents, and save everything for next time. That's the whole game. No certification required to start winning deals.

Where to go from here

The free TrustReady scanner shows you how ready you are to answer (across the exact domains questionnaires ask about) in a few minutes, entirely in your browser, so we never see your answers.

When you're ready to build the answer bank, the proof documents, and a shareable trust page, the TrustReady kit lays it all out: from $49, one-time, with a 30-day money-back guarantee.

Take the free assessment: sylvanassurance.com/free/trustready/

See the full toolkit: sylvanassurance.com/trustready.html

Scan for the free assessment that goes with this guide.

sylvanassurance.com/go/free-trustready