10 Answers Every Security Questionnaire Asks For

Sample, defensible wording for the ten most common questions — in plain English

Sylvan Assurance, LLC

Version 1.0 · Updated 2026-09-03

Contents

10 Answers Every Security Questionnaire Asks For **1**
Sample, defensible wording for the ten most common questions 1
1. “Do you enforce Multi-Factor Authentication?” 2
2. “How is access provisioned and removed?” 2
3. “Is customer data encrypted at rest?” 2
4. “Is data encrypted in transit?” 2
5. “Do you have a documented incident response plan — and has it been tested?” 3
6. “How do you manage vulnerabilities and patching?” 3
7. “Do you take backups — and have you restored from them?” 3
8. “Who are your sub-processors, and how do you manage them?” 3
9. “Do your people receive security training?” 3
10. “Do you hold SOC 2 or ISO 27001?” 4

About This Guide **5**

10 Answers Every Security Questionnaire Asks For

Sample, defensible wording for the ten most common questions

Who this is for: the founder or team lead who just received a vendor security questionnaire (180 questions about controls and certifications you have mostly heard mentioned in passing) and needs to answer honestly without losing the deal. Nearly every questionnaire, whatever its format, asks some version of the ten questions below. Each comes with what the question is really asking and sample wording you can adapt.

The one rule before you write anything: answer the company you are, not the company you plan to be. Reviewers read hundreds of these; inflated answers are easy to spot and expensive to walk back. An honest “partial, with a date” consistently outperforms a hopeful “yes”, and “evidence available under a Non-Disclosure Agreement (NDA)” signals you actually have the artefact behind the answer.

How to use the samples: the wording in `[brackets]` is yours to fill. Name your real provider, your real timeline, your real gaps. Every sample ends with the evidence you

would show if asked, because the evidence line is what separates an answer from an assertion.

A note on acronyms: Multi-Factor Authentication (MFA), Non-Disclosure Agreement (NDA), Transport Layer Security (TLS), Advanced Encryption Standard (AES), System and Organization Controls 2 (SOC 2), International Organization for Standardization 27001 (ISO 27001), the Standardized Information Gathering questionnaire (SIG), the Consensus Assessments Initiative Questionnaire (CAIQ).

---

1. "Do you enforce Multi-Factor Authentication?"

What it is really asking: whether a stolen password, on its own, gets an attacker into your systems.

Sample wording: *All administrative access to production systems requires MFA, enforced through `[identity provider]` using authenticator apps or hardware keys, with text-message codes disabled for administrative roles. End-user access `[does / does not yet]` require MFA; `[if not yet: enforcement is scheduled for [date]]`. Evidence available under NDA: identity-provider policy export and enrolment report.*

2. "How is access provisioned and removed?"

What it is really asking: whether a departed employee's accounts keep working after they leave.

Sample wording: *Access is granted through a documented, role-based onboarding workflow and removed by the offboarding workflow; all access is revoked within `[one business day]` of departure. We review administrative and customer-data access `[quarterly]`, and findings are tracked to closure. Evidence available under NDA: onboarding/offboarding policy and the most recent access review.*

3. "Is customer data encrypted at rest?"

What it is really asking: whether a stolen disk or copied database file is readable.

Sample wording: *Yes. Customer data at rest is encrypted with AES-256 or stronger. Keys are `[managed by our cloud provider's key-management service / managed by us]` and access to them is restricted to `[named roles]`. Evidence available under NDA: cloud configuration export showing encryption at rest enabled.*

4. "Is data encrypted in transit?"

What it is really asking: whether traffic between your customers, your services, and your vendors can be read on the wire.

Sample wording: *Yes. All customer data in transit uses TLS 1.2 or higher, enforced at our load balancer, with TLS 1.3 preferred where the client supports it. Evidence available under NDA: load-balancer configuration and a recent independent TLS scan report.*

5. “Do you have a documented incident response plan — and has it been tested?”

What it is really asking: whether a bad day at your company becomes a bad month for theirs.

Sample wording: *Yes. We maintain a written incident response plan naming who declares an incident, who leads the response, and when and how customers are notified. The plan was last reviewed [date] and exercised [date — a tabletop counts; say so plainly]. Evidence available under NDA: the plan document with its review date.*

6. “How do you manage vulnerabilities and patching?”

What it is really asking: whether known holes stay open in your systems for months.

Sample wording: *Dependencies and images are scanned [on every build / weekly] via [tool]. Findings are triaged by severity; critical items are patched within [X days], high within [Y days], and exceptions are documented with an owner and a date. Evidence available under NDA: the patching policy and a recent scan summary.*

7. “Do you take backups — and have you restored from them?”

What it is really asking: whether your service (and their data) survives your worst day.

Sample wording: *Customer data is backed up [daily] to [a separate account / region], with restores tested [quarterly / date of last test]. Our recovery targets are [recovery time objective / recovery point objective, if defined]. Evidence available under NDA: backup configuration and the most recent restore-test note.*

8. “Who are your sub-processors, and how do you manage them?”

What it is really asking: whether their data quietly flows to vendors nobody has vetted.

Sample wording: *We maintain a current list of sub-processors that handle customer data ([cloud provider, email provider, analytics, support tooling]), reviewed [annually] against each vendor’s security posture and data-processing terms. The list is available [on our website / on request]. Evidence available under NDA: the vendor register with review dates.*

9. “Do your people receive security training?”

What it is really asking: whether the humans (the most common way in) are part of your security programme.

Sample wording: *Yes. All staff complete security-awareness training at onboarding and [annually] thereafter, covering phishing, data handling, and incident reporting. Completion is tracked. [If you screen: New hires undergo background checks where local law permits.] Evidence available under NDA: training records.*

10. “Do you hold SOC 2 or ISO 27001?”

What it is really asking: whether an independent party has checked any of the above and, if not, whether you know where you stand without one.

Sample wording (the honest no): *Not yet. We [are pursuing SOC 2 Type I with a target of [date] / have not yet begun a certification]. In the meantime, the controls described in this questionnaire are in place and we are glad to evidence any of them under NDA, or to complete your assessment against [SIG Lite / CAIQ].* A dated, concrete “not yet” with evidence behind it wins deals that a vague “in progress” loses.

These ten are a sampler: the full TrustReady toolkit carries the thirty-question answer bank these are drawn from, the proof-document builders, and the shareable trust profile that heads off the next questionnaire before it arrives.

About This Guide

This guide is produced by **Sylvan Assurance, LLC** and reflects professional experience translated into plain-language guidance for small business owners.

It provides **general guidance and recommended practices**. It is **not** legal advice. Every recommendation is **optional** - a widely accepted way to reduce a common risk. Responsibility for your business remains with you.

For full terms, see the Terms of Use provided with TrustReady.

Copyright 2026 Sylvan Assurance, LLC. Not for resale.

Free to share unchanged with credit. Terms: sylvanassurance.com/licence/free/