THE PLAYBOOK

Security Questionnaire Response Playbook

How to triage the full document, answer honestly, and keep a stalled deal moving.

Dr. Leonard Simon
professorsimon.com

Before You Start

Most security questionnaires feel bigger than they are. Fifty questions arrive at once, the deal is on the line, and the instinct is to either answer everything as fast as possible or freeze.

This playbook walks through the same process I use with clients: triage the document first, answer honestly with a real plan attached where you have gaps, and know what to do when a reviewer comes back with a question you weren't expecting.

It's meant to be used, not just read. Keep it open next to the actual questionnaire.

Step 1: Triage Before You Answer Anything

Read the entire questionnaire once before answering a single question. Sort every item into one of three piles.

> **Pile 1: You Have This**
> Answer cleanly and move on. Don't explain more than you need to about something that's genuinely in place. A confident short answer is stronger than a paragraph that sounds like it's trying too hard.

> **Pile 2: You Don't Have This, But It Won't Sink the Deal**
> Most questionnaires have a long tail of items that matter in aggregate but rarely block a deal on their own: a specific certification, a policy for something with minor risk, a monitoring tool that would be nice to have. State plainly that it's not yet in place, and give a rough timeline. Don't dress these up with jargon; reviewers see through that quickly.

> **Pile 3: The Two or Three Questions That Actually Matter**
> These cluster around data handling, access control, and incident response. These are the things that would genuinely hurt the buyer if you got them wrong. This is where you spend real time. If there's a gap here, it's worth a short internal conversation before you respond.

In practice, Pile 3 is usually three to five questions out of fifty. Once you've separated it from the noise, the rest of the document moves much faster than it feels like it will on first read.

Step 2: Language for Common Gaps

Below are the questions that come up most often, with template language for when you have a real gap. Adjust the specifics to your actual situation. The goal is a structure, not a script to copy verbatim.

Question: *Do you have a SOC 2 report?*
Template language: We are currently in the readiness phase for SOC 2 Type II, with a target audit start date of [date]. In the meantime, we can share our current control documentation, including [access control policy / data handling practices], and are happy to walk through our security posture directly with your team.

Question: *Do you have a formal, documented incident response plan?*
Template language: We currently manage incidents through [describe your actual current process, even if informal]. We are formalizing this into a documented IR plan, targeted for completion by [date], which will define roles, an escalation path, and a customer communication process for any incident affecting customer data.

Question: *Do you conduct regular access reviews?*
Template language: We currently review access to production systems and customer data on a [monthly/quarterly] basis, led by [role]. We are moving toward a fully documented review process with retained evidence, targeted for [date].

Question: *Do you have a formal vendor risk management program?*
Template language: We evaluate new vendors and subprocessors prior to engagement, focused on [data access level / criticality]. We are formalizing this into a documented vendor risk program with tiered assessments, targeted for [date].

Question: *Do you encrypt data at rest and in transit?*
Template language: Yes. Data in transit is encrypted using [TLS version]. Data at rest is encrypted using [method/provider]. [Include this only if accurate. This is a Pile 1 item for most modern SaaS companies; if it isn't true yet, treat it as a Pile 3 gap and prioritize closing it before the deal timeline forces the question again.]

Step 3: When a Reviewer Pushes Back

A question that comes back a second time is not a rejection. It usually means the reviewer is building a defensible file and needs more specificity than your first answer gave them. A few principles for this stage:

- Respond quickly, even if the full answer isn't ready. “We're pulling this together and will have a complete answer by [date]” keeps momentum and signals you're not avoiding the question.
- If they're pushing on a Pile 3 gap, this is the moment to loop in whoever owns that area internally. Don't guess at technical specifics you're not certain of.
- If a question feels disproportionate to your risk profile (for example, a requirement built for enterprise scale applied to a relationship involving very little sensitive data), it's fair to ask what's driving the requirement. Reviewers often have some flexibility they don't offer up front.
- Keep a single point of contact managing the thread. Multiple people answering piecemeal is what creates the inconsistencies that trigger deeper scrutiny.

A note on escalation

If a reviewer's next question starts to feel like it's stalling rather than clarifying, it's reasonable to loop in your champion on the buyer's side and ask them to help understand what's needed to move forward. This isn't going around the reviewer. It's normal deal management, and most experienced champions expect to do this.

Quick Reference: The Single Page Version

> **Before you answer anything**
> Read the whole document. Sort into three piles: have it, don't have it but it's minor, don't have it and it matters.

> **For every real gap**
> State it plainly. Give a specific plan with a rough date. Never claim a control you don't have.

> **When a reviewer follows up**
> Respond fast, even if incomplete. Loop in the right internal owner. Keep one point of contact managing the thread.

A Closing Thought

The questionnaire is rarely the real obstacle. How clearly and honestly you respond to it is what actually determines whether the deal keeps moving. Most gaps are survivable when they're paired with a credible plan. What stalls deals is silence, or answers that don't hold up under a second look.

About Dr. Leonard Simon

Dr. Leonard Simon is a cybersecurity executive, CISSP, and adjunct professor who has guided organizations through SOC 2 readiness, risk assessments, and enterprise security reviews. For more resources like this one, visit professorsimon.com.