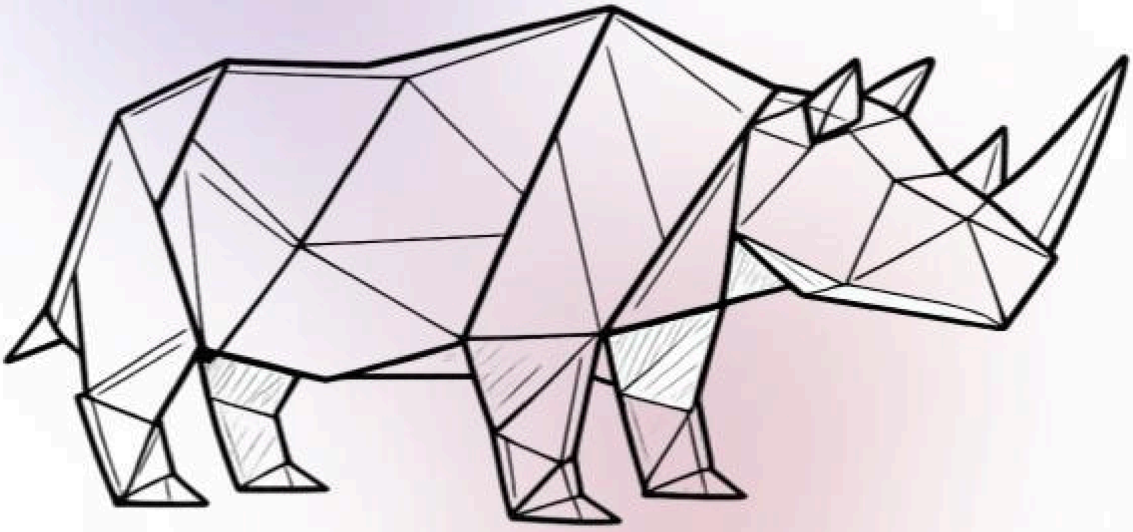
ResponseHub



The Security Questionnaire Survival Guide

A practical guide to the worst part of enterprise sales

About the Author

Neil Cameron has spent two decades building software products, previously as co-founder and CTO of Progression, a venture-backed HR tech startup which was acquired at the end of 2024. Prior to that, he was founding CTO at EmpowerRD, a market leading R&D tax credit claim product. It was at Progression where he first experienced the pain of security questionnaires while selling to mid-market and enterprise customers. After dealing with dozens of them, often while juggling hiring, product work and helping close deals, he became convinced there had to be a better way.

About the ResponseHub

ResponseHub helps teams respond to security questionnaires quickly and accurately without needing a dedicated compliance function.

ResponseHub is designed for speed and self-serve use. Upload a questionnaire and get AI-generated answers grounded in your policies and knowledge base, with confidence ratings and clear citations. Built-in explainers help you understand what reviewers are actually looking for, and a knowledge base with semantic search means you never start from zero.

Learn more at responsehub.ai.

Introduction

Updated 22 January 2026

Four years ago I was in the thick of it: we had just closed a $3.1m seed round, we had pivoted our HR tech product to target mid-market rather than SMB and I had a never-ending to-do list including hiring, firing and helping close our most important deals. I was co-founder and CTO but in reality that meant doing a bit of everything. The other thing that happened at that time was that I got my first experience of security questionnaires.

The first one was fine, just another task to grind through. The second one was interesting, I could re-use some things but the questions were worded a bit differently. The third one was for a stodgy corporate and was 300 questions long - that one really tested my resilience. After questions four, five and beyond I could only think one thing: *there must be a better way than this…*

Fast forward to 2026 and I am building the tool I wish I had back then to help teams to quickly and accurately respond to security questionnaires so they can get back to the really important work of building their business.

This guide is the missing manual that I needed when we started selling to larger companies. It will help you understand why you are being sent the questionnaires, how to optimise your responses, what to do when you do not meet the customer’s requirements and how to automate the whole process using AI.

1. Why security questionnaires exist (and why they won't go away)

Whether you realize it or not, you are now on the receiving end of Third Party Relationship Management (TPRM). You are the third party and your relationship is being managed. TPRM is the process of vetting, onboarding, and continuously monitoring every vendor an enterprise works with. When an enterprise adopts a product they are delegating a business process and all its associated risk and data. This can create huge upside for both parties: the enterprise gets a best-in-class, battle-tested solution; the vendor gets to do one thing extremely well and get paid handsomely for it.

However, this upside is not without risk. Enterprises are no strangers to risk and it is not an inherently bad thing but it does need to be understood and, as much as possible, quantified. And what is the best way to do that? A 300-question Excel spreadsheet of course! Well not really, but until a universally adopted standard or marketplace emerges, it will likely remain the dominant method.

As companies grow and mature there comes a point when they start thinking about their own TPRM. Small companies often rely only on large, established vendors like Google, Notion or AWS. It is a safe bet that these companies have excellent security practices. As a company grows it will begin to establish new functions like Sales, Marketing, Legal, HR each of which will start to adopt tools to help with their line of business, sometimes these will be cutting-edge tools from early-stage startups. Suddenly the risk profile is not so clear and you might question the wisdom of trusting your business critical data to an 18 month old company.

Around this time companies start looking for standards and structure for how to scale their operations. The two most common options are SOC 2 and ISO 27001 both of which require the practice of TPRM.

SOC 2

SOC 2 is the more common choice for US-based startups, largely because it is faster to achieve and more familiar to American buyers. The Trust Services Criteria address vendor risk primarily through CC9.2, which requires organizations to assess and manage risks from third parties. It is not the most heavily weighted area of a SOC 2 audit, but you cannot ignore it and pass. Auditors will look for evidence that you:

- Identify and assess vendor risks
- Have criteria for selecting vendors
- Monitor vendor performance and compliance
- Have contractual protections in place

In practice, this means maintaining a vendor register, documenting your selection process, and periodically reviewing whether your vendors still meet your standards. The good news is that for most early-stage companies, your vendor list is short and dominated by well-known names—making this relatively painless to implement.

ISO 27001:2022

ISO 27001 carries more weight internationally and is often the preferred (or required) standard when selling into European enterprises or regulated industries. It is also more explicit about TPRM. Annex A dedicates four controls specifically to supplier relationships:

- A.5.19 – Information security in supplier relationships
- A.5.20 – Addressing security within supplier agreements
- A.5.21 – Managing security in the ICT supply chain
- A.5.22 – Monitoring and review of supplier services

Regulated Industries

Companies that operate in a regulated industry will often have no choice but to run a rigorous TPRM as part of their legally required regulations. When your prospective customer operates in financial services, healthcare, or government, expect longer sales cycles, more detailed questionnaires, and requirements that go beyond what a typical compliance framework demands.

Financial Services

Banks and financial institutions face some of the most prescriptive vendor management requirements. In the US, the OCC and FFIEC have issued detailed guidance that expects board-level oversight of critical vendors, comprehensive due diligence before onboarding, and ongoing monitoring throughout the relationship. This isn't just security theatre, regulators actively examine how banks manage their third parties and have issued enforcement actions when oversight falls short.

In the EU, things got significantly more demanding with DORA (the Digital Operational Resilience Act), which came into effect in January 2025. DORA introduces detailed requirements for ICT third-party risk management, including concentration risk limits (to prevent over-reliance on a single vendor), mandatory contract clauses, and documented exit strategies. If you are selling software to European financial institutions, expect to demonstrate how they could migrate away from your platform if needed.

The UK has its own flavour of these requirements, shaped by the FCA and PRA. The FCA's outsourcing guidance and the PRA's Supervisory Statement SS2/21 set clear expectations for how regulated firms manage third-party relationships, particularly for material outsourcing arrangements. What makes the UK regime distinctive is the emphasis on personal accountability, under the Senior Managers and Certification Regime (SM&CR), specific individuals within the firm are responsible for oversight of outsourcing and third-party risk. This tends to make UK financial services buyers particularly thorough in their due diligence, because someone's name is attached to the decision. Expect detailed questions about business continuity, data location, sub-contracting arrangements, and your own financial stability.

Healthcare

Selling into US healthcare means navigating HIPAA. Any vendor that will create, receive, maintain, or transmit Protected Health Information (PHI) must sign a Business Associate Agreement. But the BAA is just the starting point, healthcare organizations are expected to conduct due diligence on their business associates and can face penalties if a vendor breach traces back to inadequate vetting. Expect questions specifically about PHI handling, breach notification procedures, and encryption practices.

Government

Government contracts bring their own alphabet soup: FedRAMP for cloud services, NIST 800-53 for security controls, and increasingly CMMC for defence contractors. What makes government different is the concept of flow-down requirements—the security obligations in the prime contract often extend to subcontractors and vendors. You may find yourself answering questionnaires not from the government directly, but from a contractor who needs to demonstrate that their entire supply chain meets federal standards.

2. What a security questionnaire actually is

The most important thing to understand about security questionnaires is that they are not a pass/fail exam, they are a way for your potential customer to build up a risk profile of your business based on a whole range of factors…

The most important thing to understand about security questionnaires is that they are not a pass/fail exam

The kind of data you will process

This is often where the questionnaire starts, and it determines how much scrutiny everything else receives. Will you handle personally identifiable information? Financial data? Health records? Intellectual property? The more sensitive the data, the more rigorous the expectations. A tool that only processes anonymized usage metrics will face far fewer questions than one that stores customer PII. Be precise here. Vague answers like "we may process some personal data" will only generate follow-up questions.

The security posture of your hosting and technical infrastructure

Expect detailed questions about where your application runs, how it is architected, and what protections are in place. This includes encryption (at rest and in transit), access controls, network security, vulnerability management, and incident response. If you are hosted on a major cloud provider like AWS or GCP, you can lean on their certifications for the physical and infrastructure layers. But you are still responsible for how you have configured and secured your application on top of that foundation.

The third parties you rely on to deliver the service

This is where TPRM comes full circle. Just as your customer is assessing you, they expect you to assess your own vendors. Who hosts your infrastructure? Who processes payments? Do you use any sub-processors for data handling? What happens if one of them has a breach? Your customer's risk extends through you to your vendors, so expect questions about your own vendor management practices and possibly requests for a list of sub-processors.

Your internal business processes that impact security and reliability

Security is not just technical. It is operational. Questionnaires probe how you handle access management, employee onboarding and offboarding, background checks, security training, change management, and business continuity. A common area of focus is the principle of least privilege: who in your organization can access customer data, and how do you ensure that access is appropriate and auditable? For a small team, the honest answer might be "a limited number of people with a genuine need," which is often perfectly acceptable if you can demonstrate the controls around it.

The business criticality of the service you will provide

Not all vendors are equal in the eyes of a TPRM program. A tool that sits in the critical path of your customer's operations (their CRM, payments infrastructure, or core product) will receive far more scrutiny than a nice-to-have utility. The questionnaire helps the buyer understand what happens if your service goes down or is compromised. What is your uptime track record? Do you have an SLA? What is your disaster recovery plan? The more critical your service, the more robust your answers need to be.

Not all vendors are equal in the eyes of a TPRM program. A tool that sits in the critical path of your customer's operations will receive far more scrutiny than a nice-to-have utility.

Legal and contractual

Liability caps, indemnification, insurance coverage (particularly cyber liability and E&O), jurisdiction, and how you handle law enforcement requests or subpoenas. Larger enterprises often have non-negotiable positions on some of these, so expect your contracts to get scrutinized alongside your technical controls.

Compliance and certifications

Certifications like SOC 2, ISO 27001, PCI DSS, and HIPAA serve as shorthand for security maturity. They do not eliminate questions, but they can sometimes significantly reduce them and provide third-party validation that you do what you say you do. We will explore this more in section 5: “But we have SOC 2 / ISO 27001…”

Privacy

Privacy is distinct from security and has grown substantially as a questionnaire topic since GDPR came into force. Expect questions about your compliance with data protection regulations like GDPR and CCPA, your process for handling data subject access requests, and your data retention policies. Many questionnaires will ask whether you have appointed a Data Protection Officer and how you handle cross-border data transfers. The focus here is on demonstrating that you treat personal data as a liability to be minimized and managed, not just an asset to be protected.

Secure development practices

Questionnaires probe how you build and maintain your software, covering secure coding standards, code review processes, static analysis tools, and penetration testing. Vulnerability management is a key focus: how you identify, prioritise, and remediate security issues, and how quickly patches reach production. The underlying concern is straightforward. A vulnerability in your code becomes your customer's problem, so they want confidence that security is embedded in your development lifecycle rather than treated as an afterthought.

Product-specific access controls

Enterprise buyers care deeply about how their users will authenticate and what controls exist within your product. Support for Single Sign-On (SSO) is often a hard requirement, as it allows customers to enforce their own identity policies and simplify offboarding when employees leave. Multi-factor authentication, role-based access control, and audit logging are also common expectations. The goal is to ensure that the customer retains control over who accesses their data within your platform, rather than relying solely on your internal safeguards.

Data residency and portability

Questionnaires address where data is stored geographically and whether it can be restricted to specific regions. For customers in regulated industries or those subject to data protection laws like GDPR, regional data storage can be a dealbreaker. Equally important is what happens when the relationship ends. Customers want assurance that they can export their data in a usable format and that you will delete it completely upon request. Nobody wants to be locked into a vendor, and demonstrating a clean exit path builds trust from the outset.

3. The legal and insurance implications of security questionnaires

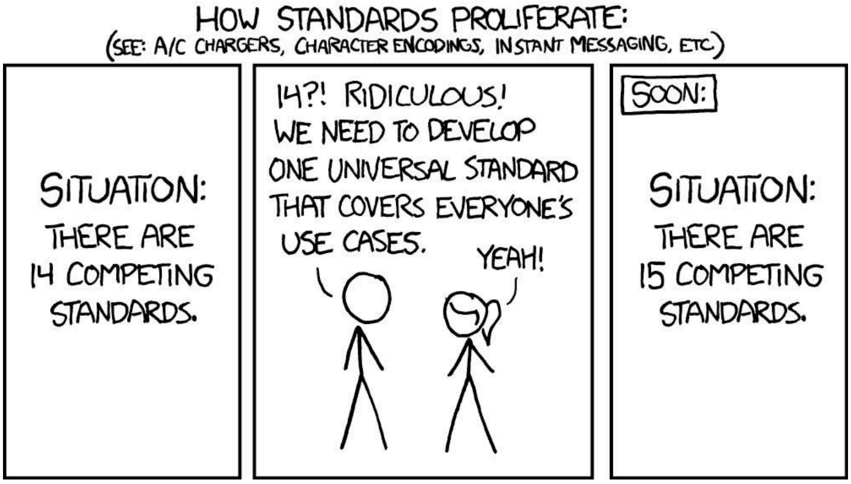
Your questionnaire responses are not just a box-ticking exercise. They often become contractual representations. Many enterprise contracts include clauses stating that your questionnaire responses are accurate and that you will notify the customer if anything material changes. Some go further and incorporate the questionnaire by reference into the agreement itself. This means a careless or optimistic answer can create legal exposure down the line.

If you claim to have annual penetration testing and do not, or say you encrypt data at rest when you only encrypt some of it, you may be in breach of contract before you have even delivered anything. Review your responses with the same care you would give to the contract itself, because functionally they are part of it.

Review your responses with the same care you would give to the contract itself, because functionally they are part of it.

Insurance adds another layer. Cyber liability insurers ask many of the same questions your customers do, and they are equally interested in accurate answers. Misrepresentation on an insurance application can void your coverage entirely, leaving you exposed precisely when you need protection most. There is also a practical connection between questionnaires and insurability. Strong security practices demonstrated through questionnaire responses can help you secure better coverage at lower premiums, while repeated gaps may make you harder to insure. Some enterprise customers now ask for proof of cyber insurance as part of their vendor assessment, so the two processes increasingly overlap. Getting your security house in order pays dividends on both fronts.

4. The major questionnaire families


HOW STANDARDS PROLIFERATE:
(SEE: A/C CHARGERS, CHARACTER ENCODINGS, INSTANT MESSAGING, ETC.)
SITUATION: THERE ARE 14 COMPETING STANDARDS.
14?! RIDICULOUS! WE NEED TO DEVELOP ONE UNIVERSAL STANDARD THAT COVERS EVERYONE'S USE CASES.
YEAH!
SOON:
SITUATION: THERE ARE 15 COMPETING STANDARDS.

If you have already been receiving security questionnaires you will have noticed that the questions in different questionnaires often overlap and can be very similar but are always worded slightly differently. That is because there is a whole universe of standards and systems for evaluating vendors. Here are the most common ones.

SIG (Standardized Information Gathering)

Pain rating: 😖😖😖😖

The SIG questionnaire is maintained by Shared Assessments and has become one of the most widely adopted formats in enterprise procurement. It is comprehensive, covering 18 risk domains including security, privacy, business continuity, and operational resilience. The full SIG can run to several hundred questions depending on which modules apply to your service. Many large enterprises use SIG as their default questionnaire, so completing one thoroughly and maintaining your answers in a reusable format pays dividends. The structured nature of SIG also makes it well-suited to automation, as the questions remain consistent across customers even if individual companies add supplementary sections.

SIG Lite

Pain rating: 😖😖

SIG Lite is a condensed version of the full SIG, designed for lower-risk vendors or as an initial screening tool before a more comprehensive assessment. It typically contains around 100-150 questions and covers the same risk domains as the full SIG but in less depth. Buyers often use SIG Lite for vendors who will not handle sensitive data or whose services are not business-critical. For early-stage startups, a completed SIG Lite can be a useful asset to have ready, as it demonstrates security maturity without requiring the extensive documentation needed for the full SIG. If a customer starts with SIG Lite and later requests the full SIG, much of your work carries over.

CAIQ

Pain rating: 😖😖😖

The Consensus Assessments Initiative Questionnaire (CAIQ) is published by the Cloud Security Alliance and focuses specifically on cloud service providers. It maps directly to the CSA Cloud Controls Matrix (CCM), which provides a framework of security controls tailored to cloud environments. CAIQ is particularly common when selling to customers who are themselves cloud-focused or who have adopted the CCM as part of their internal security program. The questionnaire is more technical than some alternatives, with detailed questions about virtualization, multi-tenancy, and cloud-specific concerns like data segregation between customers. If you are a SaaS vendor, expect to encounter CAIQ regularly, especially from technology companies and cloud-native buyers.

NIST-based

Pain rating: 😖😖😖😖

Many organizations, particularly those in the US federal supply chain or regulated industries, use questionnaires based on NIST frameworks. The two most common foundations are NIST SP 800-53 (a comprehensive catalogue of security controls used in federal systems) and the NIST Cybersecurity Framework (CSF), which organizes controls into five functions: Identify, Protect, Detect, Respond, and Recover. NIST-based questionnaires tend to be thorough and control-focused, often asking for specific evidence of implementation rather than simple yes/no answers. Government contractors and defence-adjacent companies are the most likely to send NIST-based assessments, but the framework has gained traction in private sector enterprises as well, particularly in financial services and critical infrastructure.

HECVAT

Pain rating: 😖😖😖

The Higher Education Community Vendor Assessment Toolkit (HECVAT) was developed specifically for colleges and universities and has become the standard questionnaire format in the education sector. It comes in three versions: HECVAT Full for high-risk vendors handling sensitive data, HECVAT Lite for lower-risk engagements, and the HECVAT On-Premise for locally hosted solutions. HECVAT questions align closely with concerns specific to educational institutions, including FERPA compliance (the US law protecting student records), accessibility requirements, and integration with campus identity systems. If you are selling to universities or edtech platforms, expect to complete HECVAT repeatedly. The good news is that EDUCAUSE maintains a community index where vendors can publish their completed assessments, allowing multiple institutions to reference your answers without requiring you to complete the questionnaire from scratch each time.

Custom/Bespoke questionnaires

Pain rating: 😖😖😖😖😖

The most common format, unfortunately. Many enterprises develop their own questionnaires tailored to their specific risk concerns, regulatory requirements, or industry. These range from well-structured documents clearly derived from established frameworks to chaotic spreadsheets that have grown organically over years of internal additions. Custom questionnaires are the most time-consuming because answers cannot be directly reused, though you will find significant overlap with standard formats once you have completed a few.

VSA (Vendor Security Alliance)

Pain rating: 😖😖

Created by a consortium of technology companies including Google, Uber, and Twitter, the VSA questionnaire aims to standardize vendor assessments across the tech industry. It is more concise than SIG and focuses on the controls that matter most to software and SaaS buyers. The VSA is freely available and has gained traction among technology companies, though it remains less common than SIG in traditional enterprises.

ISO 27001-mapped

Pain rating: 😖😖

Some organizations structure their questionnaires directly around ISO 27001 Annex A controls. These are particularly common among European buyers or companies that have adopted ISO as their primary security framework. If you are ISO 27001 certified, these questionnaires are relatively straightforward because your Statement of Applicability already documents your position on each control.

SOC 2-mapped

Pain rating: 😖😖

Similar to ISO-mapped questionnaires, these align directly to the Trust Services Criteria. They are often used by organizations that have standardized on SOC 2 as their vendor assessment baseline. Having a current SOC 2 report can significantly accelerate completion, as you can reference specific sections of the report rather than explaining each control from scratch.

PCI DSS SAQ

Pain rating: 😖😖😖😖

If your product handles payment card data, expect the PCI Self-Assessment Questionnaire. There are multiple SAQ types (A, A-EP, B, C, D, and others) depending on how you interact with cardholder data. These are highly prescriptive with specific technical requirements and little room for interpretation. PCI compliance is typically binary: you either meet the requirements or you do not.

CIS Controls-based

Pain rating: 😖😖

The Center for Internet Security publishes a set of prioritized security controls that some organizations use as their assessment framework. CIS Controls are organised into Implementation Groups (IG1, IG2, IG3) based on organizational maturity, which can work in your favour as a smaller vendor since IG1 represents a reasonable baseline without requiring enterprise-scale security operations.

Cyber Essentials / Cyber Essentials Plus

Pain rating: 😖

A UK government-backed scheme that provides a baseline of security controls. Many UK public sector contracts require Cyber Essentials certification, and it has gained adoption among private sector buyers as well. The basic Cyber Essentials is a self-assessment, while Cyber Essentials Plus involves external verification. It is less comprehensive than SOC 2 or ISO 27001 but serves as a useful entry point for smaller vendors.

GDPR/Privacy-specific assessments

Pain rating: 😖😖😖

Some organizations send dedicated privacy questionnaires separate from their security assessments, focusing specifically on data protection compliance. These cover lawful basis for processing, data subject rights, cross-border transfers, Data Protection Impact Assessments, and your arrangements with sub-processors. Expect these more frequently from European customers or those handling significant volumes of personal data.

4. The format wars: spreadsheets vs portals

At some point, somebody realised that emailing spreadsheets around was a suboptimal method for exchanging data between two organizations. Unfortunately, the replacement was not much better, in fact many would say it was meaningfully worse: The Portal.

Portals are generally part of broader GRC or TPRM platforms. New vendors are invited to create an account and answer the questions online. There is usually limited scope for collaborating with your team on answering questions - everything entered into the portal will be visible to your future customer. While some portals offer a nice user experience, others offer a more nostalgic take on UI / UX.

Here are the main portals you can expect to encounter:

OneTrust

OneTrust started as a privacy management platform and has expanded into a broad GRC suite covering privacy, security, and third-party risk. Their TPRM module is one of the most commonly encountered portals, particularly among larger enterprises and companies with significant privacy compliance requirements. The interface is polished but can feel heavyweight. Expect a formal onboarding process and a structured questionnaire experience.

ProcessUnity

ProcessUnity focuses specifically on third-party risk management and vendor lifecycle management. It is popular with mid-market and enterprise buyers who want a dedicated TPRM solution rather than a module within a larger GRC platform. The portal is straightforward and questionnaire-focused, without too many distractions.

Prevalent

Prevalent is a pure-play TPRM platform that combines questionnaire-based assessments with outside-in monitoring and risk intelligence. It is particularly common in financial services and healthcare, where rigorous vendor oversight is a regulatory expectation. The platform emphasises continuous monitoring alongside point-in-time assessments.

Venminder

Venminder targets the mid-market and is especially popular with banks, credit unions, and financial services firms. Beyond the portal, they offer managed services where their team can handle vendor assessments on behalf of the buyer. If you are selling to smaller financial institutions, Venminder is one of the most likely portals you will encounter.

Archer (RSA Archer)

Archer is a legacy GRC platform that has been around for decades and remains entrenched in large enterprises, government agencies, and highly regulated industries. The interface shows its age and the user experience can be clunky, but it is deeply embedded in organizations that have built years of processes around it. Expect a more formal, structured experience.

CyberGRX

CyberGRX operates on an exchange model. Rather than completing a separate assessment for each customer, you complete one comprehensive assessment that is then shared with multiple buyers in their network. This can significantly reduce duplication if several of your prospects use the platform. They also incorporate risk ratings and continuous monitoring alongside the assessment data.

Aravo

Aravo focuses on third-party risk and supplier lifecycle management, with strength in procurement-adjacent use cases. It is common in industries with complex supply chains like manufacturing, pharmaceuticals, and retail. The platform handles supplier onboarding, risk assessment, and ongoing monitoring across the vendor relationship.

Panorays

Panorays combines security questionnaires with automated outside-in assessments, giving buyers both self-reported data and independently gathered security signals. The platform emphasises speed and automation, which can work in your favour as a vendor. It is popular among technology companies and organizations that want a more dynamic view of vendor risk.

UpGuard

UpGuard is primarily known for security ratings and attack surface monitoring, but also offers questionnaire features. Buyers use it to get an outside-in view of your security posture based on publicly observable data (exposed services, SSL configuration, leaked credentials) alongside traditional questionnaire responses. If your external security hygiene is strong, UpGuard tends to be a friendly experience.

Custom-built

Many organizations, particularly large enterprises and government agencies, build their own vendor portals using platforms like ServiceNow, SharePoint, or entirely bespoke systems. The experience varies wildly. Some are well-designed and intuitive. Others are clearly the result of a decade of accumulated requirements and zero UX investment. Custom portals often lack features like saving progress or collaborative editing, so approach them with patience and save your work frequently.

5. “But we have SOC 2 / ISO 27001…”

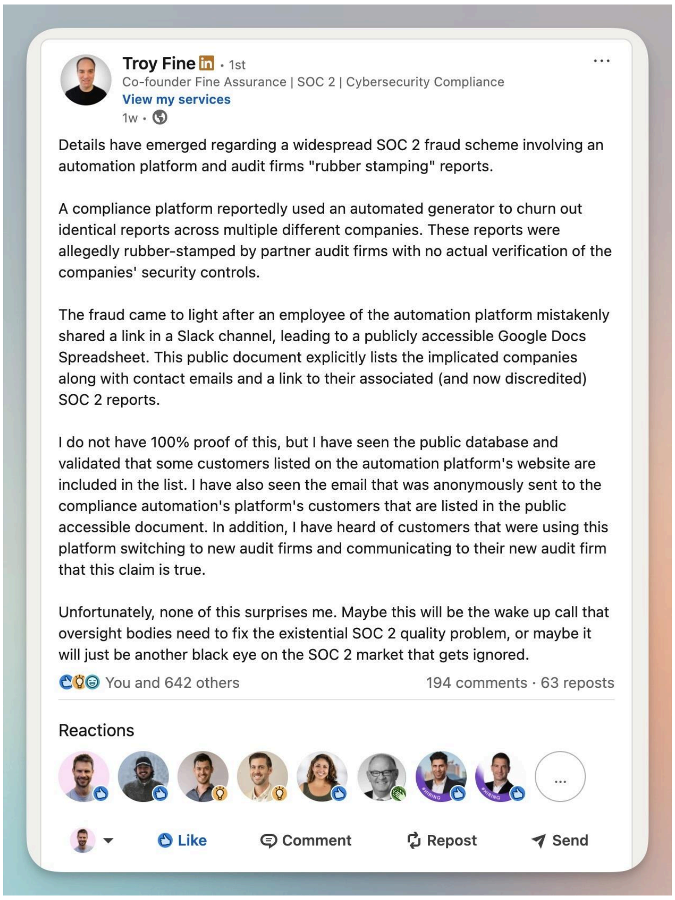
After receiving a few security questionnaires companies generally start to look around for a way to make the pain stop. SOC 2 and ISO 27001 are often marketed as standards that will “unlock enterprise deals” and “accelerate time to revenue”. The reality is… it depends.

For serious B2B software companies selling to mid-market or enterprise, getting SOC 2 or ISO 27001 is an inevitability. They are rarely hard requirements for closing enterprise deals, so often companies can delay until a Series-A or around 30 employees. However, they are flexible standards, so controls can be scaled to suit a 5 or 5000 person company.

Now, time for the bad news: SOC 2 and ISO 27001 will not stop security questionnaires. At best they might reduce the number of questions from 300 to 50. Some smaller customers with less mature TPRM programs may accept the SOC 2 report but most larger organizations will continue to do their own due diligence.

One very simple reason for this is that TPRM tools rely on having structured data about the hundreds of vendors that a typical large enterprise uses. If a vendor sends in a SOC 2 report, someone still needs to answer the specific security questions and most importantly attest they are relevant and correct.

At the time of writing there is something of a scandal rocking the SOC 2 world. A “SOC-in-a-box” provider has been accused of rubber stamping identical SOC 2 reports for startups.



Troy Fine · 1st
Co-founder Fine Assurance | SOC 2 | Cybersecurity Compliance
View my services
1w ·

Details have emerged regarding a widespread SOC 2 fraud scheme involving an automation platform and audit firms "rubber stamping" reports.

A compliance platform reportedly used an automated generator to churn out identical reports across multiple different companies. These reports were allegedly rubber-stamped by partner audit firms with no actual verification of the companies' security controls.

The fraud came to light after an employee of the automation platform mistakenly shared a link in a Slack channel, leading to a publicly accessible Google Docs Spreadsheet. This public document explicitly lists the implicated companies along with contact emails and a link to their associated (and now discredited) SOC 2 reports.

I do not have 100% proof of this, but I have seen the public database and validated that some customers listed on the automation platform's website are included in the list. I have also seen the email that was anonymously sent to the compliance automation's platform's customers that are listed in the public accessible document. In addition, I have heard of customers that were using this platform switching to new audit firms and communicating to their new audit firm that this claim is true.

Unfortunately, none of this surprises me. Maybe this will be the wake up call that oversight bodies need to fix the existential SOC 2 quality problem, or maybe it will just be another black eye on the SOC 2 market that gets ignored.

The last few years have seen a surge of new providers promising “SOC 2 in 7 days” or “ISO in 24 hours”. It is our opinion that this dilution of the seriousness of these programs will only lead to more security due diligence from potential customers.

Delve.co
Get SOC 2 done before you figure out what SOC 2 is.
Today, compliance is done in Delve.
OUTFRONT/

With all that being said, there is still tremendous value in getting SOC 2 or ISO 27001. If taken seriously, they will be a big level up for your internal processes and will meaningfully make your organization more secure and resilient. The audit process forces you to document things you have been meaning to document, formalize access controls that were informal, and actually think through incident response before you need it.

You'll also find that having a certification simplifies sales conversations, not because it eliminates questionnaires, but because it gives you a credible baseline. Buyers trust you more quickly, and their security teams have less to prove to their own leadership. The mistake is expecting certifications to be a shortcut. They are not. But as a forcing function for getting your house in order, they are hard to beat.

6. Surviving security questionnaires - what doesn’t work

Before we look at how to efficiently and effectively deal with security questionnaires, let's look at some common approaches that seem sensible but end up costing you more time than they save.

Copy-pasting from old questionnaires

This is everyone's first instinct. You have answered these questions before, surely you can just find the old spreadsheet and copy across? In theory, yes. In practice, it is a minefield.

The first problem is finding the right answer. Questions that seem identical are often worded just differently enough that your old answer does not quite fit. "*Describe your access control procedures*" and "*How do you manage user access to production systems*?" are asking for the same thing but good luck searching your folder of old spreadsheets for a match.

The second problem is context. Old answers were written for a specific customer and may contain language that made sense for that deal but sounds strange in a new one. We have seen answers that reference a customer by name, or describe integrations that were specific to that deployment. Pasting these without careful review is an easy way to look careless.

The third problem is accuracy. Your security posture changes over time. You implement new controls, deprecate old ones, switch providers, update policies. An answer that was true eighteen months ago might be misleading today. Without a system to track what has changed, you are essentially guessing whether your old answers are still valid.

Delegation

At some point you will look at your to-do list, see "complete security questionnaire" sitting there for the third week running, and think: surely someone else can do this?

Security questionnaires sit at an awkward intersection of technical knowledge, policy awareness and commercial context.

The challenge is that security questionnaires sit at an awkward intersection of technical knowledge, policy awareness and commercial context. Your engineers know how the code works and what infrastructure you are running, but they do not necessarily know your security policies or how to frame answers in a way that satisfies a reviewer. They also have better things to do with their time than fill out spreadsheets.

Your ops lead or customer success manager might be keen to help and can probably handle the straightforward questions. But they will come back to you for the hard ones, which, in our experience, is about eighty percent of them. You end up doing most of the work anyway, just with more back and forth.

There is also a hidden issue with delegation: small teams often need to make policy updates or implement new controls to meet a customer's requirements. The person filling out the questionnaire needs the authority to say "we do not do this today but we can commit to implementing it by X date", and that is usually a founder-level decision.

There is no quick win here. The best you can do is make sure your knowledge base and policies are well maintained, clearly written and accessible to whoever ends up doing the questionnaires. If you find yourself wanting to delegate, it might be a sign that you need to automate instead.

Throwing it into ChatGPT

This one is tempting. You have a pile of policy documents, maybe some old questionnaires, and a tool that can read them all and generate plausible-sounding answers. What could go wrong?

Quite a lot, it turns out. The core issue is hallucination. Even when you provide reference documents, large language models will confidently generate answers that sound right but are subtly wrong. They might claim you have a control you do not have, or describe a process that does not match how you actually operate. These mistakes are hard to spot because the language is so fluent.

Traceability is another problem. When a reviewer asks a follow-up question or an auditor wants to see evidence, you need to know exactly where an answer came from. LLMs do not provide precise references, they synthesize across their input and generate something new. Good luck explaining to a customer that your answer was "based on" your policies but you cannot point to the specific section.

Finally, there is tone and consistency. Getting the right level of detail, the right degree of confidence, and a consistent voice across hundreds of questions is genuinely difficult with raw prompting. You end up spending almost as much time reviewing and editing the output as you would have spent writing the answers yourself.

None of this means AI is useless for security questionnaires, far from it. But using ChatGPT as a first-pass answer generator without proper grounding, review workflows and traceability is a recipe for problems down the line.

7. The efficient way to deal with security questionnaires

Get your policies in order

Every startup begins without formal policies. The team is small, experienced, and has a strong sense of the right way to do things. Writing it all down feels like unnecessary overhead. But without documented policies, security questionnaires become a guessing game where you are trying to remember what you actually do and whether that is still true.

A basic set of policies gives you a single source of truth.

A basic set of policies gives you a single source of truth. When a questionnaire asks about your access control procedures or incident response process, you are not reconstructing the answer from memory or digging through old spreadsheets. You are pointing to a document that reflects how your team actually operates. This also makes delegation possible, since anyone on your team can reference the same policies and give consistent answers.

Start with the essentials: an Information Security Policy, Access Control Policy, Incident Response Plan, Disaster Recovery and Business Continuity Plan, and Data Management Policy. You do not have to write these from scratch. There are good open source templates available, and tools that can generate policies based on your specific business context.

Build and maintain a knowledge base

A centralized knowledge base of previous questions and answers will save you significant time. The challenge is that questionnaires come in many formats and phrasings. "Describe your access control procedures" and "How do you manage user permissions?" are asking for the same thing, but keyword search will not connect them.

Use something like Notion rather than a spreadsheet. Questionnaire responses tend to be text heavy, and spreadsheets make it hard to scan and find what you need. Notion also gives you automatic timestamps so you can see how fresh each answer is, and better search functionality when you are dealing with hundreds of entries. Add alternate phrasings for each question so you can find the right answer even when the wording differs.

Check out our Notion security questionnaire template.

The hard part is maintenance. After each questionnaire, take twenty minutes to review what you have. Add new questions that came up, update answers where things have changed, and remove any customer-specific language that crept in. This is tedious and easy to skip, but without it your knowledge base gradually drifts out of sync with reality. Six months later you will be copying answers that no longer reflect how your team actually operates.

Be precise, not aspirational

When answering questions, describe what you actually do today, not what you plan to do or what you think sounds good. It is tempting to round up, to say you have "24/7 monitoring" when really you check logs daily, or claim you have a formal change management process when it is more like "we talk about it in Slack before deploying." Reviewers are experienced at spotting answers that sound too polished.

Do not be afraid to say no. Security questionnaires are used to create a risk profile of your business relative to the criticality of the service you provide. For medium or low risk products, it is perfectly acceptable to state that you do not have a sustainability policy or SLA-backed recovery time objectives. A clear "no" is better than a vague answer that creates ambiguity.

> *The goal is not to look impressive. The goal is to create an accurate record that you can stand behind if anyone ever asks for evidence.*

Assume your answers will be audited. If you have a data breach and your questionnaire claimed you had certain controls in place when you did not, you have given them ammunition for a legal claim. The goal is not to look impressive. The goal is to create an accurate record that you can stand behind if anyone ever asks for evidence.

8. Dedicated tools

GRC platforms

Governance, Risk and Compliance platforms like Vanta and Drata have become popular with startups pursuing SOC 2 or ISO 27001. Their primary function is evidence collection: connecting to your infrastructure, pulling configurations, and packaging everything for auditors. Most of them have added security questionnaire modules as a secondary feature.

The challenge is that these modules tend to be an afterthought. They work, but they are not built for teams who need to move quickly through questionnaires. The user experience is designed for compliance specialists, not founders or engineers who are trying to get back to product work. You also typically cannot access the questionnaire functionality without buying the full platform, which means paying for a lot of capability you may not need yet.

Pricing is another consideration. GRC platforms are designed for companies who are already committed to a formal compliance program. If you just need to respond to questionnaires efficiently and are not yet pursuing certification, you end up paying enterprise prices for a small slice of the functionality.

TPRM platforms

Third Party Risk Management platforms sit on the other side of the table. These are the tools that enterprises use to send questionnaires to vendors like you, assess risk, and manage their vendor portfolio. Names you might encounter include OneTrust, ServiceNow, and Prevalent.

Some of these platforms also offer functionality for responding to questionnaires, not just sending them. The logic is that if you are already using the tool to assess your own vendors, you might as well use it to manage inbound questionnaires too. In practice, this capability is aimed at large organizations with dedicated procurement and compliance teams.

For smaller teams, TPRM platforms are almost certainly overkill. They are priced for enterprises, designed for specialists, and assume you have the headcount to manage complex workflows. If you are a ten-person startup, this is not your tool.

Specialist questionnaire tools

A newer category of tools focuses specifically on security questionnaire response. These range from products like Conveyor, which serve sales operations teams at larger companies processing hundreds of questionnaires per year, to tools built for smaller teams who need something lightweight and fast.

The enterprise-focused options tend to share some characteristics: long sales cycles, demo-required onboarding, and pricing that assumes a dedicated compliance function. They are powerful, but if you are a small team trying to close a deal this week, waiting two weeks for a demo is not practical.

ResponseHub is built for smaller teams who need to move quickly. It is self-serve, so you can start immediately without scheduling a call. Every question includes a one-click explainer tailored to your business context, so you are not left wondering what "RBAC" means or why someone is asking about your BCP. The AI generates answers with confidence ratings and clear citations back to your policies and knowledge base, so you know exactly where each response came from.

Conclusion

It might not feel like it, but security questionnaires are your prize. It means you've built a valuable product that an established business is willing to invest time and energy into figuring out how to adopt it. It means you are doing something right.

It also means you now need a robust security posture across your organization and you need to effectively convey this to your potential customers. The way this needs to be done, whether in a spreadsheet or portal, is time-consuming, tedious work.

The tactics in this guide will help. Getting your policies documented, building a knowledge base, being precise rather than aspirational, understanding what reviewers actually care about. These practices can make the process meaningfully more efficient, perhaps 20 or 30 percent faster. But if you want to make it ten times easier, you will need tooling. The right tool depends on your organization's size and complexity. If you are already deep into a formal compliance program with dedicated staff, a full GRC suite might make sense. For smaller teams who need to move fast without enterprise overhead, an AI-native tool built specifically for questionnaires is the better fit. That is why we built ResponseHub. We have been on the receiving end of these questionnaires and know how much time they consume. Our goal is to give you that time back so you can focus on the work that actually moves your business forward.