



Accelerate Security Reviews with Questionnaire Automation

Stop losing deals to slow, manual security reviews. There's a smarter way.

Security Reviews Are Killing Your Deal Velocity

23 Assessments/Month

The average vendor responds to 23 security assessments per month — each taking ~3.5 hours. That's **80+ hours monthly**, the equivalent of half an FTE.

\$700–\$2,000 Per Questionnaire

A mid-complexity questionnaire (150–200 questions) costs **\$700–\$900** in fully loaded SE and GRC labor. HIPAA and EU AI Act formats run **\$1,000–\$2,000** each.

\$72,000 Hidden Labor Cost

Teams handling 100 questionnaires/year spend roughly **\$72,000** in **direct labor** — never tracked, never budgeted, never visible on any cost report.





The Friday Scramble: A Story You Know

A 200-question SIG Lite lands Thursday afternoon. The deal is six figures. The prospect wants it back by Monday.

The CTO gets pulled off product work. Someone digs through Confluence for last year's answers. Three people spend their **entire Friday** writing responses they've written a dozen times before.

⚠ This is the hidden tax on every enterprise sales cycle — and almost no one is measuring it.

72% of Questions Are the Same Every Time

72%

Functionally Identical

One two-person security team found that 72% of questions across 43 questionnaires were functionally identical — just different phrasing, same underlying question.

8,000

Questions Answered in 2025

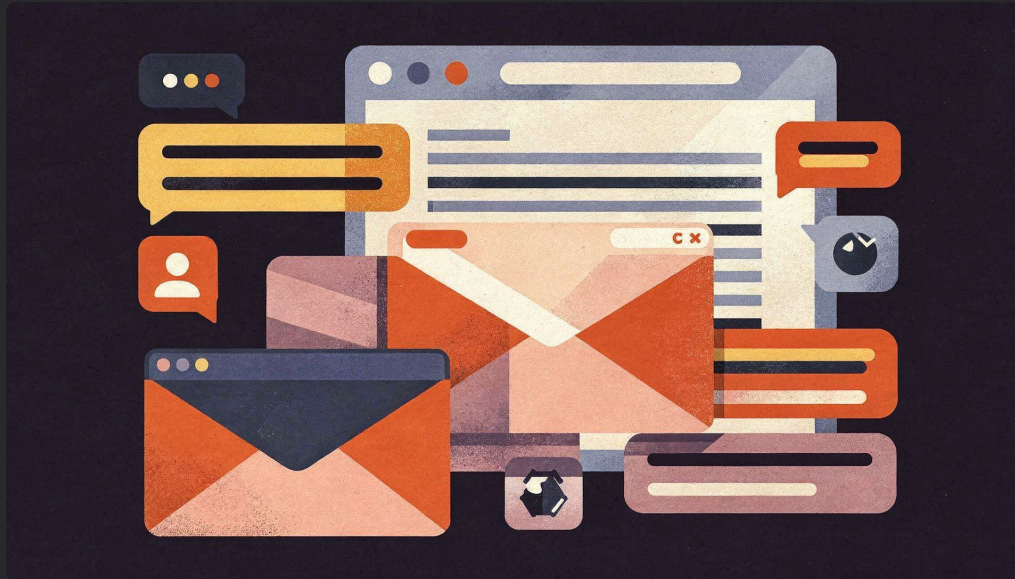
That same team answered approximately 8,000 questions across 43 questionnaires in a single year — almost all repeat work.

280hrs

Wasted on Copy-Paste

280 hours spent copying and pasting from previous responses. That's **3.5 months** of one person's full-time capacity — gone.

Why Manual Workflows Break Down



Scattered Knowledge

Policies, audit reports, and prior responses live in Confluence, Google Drive, and email threads — no single source of truth.

No Single Owner

Sales, Security, and GRC all share responsibility. Coordination overhead compounds delays at every handoff.

Accuracy Risk

Copy-pasting stale answers introduces compliance gaps and inconsistencies across submissions.

Context-Switching Tax

Past ~2 concurrent questionnaires per SE, per-questionnaire time and error rates rise together — costs stop scaling linearly.

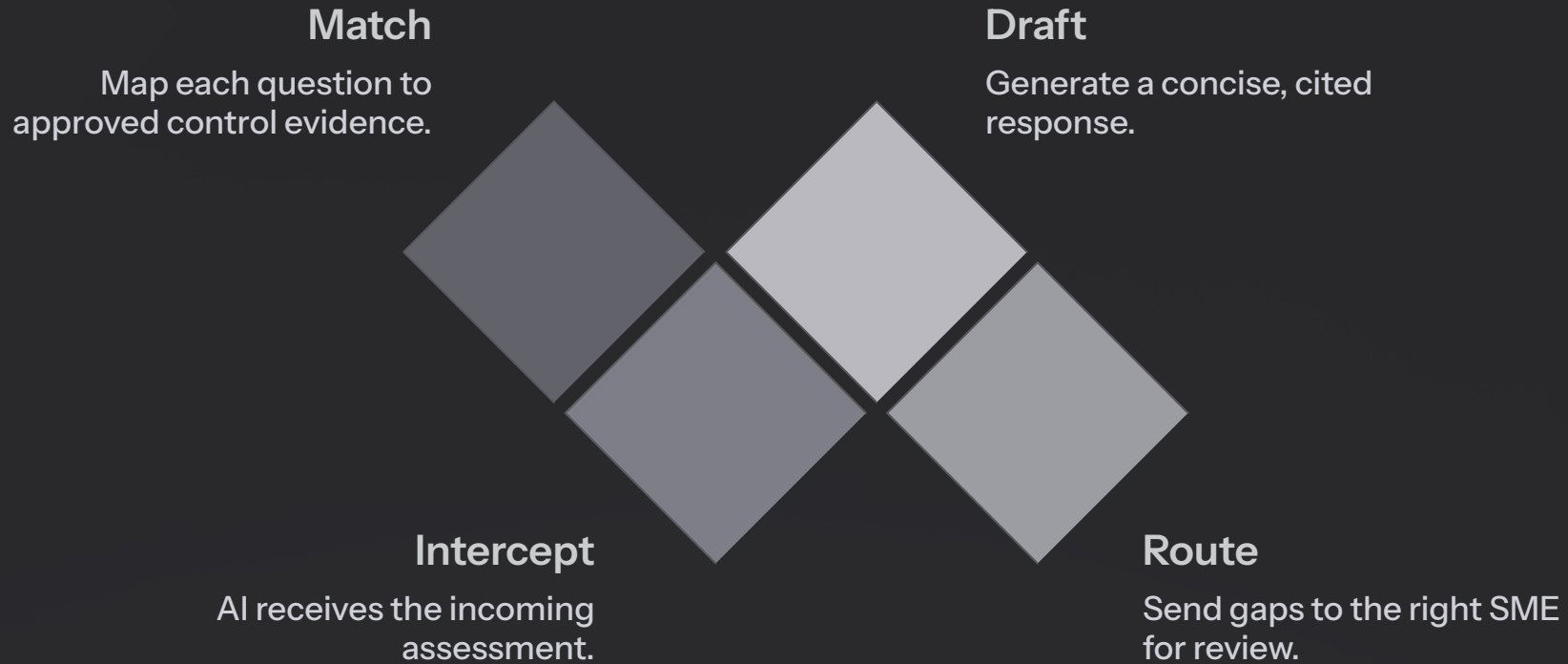


CHAPTER 1

The Automation Advantage

From fire drill to system — how AI transforms the questionnaire response process.

What Security Questionnaire Automation Actually Does



Automation doesn't replace your security team — it eliminates the manual triage, the Confluence archaeology, and the copy-paste marathon. The output is a **complete, auditable response package** ready for buyer submission, with every answer traced back to approved evidence.

The Results Speak for Themselves

80–90% Time Reduction

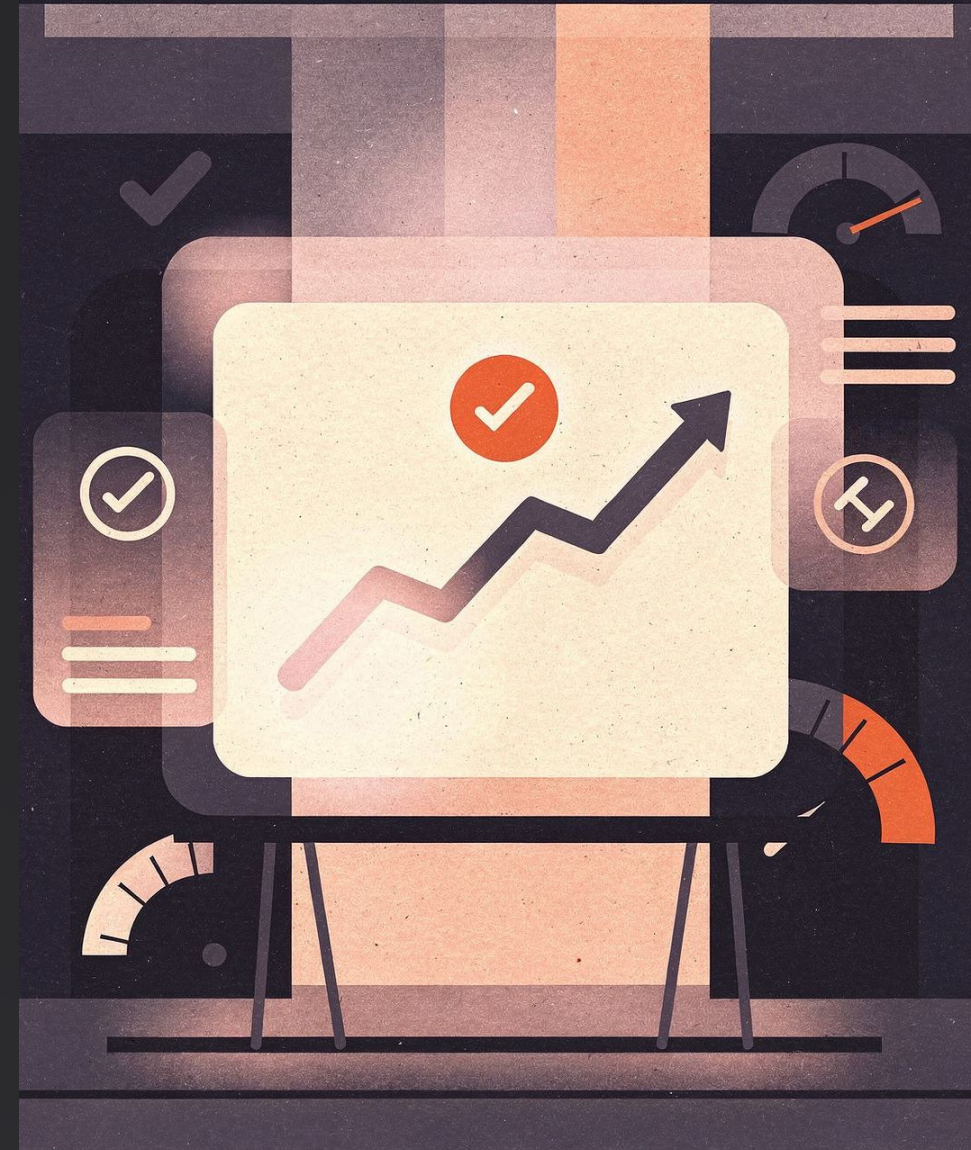
Per questionnaire, automation slashes response time by **80–90%** — turning a multi-day scramble into hours.

95%+ First-Draft Accuracy

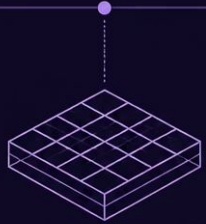
Teams that invest two weeks in knowledge base setup consistently achieve **above 95% accuracy** on first drafts.

60–70% Auto-Answered

Companies with SOC 2 can automatically answer **60–70% of any standard questionnaire** by pointing to specific controls — with zero manual effort.



Frameworks Covered Out of the Box



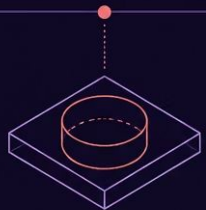
SIG/SIG Lite

(~1,800 control points across 21 domains, gold standard for financial services)



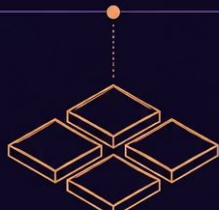
CAIQ v4

(cloud-specific controls aligned to CSA framework)



SOC 2 / ISO 27001 / NIST CSF

(map directly to 60–70% of any standard questionnaire)



VSAQ + Custom Formats

(flexible ingestion for bespoke buyer templates)

Universal Framework Coverage

The most common questionnaires — SIG, CAIQ, VSA, and custom variants — map directly to the frameworks your security team already maintains.

That means your existing SOC 2 report, ISO 27001 certification, and NIST CSF documentation are already doing most of the work. Automation simply connects the dots — instantly, accurately, at scale.



One well-maintained knowledge base covers the vast majority of all incoming questionnaire formats.



CHAPTER 2

How to Implement It Right

Eight steps from chaos to a system that runs itself.

The 8-Step Implementation Playbook

01

Audit Your Workflow

Map exactly where time is lost today — hours per questionnaire, handoff delays, rework loops.

02

Centralize Documentation

Consolidate all policies, audit evidence, and prior responses into a single knowledge base.

03

Map Controls to Frameworks

Align your existing SOC 2, ISO 27001, and NIST CSF evidence to common questionnaire domains.

04

Connect & Pilot

Integrate knowledge sources with the automation platform, then run a pilot on 2–3 real questionnaires before full rollout.

05

Configure, Review & Measure

Set up SME routing for edge cases, establish approval workflows, then track hours saved, throughput, and deal velocity.

The Critical Prerequisite: Your Knowledge Base

Automation quality is entirely determined by what you feed it. There are no shortcuts here — but the investment pays back immediately.

- Consolidate your **SOC 2 report**, security policies, prior approved responses, and audit evidence into one structured repository
- Teams that **skip documentation setup** see first-draft accuracy below 60%
- Teams that invest **two weeks in setup** see accuracy consistently above 95%

✓ Two weeks of setup work unlocks 80–90% time savings on every questionnaire from that point forward.





Choosing the Right Questionnaire Format

Match Depth to Materiality

Over-engineering your questionnaire creates supplier fatigue and degrades response quality. Assess depth proportional to vendor criticality — not one-size-fits-all.

The Stakes Are High

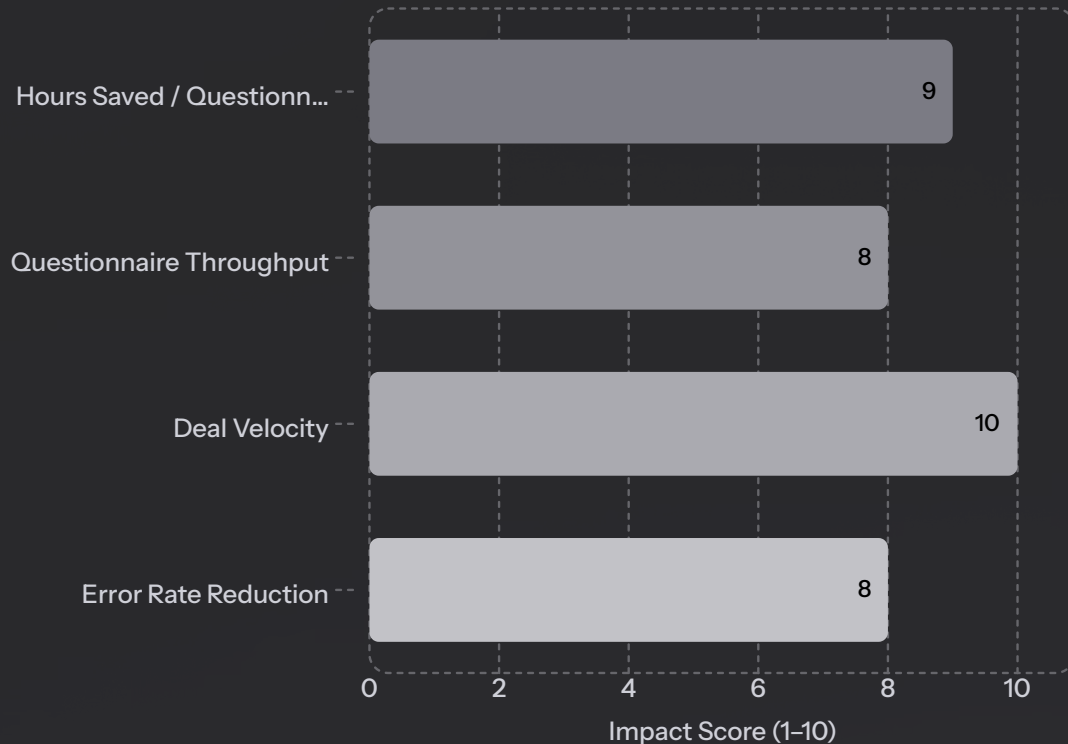
Completion rates varied by **40 percentage points** and time-to-completion by a **factor of 4** depending on questionnaire choice. Format selection materially changes outcomes.

Regulatory Expectation

Under **DORA Article 30**, regulators explicitly expect proportionality in due diligence depth. Disproportionate assessments are not just inefficient — they may be non-compliant.

Measuring ROI: What to Track

ROI Metric



Four Metrics That Matter

- **Hours saved** per questionnaire vs. your manual baseline — the most immediate indicator
- **Questionnaire throughput** per quarter — how much volume your team can now absorb without headcount increases
- **Deal velocity** — weeks removed from the sales cycle per deal closed
- **Error rate** — compliance gaps caught before submission, not after

Track these from day one. The ROI story writes itself within the first quarter.

Turn Security Reviews Into a Competitive Advantage

Buyers are more sophisticated than ever. The people running these reviews increasingly have compliance or security backgrounds — **they know what a substantive answer looks like, and they know when someone is stalling.**



Fast = Trust

Automation transforms the security review from a bottleneck into a **trust signal**. Fast, accurate, auditable responses win deals.



Start in 30 Days

Centralize your knowledge base, run a pilot on real questionnaires, and measure the impact — all within 30 days.



Differentiate Now

The vendors who respond in hours — not weeks — are the ones who close. Make automation your competitive edge before your competitors do.



Sources

- [How to Increase Efficiencies in Vendor Assessment Process? | Whistic](#)
- [The real cost of manual questionnaires | Wolfia](#)
- [Security Questionnaire Automation: From Fire Drill to System | Truvo](#)
- [Your security team answers the same vendor questionnaire 40 times a year | Moonpool](#)
- [How to Automate Security Questionnaire Responses | Tribble](#)
- [SIG vs CAIQ vs Custom: Vendor Questionnaire Decision Matrix | RiskImmune™](#)