CAREFUL SECURITY

The Security Partner Evaluation Guide

20 Questions to Ask Before You Hire

Choosing a security and compliance partner is one of the most consequential decisions you'll make. The wrong choice costs you time, money, and potentially your reputation. The right partner accelerates your growth, protects your business, and becomes a trusted advisor for years.

This guide gives you the exact questions to ask — and what good answers look like. Use it to evaluate any security consultant, compliance firm, or vCISO provider. The best partners will welcome these questions. The rest will squirm.

PRICING & TRANSPARENCY

Question 1

Is your pricing fixed, or will it change mid-project?

Why it matters: Hourly billing incentivizes delays. Fixed pricing aligns your consultant's success with yours.

✓ Green flag: Published pricing on their website. No 'it depends' answers.

Question 2

What exactly is included vs. charged as add-ons?

Why it matters: Hidden fees for 'policy customization' or 'extra meetings' can double your final cost.

✓ Green flag: Clear scope document listing every deliverable before you sign.

Question 3

Can I see your full pricing before a sales call?

Why it matters: If they won't share pricing, they're sizing you up to maximize what they can charge.

✓ Green flag: Transparent pricing page. No forms required to see costs.

EXPERTISE & CREDENTIALS

Question 4

Who actually does the work — partners or junior staff?

Why it matters: Many firms sell senior talent, then assign fresh graduates to your project.

✓ Green flag: Named team members with bios. Direct access to senior consultants.

Question 5

How many certifications have you completed this year?

Why it matters: Experience compounds. A firm with 50+ certifications has seen every edge case.

✓ Green flag: Specific numbers, not vague claims. Case studies with outcomes.

Question 6

Do you specialize in my industry?

Why it matters: Healthcare, FinTech, and SaaS have different compliance nuances. Generalists miss details.

✓ Green flag: Industry-specific case studies. Knowledge of your regulatory landscape.

Question 7

Can you handle multiple frameworks simultaneously?

Why it matters: SOC 2 + ISO 27001 + HIPAA share 60-70% overlap. Doing them together saves time and money.

✓ Green flag: Multi-framework experience. Integrated approach, not sequential projects.

DELIVERY & TIMELINE

Question 8

What is your guaranteed timeline?

Why it matters: Vague timelines ('4-6 months') often become 9-12 months. You need a date.

✓ Green flag: Specific commitment (e.g., '90 days'). Written into the contract.

Question 9

What happens if YOU miss the deadline?

Why it matters: If there's no penalty for delays, there's no incentive to prioritize your project.

✓ Green flag: Money-back guarantee or fee reduction for missed timelines.

Question 10

How much of my team's time is required?

Why it matters: Some consultants dump work on your staff. Others handle everything.

✓ Green flag: Clear hour estimates per role. Turnkey options available.

TECHNOLOGY & TOOLS

Question 11

Do you provide software/platforms, or just consulting?

Why it matters: Spreadsheets don't scale. Modern compliance requires continuous monitoring.

✓ Green flag: Integrated platform included. Real-time dashboards and evidence collection.

Question 12

How do we maintain compliance after certification?

Why it matters: Certification is day one, not the finish line. Auditors return annually.

✓ Green flag: Ongoing monitoring tools. Clear maintenance program options.

Question 13

Can I see dashboards and progress in real-time?

Why it matters: You shouldn't wait for weekly status calls to know where you stand.

✓ Green flag: Client portal access. Live progress tracking from day one.

vCISO & STRATEGIC SECURITY

Question 14

If I need strategic security leadership, what does that look like?

Why it matters: Compliance is tactical. Security strategy is what protects you long-term.

✓ Green flag: Defined vCISO service tiers. Clear deliverables (roadmaps, board decks).

Question 15

Can you represent us to our board, customers, or auditors?

Why it matters: Your security leader should be able to speak on your behalf externally.

✓ Green flag: Executive communication experience. Board presentation samples.

Question 16

How do you handle incidents if they occur?

Why it matters: Breaches happen. Your partner should have a response plan, not just prevention.

✓ Green flag: Incident response included. 24/7 availability for emergencies.

ASSESSMENTS & TESTING

Question 17

What credentials do your pentesters hold?

Why it matters: OSCP, GPEN, GWAPT matter. Uncertified testers miss critical vulnerabilities.

✓ Green flag: Named testers with verifiable certifications. Methodology documentation.

Question 18

What's actually in a risk assessment deliverable?

Why it matters: A 5-page generic report isn't worth $15K. You need actionable specifics.

✓ Green flag: Sample deliverables available. Risk register, roadmap, executive summary.

Question 19

Do you remediate findings or just report them?

Why it matters: Knowing you have 47 vulnerabilities isn't helpful if no one fixes them.

✓ Green flag: Remediation services available. End-to-end accountability.

TRUST & REFERENCES

Question 20

Can I speak with 3 recent clients in my industry?

Why it matters: References reveal reality. Any hesitation here is a red flag.

✓ Green flag: Immediate offer to connect you. Named clients on their website.

How to Score Your Evaluation

After meeting with a potential partner, rate them on each question:

2 points — Strong answer with evidence (case studies, samples, specific commitments)
1 point — Adequate answer but vague or lacking proof
0 points — Poor answer, deflection, or red flags

Scoring Guide:
35-40 points: Excellent partner candidate. Move forward with confidence.
25-34 points: Acceptable, but clarify weak areas before signing.
15-24 points: Significant concerns. Consider alternatives.
Below 15: Walk away. This engagement will likely disappoint.

Universal Red Flags

Regardless of their answers, walk away if you encounter:

• **No published pricing** — They're optimizing for maximum extraction, not fair value
• **Reluctance to provide references** — Happy clients are eager to recommend
• **Vague timelines** — "It depends" means they don't control their process
• **Junior staff on calls, seniors on proposals** — Bait and switch is coming
• **No technology platform** — Spreadsheet-based compliance doesn't scale
• **Pressure tactics** — Good partners don't need to manufacture urgency

---

Ready to Talk?

We created this guide because we're confident in our answers.

Ask us anything. We'll respond within 24 hours.

Careful Security
icare@carefulsecurity.com | +1-818-533-1402
www.carefulsec.com

Book a consultation: calendly.com/carefulsecurity

Our Services

Quick Fix 30 — Risk assessments, penetration testing, gap analysis (1-4 weeks)

Report Ready 90 — Full certification: SOC 2, ISO 27001, ISO 42001, HIPAA, PCI DSS (90 days guaranteed)

Securely Ever After — Ongoing vCISO services, managed security, continuous compliance

dashr.ai Platform — Real-time security dashboards, evidence automation, compliance monitoring (included Year 1 with all programs)

Cybersecurity with a Soul™