Axiom Sovereign

TECHNOLOGY SOVEREIGNTY ADVISORY

VIRTUAL CISO SERVICE — CLIENT EDUCATION GUIDE

Cyber Insurance Application Walkthrough

Common Questions · Accurate Answers · How a vCISO Helps

v1.0 — 2026

Axiom Sovereign LLC · Severna Park, MD · info@axiomsovereign.com · axiomsovereign.com

Cyber Insurance Application Walkthrough

How a vCISO Helps You Answer — and Survive — Your Cyber Insurance Renewal

Most organizations approach their cyber insurance renewal the same way they approach a tax return: fill in the boxes, sign at the bottom, hope for the best. This approach has become genuinely dangerous. Carriers are conducting post-incident investigations to verify application accuracy, and misrepresentation — even unintentional — is being cited as grounds for claim denial. This guide walks through the questions carriers actually ask, what they mean, what the correct answer looks like, and how a vCISO helps you get there.

The Stakes Have Changed

In 2020, cyber insurance was largely a commodity product with minimal underwriting scrutiny. Today, it is an actively underwritten product with specific technical requirements. Organizations that cannot demonstrate basic controls face: denial of coverage, policy exclusions that eliminate coverage for the most likely attack scenarios (ransomware, BEC), premium increases of 30–200%, and post-incident claim investigation that reviews your application answers against what was actually in place. A vCISO ensures your answers are accurate, your controls are real, and your program is positioned for favorable underwriting.

PART 1: THE QUESTIONS CARRIERS ACTUALLY ASK

The following table walks through the most common cyber insurance application questions, what the carrier is really evaluating, and how a vCISO helps you answer correctly.

Application Question	What the Carrier Is Really Asking	Correct Answer Looks Like	vCISO Role
Do you require multi-factor authentication for remote access and email?	Is your single largest attack surface (email + remote access) protected against credential theft?	"Yes — MFA is enforced via conditional access policy on all O365/Google accounts and VPN. Exceptions require documented approval."	Deploys and documents MFA enforcement. Verifies no gaps (shared mailboxes, service accounts).
Do you have an incident response plan?	If you are breached, will you know what to do in the first 72 hours? (GDPR notification deadline).	"Yes — documented IR plan reviewed within past 12 months, designates named response roles, includes regulatory notification procedures and IR firm contact."	Develops, documents, and exercises IR plan. Ensures notification timelines are accurate for applicable regulations (HIPAA 60-day, GDPR 72-hour, state breach laws).

Application Question	What the Carrier Is Really Asking	Correct Answer Looks Like	vCISO Role
Do you perform regular backups? Are they tested?	Can you recover from ransomware without paying the ransom?	"Yes — daily backups to Azure with immutability enabled and weekly offsite rotation. Restoration tested quarterly. Last test date: [DATE]. Result: successful."	Establishes backup policy, immutability configuration, and testing cadence. Documents test results for evidence purposes.
Do you conduct security awareness training?	Are your employees a security asset or your biggest liability?	"Yes — all staff complete annual training. Phishing simulations conducted quarterly. Q1 2026 click rate: 4%. Completion tracked individually."	Designs training program, documents completion, and tracks metrics that demonstrate effectiveness.
Is RDP exposed to the internet?	Are you an easy ransomware target? Exposed RDP is the #1 ransomware initial access vector.	"No — RDP is not exposed to the internet. Remote access is exclusively via VPN with MFA required."	Audits external attack surface. Identifies and remediates exposed RDP before application. Documents remediation for evidence.
Do you have a vulnerability management program?	Do you patch known vulnerabilities before attackers exploit them?	"Yes — critical patches applied within 30 days. Monthly vulnerability scan conducted. End-of-life software inventory maintained. Last scan date: [DATE]."	Establishes patch management policy, scan cadence, and documents findings and remediation timelines.
Do you have a data inventory identifying what sensitive data you hold?	Do you know what you are insuring? (Carriers price risk based on data types.)	"Yes — annual data inventory completed. We hold: [PII types, PHI Y/N, financial account data Y/N]. Records stored in [systems]. Retention schedule documented."	Conducts data discovery and classification. Ensures inventory is current and application answers are accurate — protecting against post-incident misrepresentation claims.

PART 2: QUESTIONS THAT COMMONLY PRODUCE INACCURATE ANSWERS

The following questions are frequently answered inaccurately — sometimes due to misunderstanding, sometimes because the person completing the application does not know what is actually deployed. Each one has been cited in claim denial proceedings.

"Do you require MFA for all privileged/admin accounts?"

Why answers are often wrong: Many organizations enable MFA for regular accounts but overlook service accounts, shared admin accounts, and domain administrator accounts. These are the accounts attackers target first.

How a vCISO helps: A vCISO audits all accounts with elevated privileges, verifies MFA is enforced on each, and documents any exceptions with compensating controls.

"Do you have written security policies?"

Why answers are often wrong: Organizations often answer Yes because they have a vague IT policy from 2018. Carriers increasingly mean: current, signed-off, role-specific policies covering the domains the carrier is evaluating.

How a vCISO helps: A vCISO develops a current policy library — Information Security Policy, AI Acceptable Use, Incident Response, Acceptable Use, Data Classification — reviewed and signed within the past 12 months.

"Do you have a business continuity / disaster recovery plan?"

Why answers are often wrong: Having a backup is not the same as having a tested recovery plan. Carriers are asking whether you can restore operations, not whether data exists somewhere.

How a vCISO helps: A vCISO develops a BCP/DR plan, ensures recovery procedures are documented, and oversees annual testing with documented results.

"Are employees trained on recognizing phishing?"

Why answers are often wrong: "Yes, we send occasional emails" does not constitute a training program. Carriers expect annual documented training with phishing simulation data.

How a vCISO helps: A vCISO designs a formal training program with documented completion records and quarterly phishing simulation results — the evidence package carriers require.

PART 3: THE VCISO RENEWAL WORKFLOW

A vCISO engagement with Axiom Sovereign includes a structured annual renewal support process:

Step	Activity	Timing	Output
1	Pre-Renewal Controls Audit — verify every application question against actual deployed controls	90 days before renewal	Gap list with priority remediation items
2	Remediation Sprint — close identified gaps before application is submitted	60–30 days before renewal	Evidence package for each control
3	Application Review — review every question and answer for accuracy	30 days before renewal	Reviewed and signed application
4	Evidence Package — compile documentation for each control claimed on application	30 days before renewal	Binder of supporting evidence
5	Broker Briefing — prepare summary of security program improvements for broker	30 days before renewal	Program narrative for underwriter
6	Post-Renewal Gap Assessment — document remaining gaps for next-year planning	Within 30 days of renewal	Roadmap for following year

Ready to Get Started?

Schedule your complimentary 30-minute discovery call: calendly.com/cmissimore-62kc/30min
info@axiomsovereign.com · axiomsovereign.com