SECUREVERYONE · SECUREVERYONE.COM

Free Resource · Insurance & Financial Services Edition · 2026

# Vendor Security Response Library 2026

## Insurance & Financial Services Edition

CAIQ v4 · SIG Core · Audit Evidence Templates

| 28+ | 9 | 4 | <45 min |
|---|---|---|---|
| Pre-Written Responses | Sections Covered | Framework Crosswalks | Insurance Q Completion |

**What You Get:**

- Insurance-specific cyber questionnaire responses covering claims, regulatory, and coverage assessment
- Financial audit evidence templates for SOX, GLBA Safeguards, and FFIEC examination prep
- CAIQ v4 Governance and Compliance domain responses with board-level and CISO-level language
- SIG Core Sections A, B, and C: Information Security, Incident Management, Business Continuity
- Insurance Questionnaire Red-Flag Guide — 5 dangerous answers with defensible replacements

HOW TO USE THIS LIBRARY

# Getting the Most from Your Responses

1. Identify your questionnaire type: This library covers insurance underwriter assessments, financial audit evidence requirements, CAIQ v4 Governance and Compliance domains, and SIG Core Sections A, B, and C. Match the section to the questionnaire you are completing.
2. Replace all [BRACKET] placeholders before submitting: Every bracketed item is a customization point. Generic responses with unfilled brackets are worse than no response — they signal an unreviewed template. Treat brackets as a checklist.
3. Review the Insurance Red-Flag Guide (Section 9) before any insurance submission: Insurance underwriters see thousands of questionnaires. The five dangerous answers in Section 9 are the ones most likely to trigger a coverage denial or premium increase.
4. Cross-reference with your SOC 2 report: Most responses reference SOC 2 TSC controls. Before submitting, confirm the referenced controls appear in your most recent SOC 2 Type II report. If they do not, qualify your response appropriately.
5. Update after any incident, audit finding, or control change: These responses are a point-in-time snapshot. Material changes to your security program should be reflected in an updated questionnaire within 30 days of the change.

## Section Map

| Section | Title | Covers |
|---|---|---|
| **Section 1** | Insurance-Specific Questionnaire Responses | Cyber insurance assessment, regulatory, claims security |
| **Section 2** | Financial Audit Evidence Templates | SOX ITGC, GLBA Safeguards, FFIEC exam prep |
| **Section 3** | CAIQ v4 Governance Domain | Board oversight, CISO reporting, security budget |
| **Section 4** | CAIQ v4 Compliance & Audit | Audit rights, regulatory change, attestation SLAs |
| **Section 5** | SIG Core A — Information Security | ISMS scope, policy review, exception management |
| **Section 6** | SIG Core B — Incident Management | Escalation matrix, regulator notification, PIR |
| **Section 7** | SIG Core C — Business Continuity | Alternate site, supply chain, crisis communication |
| **Section 8** | Audit Scheduling & Evidence Delivery | Audit coordination, evidence packaging, SLAs |
| **Section 9** | Insurance Red-Flag Guide | 5 dangerous answers with better replacements |

SECTION 1

# Insurance-Specific Questionnaire Responses

### Q1: DOES YOUR ORGANIZATION CARRY CYBER LIABILITY INSURANCE, AND WHAT CONTROLS DOES YOUR INSURER REQUIRE?

[COMPANY NAME] maintains a cyber liability insurance policy with a limit of [AMOUNT] per occurrence, underwritten by [INSURER]. Our insurer requires the following controls as a condition of coverage: (1) Multi-factor authentication on all email and remote access systems enforced via [MFA SOLUTION]; (2) Endpoint detection and response (EDR) deployed on all endpoints with 24/7 monitoring via [EDR TOOL]; (3) Privileged access management (PAM) for all administrative accounts via [PAM TOOL] with just-in-time access provisioning; (4) Tested and verified offline backups with 3-2-1 backup methodology restored successfully in the last quarterly DR test on [DATE]; (5) Annual security awareness training with phishing simulation with completion rate [X]% as of [DATE]. Evidence of compliance with insurer requirements is available under NDA upon request.

### Q2: HOW DOES YOUR ORGANIZATION COMPLY WITH STATE INSURANCE REGULATORY CYBERSECURITY REQUIREMENTS (NAIC MDL-668 / NYDFS PART 500)?

[COMPANY NAME] maintains a documented information security program that satisfies the NAIC Insurance Data Security Model Law (MDL-668) and, where applicable, NYDFS Cybersecurity Regulation (23 NYCRR Part 500). Key program elements include: (1) Annual risk assessment by a qualified assessor covering identification of nonpublic information, threat assessment, vulnerability assessment, and control gap analysis - most recent assessment completed [DATE]; (2) Designated CISO or equivalent ([CONTACT NAME]) with board-reporting responsibility; (3) Comprehensive written cybersecurity policy approved by senior leadership, last reviewed [DATE]; (4) Incident response plan tested at least annually - most recent tabletop exercise [DATE]; (5) Third-party service provider oversight program with annual review of all providers with access to nonpublic information; (6) Annual penetration testing by an independent third party; (7) Employee cybersecurity awareness training. For NYDFS Part 500-covered entities, our program satisfies the enhanced requirements effective November 1, 2023, including the annual certification requirement. Regulatory certification documentation is available upon request.

### Q3: WHAT SECURITY CONTROLS GOVERN CLAIMS HANDLING DATA, INCLUDING CLAIMANT PII AND HEALTH INFORMATION?

[COMPANY NAME] classifies claims data, including claimant personally identifiable information (PII) and protected health information (PHI), as Restricted data under our data classification policy (DCP-001). Controls applied to Restricted data: (1) Access restricted to authorized personnel on a need-to-know basis, enforced via role-based access control (RBAC) reviewed quarterly; (2) Claims data encrypted at rest using AES-256 and in transit using TLS 1.2+; (3) Claims data never processed or stored in AI or LLM systems without explicit written consent; (4) Audit logging of all access to claims records retained for a minimum of 7 years; (5) Claimant data subject rights requests (deletion, correction, portability) fulfilled within 30 days; (6) Breach notification to affected claimants within timeframes required by applicable state law. For HIPAA-covered claims data, our HIPAA Security Rule program is documented in our HIPAA Compliance Manual (HCM-001), available under NDA.

SECTION 2

# Financial Audit Evidence Templates

**Q1: HOW DO YOU SUPPORT SOX IT GENERAL CONTROLS (ITGC) ATTESTATION REQUIREMENTS FOR FINANCIAL AUDIT PURPOSES?**

[COMPANY NAME] supports SOX IT General Controls attestation for the following ITGC domains: (1) Access to Programs and Data: Role-based access control with quarterly access reviews, privileged access managed via [PAM TOOL], segregation of duties enforced technically - evidence available as access review reports and SOC 2 CC6 narratives; (2) Computer Operations: Change management procedure (CMP-001) requires documented approval, testing, and rollback procedures for all production changes; (3) Program Development: SDLC policy (SSDLC-001) mandates code review, security testing, and UAT sign-off before promotion to production; (4) Program Change: Emergency change procedure (ECP-001) requires post-change documentation and management approval within 24 hours. We provide a SOX-ITGC evidence package to audit teams upon request, including relevant SOC 2 Type II report sections, system access reports, and change management logs. Contact [CONTACT] to coordinate on ITGC walkthroughs.

**Q2: HOW DOES YOUR ORGANIZATION COMPLY WITH THE GLBA SAFEGUARDS RULE (16 CFR PART 314) FOR FINANCIAL INSTITUTION CUSTOMERS?**

[COMPANY NAME] maintains a written information security program designed to protect the nonpublic personal information of financial institution customers as required by the Gramm-Leach-Bliley Act Safeguards Rule. Our program includes: (1) Designated Qualified Individual responsible for overseeing and implementing the information security program - [CONTACT NAME]; (2) Annual written risk assessment - most recent: [DATE]; (3) Access controls including multi-factor authentication for any individual accessing customer information systems; (4) Encryption of all customer information at rest (AES-256) and in transit (TLS 1.2+); (5) Secure disposal per NIST SP 800-88; (6) Change management procedures covering systems that process customer information; (7) Annual penetration testing and continuous vulnerability scanning; (8) Annual security awareness training and phishing simulation; (9) Service provider oversight with contractual flow-down of Safeguards Rule obligations; (10) Incident response plan with board notification within 30 days of discovery of a security event affecting 500 or more customers. Annual Safeguards Rule compliance attestation is available upon request.

**Q3: HOW DO YOU PREPARE EVIDENCE FOR FFIEC IT EXAMINATION PURPOSES, AND WHAT DOCUMENTATION CAN YOU PROVIDE TO EXAMINERS?**

[COMPANY NAME] supports financial institution clients in preparing for FFIEC IT Examination by providing the following documentation package upon execution of a mutual NDA and receipt of a formal examiner request: (1) Current SOC 2 Type II report covering the period [DATE] to [DATE]; (2) Penetration test summary from the most recent external assessment - [DATE]; (3) Vulnerability scanning summary showing open finding counts by severity; (4) Business Continuity Plan summary with RTO/RPO commitments and most recent DR test results; (5) Vendor and sub-processor list with security certification status; (6) Information Security Policy, Incident Response Plan, and Change Management Policy available under NDA; (7) Completed FFIEC IT Examination questionnaire available upon request. We have supported FFIEC examinations for [X] financial institution clients without material findings related to our services.

SECTION 3

# CAIQ v4 Governance Domain

**Q1: HOW IS CYBERSECURITY OVERSIGHT STRUCTURED AT THE BOARD AND EXECUTIVE LEVEL?**

[COMPANY NAME] maintains board-level cybersecurity oversight through the following governance structure: (1) The Board of Directors or Audit Committee receives a quarterly cybersecurity briefing from the CISO covering: threat landscape changes, security program KPIs, material security incidents, and budget vs. actual security spend; (2) The CISO ([NAME]) reports directly to the [CEO / CTO / General Counsel] and has authority to stop any project or deployment that represents an unacceptable security risk; (3) An executive Security Steering Committee meets monthly to review security program priorities, risk register updates, and compliance posture; (4) Annual board-level tabletop exercise simulating a material cybersecurity incident. Board meeting minutes reflecting cybersecurity agenda items are available under NDA. This governance structure satisfies CAIQ v4 GRC-01 through GRC-06 and SOC 2 CC1.1.

**Q2: WHAT IS THE REPORTING STRUCTURE AND AUTHORITY OF YOUR CHIEF INFORMATION SECURITY OFFICER (CISO)?**

[COMPANY NAME] CISO is [NAME], [CISO TITLE], who has held the role since [DATE] and maintains the following certifications: [CISSP/CISM/CISA]. The CISO reports directly to the [EXECUTIVE TITLE] and has: (1) Direct budget authority over the information security program; (2) Authority to approve or veto any system change, new vendor engagement, or product feature that processes customer data; (3) Direct access to the Board Audit Committee without requiring management approval; (4) Authority to engage external legal counsel and IR retainer firm without management approval in the event of a potential material security incident. The CISO participates in all major contract reviews involving data processing. CISO contact for security escalations: [SECURITY-EMAIL].

**Q3: HOW IS THE INFORMATION SECURITY BUDGET DETERMINED AND WHAT PERCENTAGE OF IT SPEND DOES IT REPRESENT?**

[COMPANY NAME] allocates the information security budget through an annual risk-based budgeting process in which the CISO presents the Board Audit Committee with: (1) Current risk register with financial exposure estimates per risk; (2) Gap analysis against target security posture; (3) Proposed investments ranked by risk reduction per dollar; (4) Prior year budget vs. actuals and program effectiveness metrics. The current information security budget represents [X]% of total IT budget - above the Gartner median of 10.9% for [INDUSTRY]. Budget covers: security tooling, third-party assessments, security awareness training, personnel, and IR retainer/insurance. Budget documentation is available under NDA.

SECTION 4

# CAIQ v4 Compliance & Audit

### Q1: WHAT THIRD-PARTY AUDIT RIGHTS DO CUSTOMERS HAVE, AND HOW ARE AUDITS COORDINATED?

[COMPANY NAME] grants customers the right to conduct, or commission a third party to conduct, a security audit of our services no more than once per calendar year, subject to: (1) Minimum 30 business days written notice; (2) Execution of a mutual NDA prior to audit scheduling; (3) Audit scope limited to controls relevant to the customer data processing; (4) No live penetration testing against production systems without separate written approval; (5) Audit costs borne by the requesting customer unless otherwise agreed. As an alternative, customers may elect to rely on our annual SOC 2 Type II report and ISO 27001:2022 certification, which are accepted by most enterprise security teams as satisfying audit rights. For customers requiring more frequent audit evidence, we provide quarterly security posture reports at no additional charge.

### Q2: HOW DO YOU TRACK AND RESPOND TO REGULATORY CHANGES THAT AFFECT YOUR SECURITY OBLIGATIONS?

[COMPANY NAME] maintains a Regulatory Intelligence Program (RIP-001) that tracks changes to applicable cybersecurity regulations through: (1) Subscriptions to regulatory agency publication feeds (CISA, FTC, OCR, NYDFS, NAIC) reviewed weekly by the Compliance team; (2) Membership in industry associations (ISACA, ISC2, FS-ISAC) with regulatory change alerts; (3) Quarterly review of pending regulatory changes by the Security Steering Committee; (4) External legal counsel retained for regulatory interpretation - [LAW FIRM NAME]. When a material regulatory change is identified, an impact assessment is completed within 30 days, a remediation plan is approved within 60 days, and customers with affected contracts are notified within 90 days of the effective date of the change.

### Q3: WHAT ARE YOUR SLAS FOR DELIVERING ATTESTATIONS, CERTIFICATIONS, AND AUDIT EVIDENCE?

[COMPANY NAME] commits to the following attestation and evidence delivery SLAs: (1) SOC 2 Type II report: available within 2 business days of executed NDA; (2) ISO 27001:2022 certificate: available within 1 business day of request; (3) Completed security questionnaire: turnaround within 5 business days for standard questionnaires; within 10 business days for questionnaires exceeding 100 questions; (4) Penetration test summary: available within 3 business days of executed NDA; (5) Sub-processor list: available within 1 business day; (6) Custom audit evidence requests: acknowledged within 1 business day; fulfillment timeline communicated within 3 business days. For time-sensitive requests, contact [CONTACT] with the required delivery date and we will prioritize accordingly.

SECTION 5

# SIG Core Section A — Information Security

### Q1: WHAT IS THE SCOPE OF YOUR INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS), AND WHAT IS EXCLUDED?

[COMPANY NAME] ISMS is documented in our Information Security Policy (ISP-001) and covers: (1) All production systems, infrastructure, and services used to deliver [SERVICE NAME] to customers; (2) All [COMPANY NAME] employees, contractors, and third parties with access to production systems or customer data; (3) All physical locations where production systems are operated or customer data is processed. Explicitly excluded from ISMS scope: corporate marketing systems that do not process customer data; legacy decommissioned systems isolated from production networks. No customer data processing systems are excluded from ISMS scope. The ISMS scope is reviewed annually; last reviewed and reapproved by the CISO on [DATE]. ISO 27001:2022 certification covers the full ISMS scope described above.

### Q2: HOW FREQUENTLY ARE INFORMATION SECURITY POLICIES REVIEWED, AND WHO APPROVES THEM?

[COMPANY NAME] reviews all information security policies on the following schedule: (1) Core policies (Information Security Policy, Acceptable Use Policy, Access Control Policy) reviewed annually by the CISO and approved by the [CEO/Board Audit Committee]; (2) Operational policies (Incident Response Plan, Vulnerability Management Policy, Change Management Policy) reviewed annually by the Security team and approved by the CISO; (3) Technical standards reviewed annually by Engineering Leads and approved by the CISO; (4) All policies reviewed within 30 days of any material security incident, regulatory change, or significant infrastructure change. Policy review history is maintained in our policy management system. Evidence of the most recent annual review cycle is available upon request.

### Q3: HOW DO YOU MANAGE EXCEPTIONS TO YOUR INFORMATION SECURITY POLICIES?

[COMPANY NAME] manages policy exceptions through a formal Exception Management Process (EMP-001): (1) Exception request submitted by the requestor manager with documented business justification, affected systems, risk impact assessment, and proposed compensating controls; (2) Risk assessment completed by the Security team within 5 business days; (3) CISO approval required for all exceptions; Board Audit Committee notification required for exceptions that materially affect customer data security; (4) Exceptions are time-limited - maximum 90 days for standard exceptions; maximum 180 days for exceptions with compensating controls in place; (5) Exception register maintained and reviewed monthly by the Security Steering Committee; (6) Exceptions not remediated within the approved period are escalated to executive leadership; (7) No exceptions are permitted for controls required by active customer contracts or regulatory obligations without the affected party written consent. No open exceptions affect controls that protect customer data.

SECTION 6

# SIG Core Section B — Security Incident Management

### Q1: WHAT IS YOUR INCIDENT ESCALATION MATRIX AND WHO HAS AUTHORITY TO DECLARE A CRITICAL INCIDENT?

[COMPANY NAME] uses a four-tier incident severity classification: P1 (Critical): confirmed breach of customer data, active ransomware, or service outage affecting more than 50% of customers - declared by CISO or on-call Security Lead; all executives notified within 30 minutes; customer notification within 4 hours. P2 (High): suspected breach, partial service outage, or active threat actor in network perimeter - declared by CISO or on-call Security Lead; security team and CTO notified within 1 hour. P3 (Medium): contained vulnerability with no active exploitation, service degradation - declared by on-call Security Analyst; Security team notified within 4 hours. P4 (Low): policy violation, phishing email reported, failed pen test finding - handled within normal business operations. All P1 and P2 incidents automatically activate the IR retainer with [IR FIRM NAME]. Escalation contacts are available 24/7/365 via [PAGERDUTY/EQUIVALENT] and the emergency security hotline: [PHONE].

### Q2: WHAT ARE YOUR REGULATORY NOTIFICATION PROCEDURES FOLLOWING A SECURITY INCIDENT?

[COMPANY NAME] maintains a Regulatory Notification Playbook (RNP-001) that maps incident type to applicable notification obligations: (1) HIPAA Breach Notification Rule: notification to HHS OCR within 60 days of discovery; individual notification without unreasonable delay; Business Associate breach notification to covered entity within 60 days; (2) GLBA Safeguards Rule: notification to FTC when a security event affects 500 or more customers within 30 days of discovery; (3) GDPR Article 33/34: supervisory authority notification within 72 hours of discovery; (4) NYDFS Part 500: notification to DFS within 72 hours of a Cybersecurity Event meeting the materiality threshold. Our Legal team is engaged for all P1 incidents; external counsel ([LAW FIRM]) is on retainer for regulatory notification decisions.

### Q3: WHAT IS YOUR POST-INCIDENT REVIEW (PIR) PROCESS AND HOW ARE FINDINGS TRACKED?

[COMPANY NAME] conducts a Post-Incident Review (PIR) for all P1 and P2 incidents within 10 business days of incident closure. The PIR process: (1) Timeline reconstruction from first indicator of compromise to full containment; (2) Root cause analysis using five-why method to identify systemic failures without individual blame; (3) Contributing factors analysis covering what controls failed and what detective controls were absent; (4) Action items that are specific, owner-assigned, deadline-bound remediation tasks entered into the security incident tracking system; (5) Lessons learned shared with the Security Steering Committee within 30 days; board notification for P1 incidents; (6) Customer communication: summary PIR shared with affected customers within 30 days of incident closure. PIR action items are tracked to completion; open items are reviewed monthly by the CISO. A summary of completed PIRs from the past 12 months is available under NDA.

SECTION 7

# SIG Core Section C — Business Continuity

### Q1: WHAT ARE YOUR ALTERNATE SITE AND FAILOVER CAPABILITIES IN THE EVENT OF A PRIMARY SITE FAILURE?

[COMPANY NAME] production infrastructure is deployed across a minimum of [NUMBER] geographically separated availability zones within [CLOUD PROVIDER] to ensure resilience against single-site failures. Our Business Continuity Plan (BCP-001) defines: (1) Primary production environment: [REGION/AZ] with automated load balancing and health monitoring; (2) Secondary failover environment: [REGION/AZ] warm standby with [X]-minute automated failover capability; (3) Cold disaster recovery environment: [REGION/AZ] with full environment rebuild within RTO of [X] hours. Database replication occurs in real-time between primary and secondary environments. Failover was last tested on [DATE] with the following results: failover achieved within RTO, data loss within RPO, all customer-facing services restored. Test documentation available upon request.

### Q2: HOW DOES YOUR BCP ADDRESS SUPPLY CHAIN DISRUPTIONS, INCLUDING THIRD-PARTY SERVICE PROVIDER OUTAGES?

[COMPANY NAME] maintains a Supply Chain Disruption Response Plan (SCDRP-001) as an annex to our Business Continuity Plan covering: (1) Critical third-party dependencies with documented SLAs and alternative provider options; (2) Single-point-of-failure elimination reviewed annually; (3) Contractual protections: all critical vendor contracts include uptime SLAs, breach notification obligations, and step-in rights in the event of vendor insolvency; (4) Alternate provider pre-qualification: for each critical dependency, at least one pre-qualified alternative provider has been identified with documented and tested migration runbooks; (5) In the event of a supply chain disruption affecting customer service levels, customers are notified within [X] hours via [STATUS PAGE / EMAIL] with estimated restoration timeline.

### Q3: WHAT IS YOUR CRISIS COMMUNICATION PLAN, AND HOW ARE CUSTOMERS NOTIFIED DURING A BUSINESS CONTINUITY EVENT?

[COMPANY NAME] maintains a Crisis Communication Plan (CCP-001) that defines communication protocols for business continuity events: (1) Status Page ([STATUS PAGE URL]): updated within 30 minutes of P1/P2 incident declaration; updated at minimum every 2 hours during active incidents; (2) Email notification sent to all affected customers within 1 hour of P1 incident declaration; (3) Each enterprise customer has a named relationship manager who receives direct phone notification for P1 incidents within 30 minutes; (4) For P1 incidents affecting enterprise customers critical operations, CISO-to-CISO direct contact is available; (5) Post-incident communication: written incident report issued within 5 business days of resolution, including root cause summary, remediation taken, and preventive measures implemented. A sample incident notification template is available upon request.

SECTION 8

# Audit Scheduling & Evidence Delivery

### Q1: HOW DO YOU COORDINATE AUDIT SCHEDULING, AND WHAT IS THE PROCESS FOR REQUESTING AN ON-SITE OR VIRTUAL AUDIT?

[COMPANY NAME] supports two types of customer-initiated security audits: (1) Virtual document review audit: customer or their designated third-party auditor reviews our evidence package via a secure document-sharing portal. Scheduling: contact [CONTACT] with a proposed date range and we will confirm availability within 3 business days. (2) On-site or virtual interview-based audit: our security team participates in a structured interview covering controls relevant to the customer data processing. Required notice: 30 business days. Scope agreement required prior to scheduling. Duration: typically 2 to 4 hours for a focused audit; 1 to 2 days for a comprehensive assessment. Costs are borne by the requesting party unless agreed otherwise. We conduct a maximum of [X] on-site or virtual audits per calendar year; scheduling is first-come, first-served.

### Q2: WHAT IS YOUR STANDARD EVIDENCE PACKAGE, AND HOW IS IT DELIVERED SECURELY?

[COMPANY NAME] maintains a Standard Evidence Package for vendor security assessments containing: (1) Current SOC 2 Type II report (full or bridge letter if within 3 months of prior report period end); (2) ISO 27001:2022 Certificate of Registration with scope statement; (3) Most recent external penetration test executive summary (redacted for operational security detail); (4) Current sub-processor list with security certification status; (5) Completed security questionnaire (SIG Lite, CAIQ v4, or custom questionnaire); (6) Business Continuity Plan summary (1-page); (7) Information Security Policy index (titles and effective dates only; full policies available separately under NDA). All evidence is delivered via [SECURE DOCUMENT PLATFORM]. Links are time-limited and restricted to the recipient email. Standard turnaround is 2 business days.

### Q3: WHAT SLA COMMITMENTS DO YOU MAKE FOR EVIDENCE DELIVERY, QUESTIONNAIRE RESPONSE, AND ONGOING SECURITY UPDATES?

[COMPANY NAME] commits to the following SLAs: Evidence Delivery - SOC 2 Type II report: 2 business days after NDA execution; ISO 27001 certificate: 1 business day; pen test summary: 3 business days after NDA execution; sub-processor list: 1 business day; custom evidence requests: acknowledged within 1 business day, fulfillment timeline provided within 3 business days. Questionnaire Response - Standard questionnaire (fewer than 50 questions): 5 business days; Extended questionnaire (50 to 100 questions): 7 business days; Comprehensive questionnaire (more than 100 questions): 10 business days; Re-submissions and clarifications: 3 business days. Ongoing Updates - Material security control changes: customer notification within 30 days; Sub-processor changes: 30-day advance notification; Annual questionnaire refresh: completed questionnaire reissued within 30 days of each SOC 2 Type II report renewal. SLA performance is tracked and reported monthly to the CISO.

SECTION 9

# Insurance Questionnaire Red-Flag Guide

**These answers trigger underwriter scrutiny, coverage restrictions, or premium increases.**

Review this guide before submitting any insurance underwriter questionnaire or financial audit security evidence package. Each dangerous answer below reflects real language seen in reviewed submissions. Replace with the specific, defensible language shown.

**DANGEROUS ANSWER**
"We follow industry best practices for cybersecurity."

**BETTER RESPONSE**
"We maintain SOC 2 Type II certification renewed annually (last assessment: [DATE], auditor: [FIRM]) and ISO 27001:2022 certification. Controls satisfy NAIC MDL-668 Section 4 requirements. Evidence available under NDA."

Why this triggers scrutiny: Insurance underwriters and financial auditors reject this immediately. "Best practices" is unspecific and signals no formal program. Every carrier security questionnaire asks which standard, which auditor, which date.

**DANGEROUS ANSWER**
"We have multi-factor authentication enabled."

**BETTER RESPONSE**
"FIDO2 hardware keys or WebAuthn passkeys are required for all privileged and remote access. TOTP (authenticator app) is the minimum for standard users. SMS OTP is disabled across all production systems. MFA cannot be bypassed — emergency break-glass accounts require dual approval and trigger real-time alerts."

Why this triggers scrutiny: After ransomware incidents at major insurers and 2024 NYDFS Part 500 enforcement actions, underwriters want specifics: what MFA type, on what systems, with what bypass controls. SMS OTP is no longer acceptable for privileged access.

**DANGEROUS ANSWER**
"We have cyber insurance coverage."

**BETTER RESPONSE**
"We carry [AMOUNT] cyber liability coverage with [INSURER]. Our insurer requires: MFA on email and remote access (verified quarterly), EDR on all endpoints ([TOOL]), tested offline backups (DR test: [DATE]), and annual security awareness training (completion: [X]%). Evidence of compliance available under NDA."

Why this triggers scrutiny: Underwriters already know you have coverage — they want to know what controls your insurer requires and whether you comply. Confirming coverage existence without confirming compliance signals a potential coverage gap.

**DANGEROUS ANSWER**
"Incidents are reported to customers as required by law."

**BETTER RESPONSE**
"Initial notification within 72 hours of confirmed P1 breach. NYDFS Part 500 supervisor notification within 72 hours. GLBA Safeguards FTC notification within 30 days if 500 or more customers affected. Preliminary written report within 7 business days. Full incident report within 30 days of closure. Timelines are documented in our Incident Response Plan, available under NDA."

Why this triggers scrutiny: "As required by law" varies by state, data type, and contractual obligation. Financial services regulators (NYDFS, FFIEC, FTC) have specific clocks. Auditors want to see your actual SLA, not a reference to applicable law.

**DANGEROUS ANSWER**

"Our vendors are contractually required to maintain security."

**BETTER RESPONSE**

"All vendors with access to customer data are assessed at onboarding against our Vendor Risk Policy (VRP-001) using a standardized questionnaire aligned to SIG Lite. Annual reassessment is required. Tier 1 vendors are required to provide SOC 2 Type II or equivalent annually. Sub-processor agreements include flow-down of NAIC MDL-668 and GLBA obligations, 30-day change notification, and right to audit. Vendor risk register reviewed monthly by the Security Steering Committee."

Why this triggers scrutiny: Post-MOVEit and post-Change Healthcare, "contractually required" is a starting point, not an answer. Auditors and underwriters want your vendor risk management process, how you verify compliance, how often, and what happens when a vendor fails.

# Your Questionnaire is Ready.

## Now Train Your Team to Defend What You Just Documented.

Pre-written responses close your questionnaire gap — but the real risk is the humans behind those controls. A single phishing email, vishing call, or wire-transfer BEC can invalidate every policy you just documented.

- **Executive Session — 90 —**
  CAIQ/SIG evidence walkthrough + team security briefing tailored to insurance and financial services
- **Business Program — Custom —**
  Annual security awareness training + tabletop exercises + quarterly posture reviews for your full team
- **Tabletop Exercise —**
  Live incident simulation: ransomware, BEC wire fraud, or NYDFS Part 500 breach scenario

### Book your Executive Session: book.secureveryone.com

Calendly: https://calendly.com/secureveryone/executive?utm_source=lead_magnet&utm_campaign=vendor_security_response