SECUREVERYONE · SECUREVERYONE.COM

Free Resource · 2026 Edition

Vendor Questionnaire Response Library

80+ Pre-Written Answers for SIG Lite · SIG Core · CAIQ v4

80+	12	3	<30 min
Pre-Written Responses	Security Domains	Framework Crosswalks	SIG Completion

What You Get:

- Pre-written, audit-ready responses with specific, defensible language
- SIG Lite / Core !’ CAIQ v4 crosswalk — use one response set across both frameworks
- SOC 2 TSC + ISO 27001 dual mapping — cut your audit prep time in half
- Red-Flag Guide — identify dangerous answers before your auditors do
- 12 security domains — from access controls to AI/LLM data handling

HOW TO USE THIS LIBRARY

Getting the Most from Your Library

1. Identify your questionnaire type: Use the SIG Lite/Core !' CAIQ v4 Crosswalk on Page 3. If you are completing a SIG Lite questionnaire, start with Sections 1–8. For SIG Core or CAIQ v4, use all 12 sections.
2. Find the response that matches your situation: Each response has [BRACKET] placeholders. Replace each bracket with your company specific detail. Do not remove the brackets — they signal customization is needed.
3. Review the Red-Flag Guide (last section) before submission: Even good responses can sound bad if they are generic. The Red-Flag Guide tells you what dangerous language looks like and what to say instead.
4. Use the SOC 2 TSC + ISO 27001 dual mapping: If you are under both frameworks, attach the dual mapping table from Section 14 to your submission. One response set, two frameworks, half the audit prep time.
5. Update annually or after any incident: Your responses are a snapshot. If you change your security program, update your responses. If you have a security incident, it affects several responses — update them all before your next questionnaire.

Framework Mapping

Domain	SIG	CAIQ v4	SOC 2 TSC	ISO 27001
Security Governance	SIG Section 1	CAIQ Domain 1	CC1, CC2	A.5, A.6
Access Controls	SIG Section 2	CAIQ Domain 2	CC6.1–CC6.8	A.8
Encryption	SIG Section 3	CAIQ Domain 3	CC6.7	A.8.5, A.8.8
Incident Response	SIG Section 4	CAIQ Domain 4	CC7.3, CC7.4	A.5.26
Sub-Processor Risk	SIG Section 5	CAIQ Domain 5	CC9.2	A.5.4
Business Continuity	SIG Section 6	CAIQ Domain 6	CC9.1	A.5.30
Vulnerability Management	SIG Section 7	CAIQ Domain 7	CC7.2	A.8.8
Secure SDLC	SIG Section 8	CAIQ Domain 8	CC8.1	A.8.19
Physical Security	SIG Section 9	CAIQ Domain 9	CC6.4	A.7
AI/LLM Data Handling	SIG Extended	CAIQ Domain 14	CC6.7, CC9.2	A.5.8
Regulatory Compliance	SIG Extended	CAIQ Context	CC1, CC7	
Evidence & Audit	SIG Section 13	CAIQ Overview	All TSC	All Annex A

SECTION 1

Security Governance & Certifications

Q1: WHAT SECURITY CERTIFICATIONS DOES YOUR ORGANIZATION MAINTAIN?

[COMPANY NAME] maintains SOC 2 Type II certification, renewed annually following a 6-month observation period. Our most recent assessment was completed [DATE] by [AUDITOR NAME]. The audit scope covers: CC1.1–CC1.5 (Control Environment), CC2.2–CC2.3 (Communication), CC3.1–CC3.3 (Risk Assessment), CC5.1–CC5.3 (Control Activities), CC6.1–CC6.8 (Logical and Physical Access Controls), CC7.1–CC7.5 (System Operations), CC8.1–CC8.2 (Change Management), and CC9.1–CC9.2 (Vendor Risk). We additionally maintain ISO 27001:2022 certification covering all 14 Annex A domains. Copies of executive summaries are available under NDA.

Q2: HOW FREQUENTLY DO YOU CONDUCT PENETRATION TESTING?

[COMPANY NAME] conducts external penetration testing at least annually by a qualified independent third party. Internal penetration testing is conducted quarterly. Critical and high-severity findings are remediated within 30 days; medium-severity findings within 90 days. A summary of the most recent external pen test is available to customers under NDA upon request. All pen tests are conducted in accordance with OWASP Testing Guide v4.2 and NIST SP 800-115.

Q3: WHAT SECURITY TRAINING DO YOUR EMPLOYEES RECEIVE AND HOW FREQUENTLY?

All [COMPANY NAME] employees receive role-appropriate security awareness training upon onboarding and annually thereafter. Engineering staff receive quarterly secure coding training. All staff complete annual phishing resistance testing with a minimum threshold of 85% identification rate; staff below threshold receive additional training and re-testing within 30 days. Training records are maintained and available upon request as evidence for SOC 2 CC7.3.

Q4: DOES YOUR ORGANIZATION HAVE A DOCUMENTED INFORMATION SECURITY POLICY?

[COMPANY NAME] maintains a comprehensive Information Security Management System (ISMS) documented in our Information Security Policy (ISP-001), last reviewed and approved by senior leadership on [DATE]. The ISMS is aligned to ISO 27001:2022 Annex A controls and covers all 14 domains. The policy is reviewed annually or following any material change to the security landscape. Employees acknowledge the policy upon onboarding and annually.

SECTION 2

Access Controls & Multi-Factor Authentication

Q1: HOW DO YOU ENFORCE ACCESS CONTROLS ACROSS YOUR SYSTEMS?

[COMPANY NAME] enforces role-based access control (RBAC) across all production systems. Access is provisioned on a least-privilege basis — employees receive the minimum access required to perform their job function. All production system access requires phishing-resistant MFA (WebAuthn/FIDO2 for privileged accounts; TOTP or hardware OTP for standard users). Access reviews are conducted quarterly for all production systems and monthly for privileged accounts. Terminated employee accounts are disabled within 4 hours of separation.

Q2: WHAT MFA REQUIREMENTS APPLY TO PRIVILEGED ACCOUNTS AND REMOTE ACCESS?

Privileged account access to [COMPANY NAME] production systems requires FIDO2 hardware security keys or WebAuthn-bound passkeys — Phishing-resistant MFA that is resistant to adversary-in-the-middle (AiTM) attacks. Remote VPN access requires both password + TOTP. Service accounts and non-human identities use short-lived certificates with 24-hour rotation. MFA bypass is technically prevented; emergency break-glass accounts require dual-approval and generate real-time alerts. Audit logs of all privileged access are maintained for a minimum of 12 months.

Q3: HOW DO YOU HANDLE ACCESS REVIEWS AND TERMINATION PROCEDURES?

[COMPANY NAME] conducts quarterly access reviews across all systems. Hiring managers confirm active employee access entitlements; HR provides immediate notification of termination. Terminated employees are system-disabled within 4 hours of separation for standard accounts, and within 1 hour for privileged accounts. All system access is audited monthly against current HR records. Reviews are documented and available as evidence for SOC 2 CC6.3.

SECTION 3

Encryption & Data Handling

Q1: HOW IS DATA ENCRYPTED IN TRANSIT AND AT REST?

[COMPANY NAME] encrypts all data at rest using AES-256 or equivalent. All data in transit is protected with TLS 1.2 or higher; TLS 1.0 and TLS 1.1 are disabled at the load balancer level. Certificate management is automated via [CERT-MGMT-TOOL]; certificates rotate automatically at 90-day intervals. Customer data at rest is encrypted under customer-specific encryption keys where applicable. Key management follows NIST SP 800-57 and key rotation occurs every 90 days for data-at-rest keys.

Q2: WHAT IS YOUR DATA RETENTION AND SECURE DESTRUCTION POLICY?

[COMPANY NAME] retains customer data for the duration of the service agreement plus [X] days for data portability requests, after which data is securely destroyed in accordance with NIST SP 800-88 Guidelines for Media Sanitization. Electronic data is cryptographically erased (cryptographic shredding with AES-256); physical media is shredded by a certified vendor. Data destruction is logged and the log is retained for 3 years. Upon contract termination, a data destruction certificate is issued within 30 days.

Q3: DO YOU SUPPORT DATA RESIDENCY REQUIREMENTS?

[COMPANY NAME] stores customer data in [REGION(S)] data centers. For EU personal data, all processing occurs within the European Economic Area. Sub-processor changes that would move data outside the configured region require 30-day advance notification and customer approval. For regulated industries, data residency documentation is available to support compliance assessments.

SECTION 4

Incident Response & Breach Notification

Q1: WHAT IS YOUR DOCUMENTED INCIDENT RESPONSE PROCESS?

[COMPANY NAME] maintains an Incident Response Plan (IRP-001) aligned to NIST SP 800-61 Rev. 2. The IRP defines: detection and identification procedures, severity classification (P1–P4), containment steps, evidence preservation, internal escalation thresholds, regulatory notification procedures, and post-incident review. The IRP is tested via tabletop exercise at least annually. Incident response personnel are on-call 24/7/365. The most recent tabletop exercise was conducted on [DATE] with participation from engineering, legal, and executive leadership.

Q2: WHAT BREACH NOTIFICATION TIMELINE DO YOU COMMIT TO?

[COMPANY NAME] commits to the following breach notification timelines: initial acknowledgment within 24 hours of confirmed incident; preliminary assessment within 72 hours; and written notification to affected customers within 5 business days of confirmed breach. For GDPR-covered incidents, notification to supervisory authorities occurs within 72 hours per Article 33. Notification includes: nature of the breach, categories and approximate number of data subjects, likely consequences, and measures taken/proposed. Notification is provided in English; translated versions are provided upon request.

Q3: HAVE YOU EXPERIENCED ANY SECURITY INCIDENTS IN THE PAST 3 YEARS?

[IF NO: Insert] [COMPANY NAME] has not experienced any confirmed security incidents resulting in unauthorized access to, or disclosure of, customer data in the past three years. We maintain a mature security posture through annual pen testing, quarterly vulnerability scanning, and continuous SIEM monitoring. [IF YES: Insert] [COMPANY NAME] experienced [X] security incidents in the past three years. [Brief description, date, data affected, remediation taken, regulatory notification if applicable]. All incidents were contained, remediated within SLA, and reported to affected customers per our notification commitments.

SECTION 5

Sub-Processor Management & Third-Party Risk

Q1: WHO ARE YOUR SUB-PROCESSORS AND HOW DO YOU MANAGE THEM?

[COMPANY NAME] maintains a current sub-processor list available at [URL] or provided upon request. All sub-processors are assessed for security and data handling practices at onboarding and reviewed annually. Sub-processor agreements include: flow-down of GDPR Article 28 obligations, breach notification within 24 hours, audit rights, and prohibition on sub-delegation without written consent. Major sub-processors include: [LIST PRIMARY SUB-PROCESSORS, e.g., AWS for cloud infrastructure, Twilio for communications]. Customers are notified 30 days in advance of changes to sub-processor arrangements.

Q2: DO YOUR AGREEMENTS WITH SUB-PROCESSORS INCLUDE AUDIT RIGHTS?

Yes. All [COMPANY NAME] sub-processor agreements include the right to audit or receive third-party audit reports (SOC 2 Type II or equivalent) on request. For Infrastructure-as-a-Service sub-processors (e.g., AWS, Azure), audit rights are satisfied through SOC 2 Type II and ISO 27001 certifications published on the provider trust portal. For sub-processors handling customer personal data, audit rights include the right to conduct an on-site audit upon 30 days written notice. Alternative audit evidence (pentest reports, ISO certifications) may be accepted in lieu of a dedicated audit.

SECTION 6

Business Continuity & Disaster Recovery

Q1: WHAT ARE YOUR DOCUMENTED RTO AND RPO COMMITMENTS?

[COMPANY NAME] maintains the following availability commitments: Recovery Time Objective (RTO) of [X] hours for critical systems; Recovery Point Objective (RPO) of [Y] hours for customer data. These commitments are documented in the Business Continuity Plan (BCP-001). Availability statistics for the past 12 months are published at [URL]. BCP is reviewed and updated annually and following any major incident or infrastructure change.

Q2: HOW FREQUENTLY DO YOU TEST YOUR DISASTER RECOVERY CAPABILITIES?

[COMPANY NAME] conducts DR testing at least annually. The most recent DR test was conducted on [DATE] and validated: full system failover within RTO, data restoration within RPO, and communication procedures for incident notification. DR test results are documented and available upon request. Infrastructure is deployed across [NUMBER] availability zones; automated failover is tested monthly via chaos engineering.

SECTION 7

Vulnerability Management & Patch Management

Q1: WHAT IS YOUR VULNERABILITY SCANNING AND PATCH MANAGEMENT CADENCE?

[COMPANY NAME] conducts automated vulnerability scanning of all production infrastructure at least weekly. Critical and high-severity vulnerabilities are patched within 72 hours of detection; medium-severity vulnerabilities are patched within 14 days; low-severity vulnerabilities are patched within 90 days. Patches are tested in a staging environment for a minimum of 48 hours before production deployment. Emergency patches for critical vulnerabilities can be deployed within 4 hours with executive authorization. Vulnerability scan results and patch status are reviewed in monthly security operations meetings.

Q2: DO YOU CONDUCT COORDINATED VULNERABILITY DISCLOSURE?

[COMPANY NAME] maintains a Responsible Disclosure Policy available at [URL]. Security researchers may report vulnerabilities to [SECURITY-EMAIL]. We acknowledge reports within 48 hours and commit to: initial assessment within 7 days, remediation timeline communicated within 30 days, public acknowledgment (with researcher permission) following resolution. In the past 24 months, [X] vulnerability reports were received; [Y] were validated and remediated; [Z] were determined out of scope. No critical or high-severity reports remain open.

SECTION 8

Secure Software Development Life Cycle (SSDLC)

Q1: HOW DO YOU INTEGRATE SECURITY INTO YOUR SOFTWARE DEVELOPMENT PROCESS?

[COMPANY NAME] follows a Secure Software Development Life Cycle (SSDLC) that integrates security at every phase: requirements (threat modeling), design (security architecture review), development (SAST via [TOOL], peer code review with security checklist), testing (DAST, SCA for open-source dependencies, penetration testing), and deployment (security acceptance testing, immutable infrastructure). All engineers complete secure coding training annually. Code is forbidden to reach production without: passing SAST scan, passing peer security review, and security team approval for changes to authentication, authorization, or data handling modules.

Q2: HOW DO YOU MANAGE OPEN-SOURCE DEPENDENCIES AND KNOWN VULNERABILITIES?

[COMPANY NAME] uses [SCA-TOOL, e.g., Snyk, GitHub Dependabot] for continuous Software Composition Analysis (SCA). All open-source components are scanned at every pull request; new vulnerabilities trigger a build failure. Known vulnerabilities in production dependencies are tracked in our vulnerability management system and remediated within the SLAs defined in our vulnerability management policy (VMP-001). License compliance is tracked and reviewed quarterly. Bill of materials (SBOM) in CycloneDX format is available upon request.

SECTION 9

Physical & Environmental Security

Q1: WHERE ARE YOUR DATA CENTERS LOCATED AND WHAT PHYSICAL CONTROLS ARE IN PLACE?

[COMPANY NAME] production infrastructure is hosted in [AWS/US-East/EU-West, or equivalent]. All data centers are SOC 2 Type II certified and maintain: 24/7 physical security with badge access and biometric authentication, CCTV monitoring, mantrap entry systems, and environmental controls (fire suppression, climate control, redundant power). Access to the data center floor requires dual-authentication and is restricted to authorized operations personnel. Physical access logs are retained for 12 months and reviewed monthly.

SECTION 10

AI & LLM Data Handling (2026 Addition)

Q1: DOES YOUR ORGANIZATION USE AI OR LLM SERVICES IN THE DELIVERY OF YOUR PRODUCT?

[COMPANY NAME] uses AI/ML components in our product as follows: [DESCRIBE AI USE CASE, e.g., "Product analytics — aggregated, anonymized event data is processed by a hosted LLM to generate usage insights. Customer PII is never processed by the LLM." OR "AI is not used in the delivery of core services."]. Where AI services are used, they are hosted by [PROVIDER] under a Data Processing Agreement that restricts the provider from using customer data for model training. Customer opt-out of AI data processing is available; contact [CONTACT] to request opt-out.

Q2: DO YOU ALLOW AI SERVICES TO TRAIN ON CUSTOMER DATA?

[COMPANY NAME] does not use customer data — including personal data, confidential business data, or any data processed through our services — for training or fine-tuning AI or machine learning models. This restriction is contractual and technically enforced: AI/ML services in our stack are configured with training-data exclusion flags (e.g., GCP Vertex AI data labeling, OpenAI API no-train flag). Evidence of this configuration is available upon request. Sub-processors are similarly restricted in their data processing agreements.

Q3: WHAT GOVERNANCE POLICIES COVER YOUR AI SYSTEM USE?

[COMPANY NAME] maintains an AI Governance Policy (AIGP-001) that governs: approved AI use cases and review process, data classification requirements for AI processing, human oversight requirements for AI-assisted decisions, bias and fairness testing for AI outputs affecting customers, and incident response for AI-related failures. The AIGP is reviewed annually. All AI systems in scope for customer data processing are documented in the AI System Registry, available upon request.

SECTION 11

Regulatory Compliance Mapping

Q1: HOW DO YOU SUPPORT HIPAA BUSINESS ASSOCIATE AGREEMENT REQUIREMENTS?

[COMPANY NAME] executes HIPAA Business Associate Agreements (BAAs) with covered entities and business associates that engage our services and have access to Protected Health Information (PHI). Our security controls are designed to meet the HIPAA Security Rule Safeguards: Administrative Safeguards (risk analysis, workforce training, incident response), Physical Safeguards (facility access controls, workstation security), and Technical Safeguards (access controls, audit logging, transmission security). A BAA is available upon execution of a mutual NDA. Our current BAA template is available upon request.

Q2: HOW DO YOU SUPPORT GLBA SAFEGUARDS RULE REQUIREMENTS?

[COMPANY NAME] supports financial institution clients under the GLBA Safeguards Rule (16 CFR Part 314) with: documented security policies and risk assessments reviewed annually, personnel training on safeguarding customer financial information, secure development and storage of financial data, incident response procedures aligned to FTC requirements, and vendor oversight including flow-down of Safeguards Rule obligations to sub-processors. Our security program is designed to satisfy the Safeguards Rule requirements applicable to our role as a service provider.

Q3: HOW DO YOU SUPPORT CMMC 2.0 LEVEL 2 REQUIREMENTS FOR DEFENSE CONTRACTORS?

[COMPANY NAME] supports defense contractors requiring CMMC 2.0 Level 2 compliance with: documentation of all 14 CMMC practice domains in our System Security Plan (SSP), evidence of implementation for all Level 2 practices, annual internal assessments against CMMC criteria, and flow-down of Controlled Unclassified Information (CUI) protection requirements to sub-processors. Our CMMC documentation package (SSP + Plan of Action & Milestones) is available to customers requiring CUI handling evidence. Note: [COMPANY NAME] is not a certified C3PAO; we can provide documentation supporting your self-assessment or third-party assessment.

SECTION 12

Security Assessment Evidence & Audit Support

Q1: WHAT EVIDENCE CAN YOU PROVIDE TO SUPPORT OUR SECURITY ASSESSMENT?

[COMPANY NAME] provides the following evidence to support customer security assessments: (1) Current SOC 2 Type II report — available under NDA from [CONTACT]; (2) ISO 27001:2022 certificate — available upon request; (3) Penetration test summary — available under NDA; (4) Sub-processor list — available at [URL]; (5) Completed questionnaire (this document) — countersigned and stamped. Additional evidence requests can be accommodated within [X] business days. Our security team is available for direct calls to discuss questionnaire responses.

Q2: DO YOU SUPPORT MUTUAL NDA BEFORE SHARING DETAILED SECURITY EVIDENCE?

Yes. [COMPANY NAME] executes mutual non-disclosure agreements prior to sharing detailed security evidence, including: full SOC 2 Type II reports, penetration test reports, network architecture diagrams, incident response runbooks, and system security plans. Our standard NDA is available at [URL] or contact [CONTACT] to request execution. Turnaround for NDA execution is typically 1–2 business days.

Q3: HOW DO YOU HANDLE QUESTIONNAIRE UPDATES AND ANNUAL REASSESSMENT?

[COMPANY NAME] treats vendor questionnaires as living documents. We commit to: notifying customers within 30 days of material changes to security controls, providing updated questionnaire responses upon request at no charge, participating in annual reassessment calls, and promptly notifying customers of any security incidents that may affect their data. For annual SOC 2 Type II customers, we provide updated questionnaire responses at the start of each audit cycle. Customers may request a live review call to discuss responses; we respond to scheduling requests within 5 business days.

Red-Flag Guide

& These answers trigger auditor follow-up or prospect security team scrutiny.

Review this guide before submitting any vendor security questionnaire. Each dangerous answer below is a real example from reviewed questionnaires. Replace with the specific, defensible language shown.

DANGEROUS ANSWER	BETTER RESPONSE
"We follow industry-standard security practices."	"We maintain SOC 2 Type II certification, renewed annually. Audit scope includes CC1–CC9. Our most recent assessment was [DATE] by [AUDITOR]."

Why this triggers scrutiny: Unspecific. Auditors and prospect security teams ask "which standard?" and if you can only say "best practices," it signals a checkbox mentality, not a mature program.

DANGEROUS ANSWER	BETTER RESPONSE
"We have appropriate access controls."	"All production systems require FIDO2 hardware MFA for privileged access; standard users require TOTP. Access reviews are conducted quarterly. Terminated accounts are disabled within 4 hours."

Why this triggers scrutiny: "Appropriate" is subjective and unauditable. Auditors want specificity: what type of MFA, how often access is reviewed, what the termination SLA is.

DANGEROUS ANSWER	BETTER RESPONSE
"Encryption is used where appropriate."	"AES-256 at rest on all storage; TLS 1.2+ enforced in transit. Certificate management is automated; keys rotate every 90 days per NIST SP 800-57."

Why this triggers scrutiny: "Where appropriate" is the tell — it means you have not defined the policy. GDPR and SOC 2 require you to specify the encryption standard, not just say it exists.

DANGEROUS ANSWER	BETTER RESPONSE
"We notify clients of breaches within a reasonable timeframe."	"We commit to initial notification within 72 hours of confirmed breach, preliminary assessment within 7 days, and written notification within 5 business days. For GDPR-covered data, supervisory authority notification occurs within 72 hours per Article 33."

Why this triggers scrutiny: "Reasonable" is undefined and unenforceable. Regulators and auditors expect specific commitments. GDPR requires 72-hour notification. Your answer should reflect your actual SLA.

DANGEROUS ANSWER
"All employees receive security training."

BETTER RESPONSE
"All employees complete security awareness training at onboarding and annually. Phishing simulation testing is conducted monthly; staff below 85% pass rate receive additional training and retesting within 30 days. Training and testing records are maintained."

Why this triggers scrutiny: Does not address frequency, content, or effectiveness measurement. SOC 2 CC7.3 requires awareness training AND evidence that it works — typically phishing simulation results.

DANGEROUS ANSWER
"Our sub-processors are all vetted."

BETTER RESPONSE
"All sub-processors are assessed at onboarding against our Vendor Risk Policy (VRP-001) using a standardized questionnaire. Annual reassessment is required for all sub-processors with access to customer data. Sub-processor agreements include flow-down of GDPR Art. 28 obligations and 30-day change notification."

Why this triggers scrutiny: "Vetted" is meaningless without specifics: what standard, how often, what happens when a sub-processor fails the assessment? Sub-processor risk is now a primary audit focus after MOVEit.

DANGEROUS ANSWER
"We are compliant with [Framework]."

BETTER RESPONSE
"We maintain [Framework] certification. Our last [Framework] assessment was conducted [DATE] by [BODY/auditor]. The following evidence demonstrates our current state: [list 3-4 specific control evidences]."

Why this triggers scrutiny: "Compliant with" is a binary claim that auditors immediately challenge. Compliance is a continuous state, not a one-time achievement. Better to describe the evidence.

DANGEROUS ANSWER
"Data is stored securely."

BETTER RESPONSE
"Customer data is stored in [REGION] in AES-256-encrypted volumes. Access is restricted to authorized engineering personnel via role-based access control with MFA. Data is retained per the data retention schedule ([X] years) and securely destroyed per NIST SP 800-88 at end of retention period."

Why this triggers scrutiny: Same problem as encryption — "securely" is vague. SOC 2 auditors look for: where, in what form, with what controls, for how long, and who can access it.