SALES · TEMPLATE

Reading an Enterprise Security Questionnaire

KAANSYSTEMS.COM/LIBRARY/READING-SECURITY-QUESTIONNAIRE · MAY 30, 2026

ABOUT THIS TEMPLATE

Enterprise prospects send 200-question security questionnaires. Most teams answer them painfully. How to read what they're actually asking, and answer in days, not weeks.

THE TEMPLATE

Below is the response template for thirty of the most common questionnaire questions, with answer patterns. Adapt the specifics; use the structure.

#	QUESTION	ANSWER PATTERN
1	Do you have a written information security policy?	Yes. Reviewed annually. Last review: [date].
2	Do you have a designated CISO or security lead?	[Yes — name + title] OR [Compensating: head of platform engineering, security responsibilities documented in role description]
3	Describe your background check process for employees.	[Yes — vendor + scope] OR [Compensating: smaller team, manager-led reference checks, documented]
4	Do you provide security awareness training?	Yes. Annual training via [vendor], plus quarterly phishing simulations.
5	Do you encrypt data in transit?	Yes. TLS 1.2 minimum on all external endpoints; TLS 1.3 preferred. Internal traffic via [mesh / VPC isolation].
6	Do you encrypt data at rest?	Yes. AES-256 via [KMS provider]. Customer-managed keys available on request.
7	Do you maintain an asset inventory?	Yes. [Tool] reconciled [frequency].

#	QUESTION	ANSWER PATTERN
8	Do you have a vulnerability management program?	Yes. [Scanner] running [frequency]; SLO of [X days] for critical, [Y] for high.
9	Do you perform penetration testing?	Yes. Annual third-party pen test via [vendor]. Last test: [date]. Findings remediated.
10	Do you have a SOC2 / ISO 27001 / HITRUST attestation?	[Yes — current state] OR [In progress — target date] OR [Not currently certified — compensating: SOC 2 readiness assessment, evidence available on request]
11	How do you manage privileged access?	SSO-integrated, MFA-required, [JIT / standing], audit-logged. Privileged access reviewed quarterly.
12	Do you have logging and monitoring?	Yes. [Stack]. [Retention period]. Alerts route to 24/7 on-call.
13	Describe your incident response process.	Documented IR playbook. Severity 1 = page within 5 min, comms within 30 min. Last tabletop: [date].
14	Do you maintain backups?	Yes. [Frequency, retention, cross-region status]. Restore drill annual; last: [date].
15	Describe your DR posture.	RTO: [X hours]. RPO: [Y minutes]. Tested [frequency].
16	Do you have a BCP?	Yes. Reviewed [frequency].
17	How do you handle subcontractors/sub-processors?	Maintained list. Annual security review. DPAs in place.
18	Do you support SSO via SAML/OIDC?	Yes. SAML 2.0 + OIDC. SCIM provisioning available on [tier].
19	Do you support customer-managed encryption keys?	[Yes — how] OR [Compensating: AWS KMS-managed with customer-specific key per tenant]
20	What's your data residency?	[Region(s)]. Data does not leave [region] without [process].
21	How do you handle data deletion / right-to-be-forgotten?	Documented process; X-day SLO. Soft-delete + hard-delete distinction.
22	Are you HIPAA-compliant?	[BAA available; HIPAA-aware architecture; supporting controls documented]
23	Are you GDPR-compliant?	[DPA available; sub-processor list maintained; DPO designated]

#	QUESTION	ANSWER PATTERN
24	Are you PCI compliant?	[Yes — level] OR [Not applicable — we don't process card data, payments go via [provider]]
25	How long is your data retention?	[Policy + tier-specific retention]
26	Do you maintain change management?	Yes. Every production change tied to a PR; security-relevant changes require additional review. Audit log retained [period].
27	Do you have an exception process?	Yes. Documented. Approvals tracked. Reviewed quarterly.
28	How do you handle EOL/EOS dependencies?	Automated CVE scanning. SLO of [X] for critical CVEs. Quarterly stack review.
29	Do you have a security champions program?	[Yes — structure] OR [Compensating: security review on every PR; designated security reviewer in engineering]
30	Where can I find your trust portal / security page?	Link your security page (ours lives at /security).

The thirty questions above cover ~70% of any typical questionnaire. The other 30% are environment-specific (your specific tech stack, your specific data flows). With the thirty in place as a baseline, the environment-specific questions become the focused work.

HOW TO USE IT

Treat the questionnaire as a strategic asset, not a tactical inconvenience. The answers tell prospects what you stand for operationally. Brief, honest, specific answers signal that you take security seriously. Hedge-filled, marketing-flavored answers signal that you don't.

For the first three or four questionnaires your team handles, the founder or CTO should be in the response loop. After that, the response repository is mature enough that a security or platform engineer can run the process end-to-end with senior review only on the trickier questions.

The first questionnaire takes a week. The fifth takes a day. The fiftieth is a copy-paste plus a delta review.