Completed Security Questionnaire — Sample Excerpt

Prepared by Compriska for Acme Corp vendor review · 8 of 300 questions shown

> **What this is:** a real excerpt of the deliverable format from our 48-hour questionnaire completion service. Company details are fictionalized; the format, sourcing discipline, and gap handling are exactly what you receive. Every answer cites the customer document it came from — and questions the documentation cannot support are flagged honestly instead of papered over.

Q14. Is customer data encrypted at rest?

Yes. All customer data is encrypted at rest using AES-256. Encryption keys are managed through a dedicated key management service with automatic annual rotation and strict role-based access to key operations.

⚑ Source: Information Security Policy v4, §4.2 — Data Encryption

Q15. Is data encrypted in transit?

Yes. All data in transit is encrypted using TLS 1.2 or higher (TLS 1.3 preferred). Plain-text protocols are disabled at the load balancer, and certificate lifecycles are automated.

⚑ Source: Information Security Policy v4, §4.3 — Transport Security

Q22. Describe your user access review process.

We perform quarterly access reviews across all production systems. System owners certify each user's continued need for access; exceptions are ticketed and remediated within 15 days. Review results and remediation records are retained as evidence.

⚑ Source: Access Control Standard, §2.1 — Periodic Review

Q23. How is access revoked upon termination?

Termination triggers an offboarding workflow in our HR system that notifies IT the same business day. All account access is revoked within 24 hours of termination, with revocation verified and logged as part of the offboarding checklist.

⚑ Source: Access Control Standard, §3.4; HR Offboarding Procedure

Q41. Do you have a documented incident response plan? How often is it tested?

Yes. Our incident response plan defines severity levels, escalation paths, roles, and communication procedures, including a 72-hour customer notification commitment for incidents affecting customer data. The plan is exercised annually via tabletop, and findings feed corrective actions.

⚑ Source: Incident Response Plan v3, §§1–5

Q58. Do you conduct penetration testing?

Yes. An independent third party performs an annual penetration test of our production environment. Findings are risk-rated and remediated per defined SLAs; a summary letter is available to customers under NDA.

⚑ Source: 2026 Penetration Test Summary Letter

Q73. Do you hold FedRAMP authorization? GAP FLAGGED

Not answered — no supporting evidence. Your documentation does not reference FedRAMP authorization or an active pursuit of it. We recommend answering: "No. Our roadmap is driven by customer demand; we currently maintain [SOC 2 Type II / ISO 27001] as our primary attestations." See gap memo below.

Q91. Is production data used in development or test environments? GAP FLAGGED

Not answered — documentation silent. No policy statement covers test-data handling. This is a common auditor follow-up; we recommend documenting a data-sanitization rule before responding.

Gap Memo (excerpt)

#	Question	Why it's a gap	Recommended next step
Q73	FedRAMP authorization	No mention in any provided document	Answer "No" with your actual attestations; add FedRAMP to roadmap only if federal pipeline justifies it
Q91	Production data in test	No test-data policy exists	Add a one-paragraph data-sanitization rule to the InfoSec policy; then answer confidently

The full deliverable includes: every question answered in your voice · source citation on each answer · complete gap memo with recommendations · returned in your original spreadsheet format · within 48 hours. **compriska.com/services**