Security Questionnaire Response Cheat Sheet

The 15 questions every enterprise customer asks — and the documentation you need to answer them.

Why This Matters

67% of B2B deals now require security documentation before contracts close. The average delay when documentation is not ready is 3–4 weeks — enough time for a competitor to win the deal.

This cheat sheet maps the 15 most common security questionnaire questions to the specific documents you need. If you have these documents ready, you can respond to most questionnaires within 48 hours instead of scrambling for weeks.

Section 1: Governance & Policy Questions

These appear on virtually every questionnaire. They establish whether you have a formal security programme.

#	Common Question	What They Want to See	Document You Need	Response Time
1	**Do you have a formal information security policy?**	A board-approved policy with scope, objectives, roles, review dates. Not a one-pager.	**Information Security Policy (POL-001)**	5 min with doc ready
2	**What security framework do you follow?**	Explicit mapping to a recognised framework: NIST CSF, ISO 27001, CIS Controls, or SOC 2.	**Control Framework Mapping + Policy with framework references**	5 min with mapping
3	**How do you manage security risk?**	A risk register with identified risks, likelihood, impact scores, treatment plans, and owners.	**Risk Register + Risk Assessment Process**	10 min with register
4	**Do you have an acceptable use policy?**	Policy covering employee responsibilities for IT resources, internet, email, and device use.	**Acceptable Use Policy (POL-002)**	5 min with doc ready
5	**Who is responsible for security in your organisation?**	Named roles: CISO or equivalent, IT Director, department owners. Not 'IT handles it'.	**Roles & Responsibilities (in ISP) + Org chart reference**	5 min

Pro tip: If your policies reference NIST CSF 2.0 subcategories and ISO 27001 Annex A controls, the customer immediately sees maturity. Generic policies without framework mapping look amateur.

Section 2: Technical Control Questions

These test whether you have specific, measurable controls — not just intentions.

#	Common Question	What They Want to See	Document You Need	Response Time
1	**What are your password and authentication requirements?**	Specific parameters: minimum length, complexity, MFA enforcement, rotation policy.	**Password & Authentication Standard (STD-001)**	5 min with standard
2	**How do you classify and protect data?**	Classification scheme (Public/Internal/Confidential/Restricted) with handling rules for each level.	**Data Classification Policy + Standard (POL-004, STD-002)**	10 min
3	**How do you manage access control?**	Principle of least privilege, access review frequency, joiner/mover/leaver process, admin account controls.	**Access Control Policy + User Access Mgmt Process**	10 min
4	**Do you encrypt data at rest and in transit?**	Specific algorithms (AES-256, TLS 1.2+), key management, scope of encryption coverage.	**Encryption Standard (STD-003)**	5 min with standard
5	**How do you manage vulnerabilities and patching?**	Scanning frequency, patch timelines by severity (critical: 72hrs, high: 7 days), exceptions process.	**Vulnerability Mgmt Policy + Procedure**	10 min

Pro tip: Vague answers like "we follow best practices" or "we use strong encryption" are red flags to procurement teams. Specific parameters (12-character minimum, AES-256, 90-day access reviews) signal maturity.

Section 3: Incident Response & Business Continuity

These questions test whether you can handle things going wrong. Increasingly important for cyber insurance too.

#	Common Question	What They Want to See	Document You Need	Response Time
1	**Do you have an incident response plan?**	Documented plan with roles, escalation paths, communication templates, severity classification.	**Incident Response Plan + Contact list**	5 min with plan
2	**What is your data breach notification process?**	Timelines for internal escalation and external notification (72hrs GDPR, varies by jurisdiction).	**Incident Response Policy (POL-005) + Comms templates**	10 min
3	**Do you have a business continuity / disaster recovery plan?**	RTO/RPO targets, backup procedures, recovery testing frequency, alternative processing arrangements.	**BCP/DR Policy (POL-006) + Recovery procedures**	10 min
4	**Do you assess third-party vendor risk?**	Vendor assessment questionnaire, risk tiering, ongoing monitoring, contract security requirements.	**Vendor Risk Policy + Third-Party Assessment form**	10 min

#	Common Question	What They Want to See	Document You Need	Response Time
5	**How do you handle security awareness training?**	Training programme: frequency, topics covered, phishing simulation results, completion tracking.	**Security Awareness Policy + Training records**	5 min

Pro tip: When a questionnaire asks "when did you last test your IR plan?" or "what was your last phishing simulation click rate?", they want evidence of a living programme — not a document that was written and shelved.

The 48-Hour Response Workflow

How to respond to a security questionnaire in two days, not two weeks.

Step	Action	Time
1	**Triage**: Read the entire questionnaire. Categorise questions into: have documentation / need to create / not applicable. Count the gaps.	**2 hours**
2	**Map**: Match each question to your existing documentation. Pull files. Note page/section references so you can cite specifically.	**2 hours**
3	**Fill gaps**: For questions where you have practices but no documentation, draft the minimum viable document (policy or standard).	**4–8 hours**
4	**Answer**: Write responses referencing specific documents by name, ID, and section. Attach key documents as evidence.	**4 hours**
5	**Review**: Have someone else (CISO, IT Director, or legal) review responses before submission. Check for consistency.	**2 hours**

Response Quality Checklist

■ Every answer references a specific document by name and ID (not "yes, we have that")

■ Technical parameters are specific: "12-character minimum" not "strong passwords"

■ Framework mappings are cited: "per NIST CSF PR.AC-01" not "we follow frameworks"

■ Dates are included: policy approval dates, last review dates, last test dates

■ Gaps are acknowledged honestly with remediation timelines (better than vague claims)

■ Key documents are attached as evidence (policy PDFs, not just references)

■ Answers are consistent across sections (same review frequency, same framework cited)

■ N/A answers include brief justification ("Not applicable: we do not process payment card data")

The Minimum Viable Document Stack

If you could only have 10 documents to answer 80% of security questionnaires, these are the 10:

#	Document	Covers Questions About
1	**Information Security Policy**	Security programme, governance, framework alignment, board oversight
2	**Risk Register**	Risk management, risk appetite, treatment plans, risk owners
3	**Access Control Policy + Standard**	Authentication, authorisation, least privilege, admin controls
4	**Data Classification Policy + Standard**	Data handling, labelling, storage, transmission, destruction

#	Document	Covers Questions About
5	**Encryption Standard**	Algorithms, key management, TLS config, data at rest/transit
6	**Incident Response Plan**	IR process, roles, escalation, communication, breach notification
7	**Vulnerability Management Procedure**	Scanning, patching timelines, exceptions, tool inventory
8	**Vendor Risk Assessment Form**	Third-party risk, supply chain security, vendor due diligence
9	**BCP / DR Plan**	Business continuity, disaster recovery, RTO/RPO, backup testing
10	**Control Framework Mapping**	"Which framework?", compliance coverage, audit readiness

Get the Complete Document Stack

The GRC Starter Pack ($247) includes all 10 of these documents plus 9 more supporting tools — risk registers with formulas, evidence trackers with dashboards, and control mappings to NIST, ISO 27001, CIS Controls, and SOC 2. Deploy this week.

ridgelinecyber.com/products/grc-starter-pack/

Need complete policies, standards, and procedures? The Information Security Policy Suite covers all 18 policy areas with full framework traceability. From $149.

ridgelinecyber.com/products/information-security-policy-suite/

This is a free resource from RidgeLine Cyber Defence. It is not legal advice. Organisations should seek qualified professional advice for their specific circumstances and jurisdiction.
ridgelinecyber.com | contact@ridgelinecyber.com