The Security Questionnaire Readiness Checklist

The evidence customers, insurers, and funders actually ask for — and how to have it ready before they ask.

Sooner or later, someone your business depends on will ask how you protect the information they trust you with — a customer doing vendor due diligence, a cyber insurer at renewal, a funder reviewing a grant. The hard part is rarely the questions — it is the evidence: documents, records, and screenshots that prove what you say is true. **Tick every item you could produce within one business day.** The unticked boxes are your real exposure, and your work plan.

1 Know what you have

- ☐ An inventory of computers, servers, and devices your business uses
- ☐ A list of cloud services and software, and who administers each one
- ☐ A data map: what customer, patient, or client data you hold, and where it lives
- ☐ A simple diagram or written summary of how your network fits together

2 Control who gets in

- ☐ Multi-factor authentication enforced on email, remote access, and admin accounts
- ☐ A named account for every user — no shared logins
- ☐ A current list of accounts with administrator rights
- ☐ A written joiner/leaver process for granting and removing access
- ☐ A dated record of your most recent access review

3 Keep systems defended

- ☐ A patching schedule, and the most recent patch or update report
- ☐ Endpoint protection on every device, with a coverage list to prove it
- ☐ A recent vulnerability scan or equivalent check, with results
- ☐ Email filtering and anti-phishing protection in place

4 Back up — and prove recovery

- ☐ A documented backup schedule: what is backed up, how often, and where
- ☐ Backups protected against ransomware (offline, immutable, or access-controlled)
- ☐ A dated record of a restore test — backups you have actually recovered from
- ☐ A stated retention period that matches your policy

5 Be ready for an incident

- ☐ A written incident response plan, however short
- ☐ A contact list for the first phone calls: IT provider, insurer, bank, legal counsel
- ☐ Notes from a tabletop exercise, a real incident, or lessons learned
- ☐ Your cyber insurance policy details page, if you carry cover

6 Govern it on paper

- ☐ An information security policy that is dated and signed
- ☐ Your most recent risk assessment
- ☐ A risk register: each significant risk, its owner, and its treatment
- ☐ A remediation tracker showing findings you have closed, not just opened

7 Prepare your people

- ☐ Security awareness training records for staff
- ☐ Phishing-awareness activity or results, if you run them
- ☐ Signed acceptable-use acknowledgments
- ☐ Background checks where a role or a contract requires them

8 Manage your vendors

- ☐ An inventory of vendors that access your systems or your data
- ☐ Signed data-protection or business-associate agreements where they apply
- ☐ A security review or questionnaire response on file for critical vendors
- ☐ Breach-notification commitments in your vendor contracts

If several boxes are unticked, you are not unusual — you are unready.

That gap is exactly what Clyvara's Risk & Readiness Assessment closes: a fixed-scope engagement that assesses your risk against recognized frameworks (NIST CSF, ISO 27001, CIS Controls, HIPAA), evaluates your controls, and delivers a documented risk register and a remediation roadmap — ready to hand to the next customer, insurer, or funder who asks.

Rodger Lutalo, Principal Cybersecurity Consultant · rodger.lutalo@clyvara.io · (810) 228-4345 · clyvara.io · Dallas–Fort Worth · engagements delivered remotely across the United States

General guidance for planning purposes; it is not legal advice and does not by itself establish compliance with any framework or regulation. © 2026 Clyvara LLC.