

COMPLIANCE & SECURITY · CHECKLIST

Security Questionnaire Readiness Checklist

For revenue and operations leaders who need to respond to customer security reviews quickly and consistently instead of scrambling deal by deal.

How to use this: Draft a standing answer for each item below, store it in one shared location, and update it whenever a practice changes.

Data and Access Fundamentals

- ☐ Where is customer data hosted, and in which regions?
- ☐ Who inside the company can access customer data, and how is that access controlled?
- ☐ How is customer data encrypted, both in transit and at rest?
- ☐ What is the process for provisioning and removing employee access to systems holding customer data?
- ☐ Is multi-factor authentication required for access to production and customer data?

Vendors, Subprocessors, and Data Flow

- ☐ What third-party tools or subprocessors touch customer data, and for what purpose?
- ☐ Is there a current list of subprocessors that can be shared with customers on request?
- ☐ Are subprocessor agreements in place that require equivalent data protection standards?
- ☐ Is customer data ever used for purposes beyond delivering the product (e.g., model training, analytics)?

Continuity, Backup, and Incident Response

- ☐ How often is customer data backed up, and how is a restore tested?
- ☐ What is the process if a security incident or data exposure is suspected?
- ☐ Is there a named contact and timeline for notifying affected customers of an incident?
- ☐ What is the disaster recovery plan if core infrastructure becomes unavailable?

Certifications and Formal Frameworks

Do we currently hold any certifications (SOC 2, ISO 27001, etc.)? If not, what's the honest plan and timeline?

Have we ever completed a third-party penetration test or security audit? When, and what were the results?

What is our accurate, agreed-upon answer when a customer asks for a certification we don't yet have?

Readiness Tracker

Track how prepared you are to answer the most common question categories today.

Question Category	Answer Ready? (Y / N)	Owner	Last Updated
Data hosting & encryption			
Access control			
Subprocessors & vendors			
Backup & continuity			
Incident response			
Certifications			