Supplier security request checklist

Review a supplier from the evidence they already publish, then keep your questionnaire to the questions that evidence cannot answer. Process guidance only — no legal or contractual wording. Last reviewed 10 August 2026.

1. Before you send anything

- ☐ Write down what data the supplier will process, and how sensitive it is.
- ☐ Decide the depth of review this supplier warrants (light, standard, deep).
- ☐ Check whether the supplier already publishes a trust center or security page.
- ☐ Note which of your standard questions their published material already answers.
- ☐ Confirm who on your side signs off, and what evidence they need to sign off.

2. Documents to request

- ☐ Current SOC 2 Type 2 report, or ISO 27001 certificate and Statement of Applicability.
- ☐ Bridge letter if the latest audit period has not closed yet.
- ☐ Penetration test summary from the last 12 months.
- ☐ Security overview or whitepaper covering encryption, access control and logging.
- ☐ Incident response summary, including notification commitments.
- ☐ Business continuity and disaster recovery summary, with stated RPO and RTO.
- ☐ Subprocessor list with purpose and hosting region, plus its last-updated date.
- ☐ Data processing agreement and privacy policy.
- ☐ Evidence of insurance, where your process requires it.

3. Access terms to agree up front

- ☐ Who on your side needs the sensitive documents, and who does not.
- ☐ How long access is needed, and what happens at the end of the review.
- ☐ Whether copies may be stored, and if so where and for how long.
- ☐ Which NDA covers the exchange, and who signs it.
- ☐ Whether watermarked or view-only delivery is acceptable to your reviewers.

4. Questions worth keeping in a questionnaire

- ☐ What data will you hold for us, where will it be stored, and for how long?
- ☐ How is deletion handled at the end of the contract, and how is it evidenced?
- ☐ Which authentication options are available to us (SSO, SAML, MFA enforcement)?
- ☐ What are your notification timelines for a security incident affecting our data?
- ☐ Which subprocessors touch our data, and how are we told about changes?
- ☐ Which regions can we choose for hosting and support access?
- ☐ Any control your own obligations require that the published evidence does not cover.

5. Reviewing the evidence

- ☐ Check the report or certificate covers the service you are buying, not just the company.
- ☐ Check the audit period or certificate validity dates are current.
- ☐ Read the exceptions or non-conformities section, not only the opinion.
- ☐ Confirm the scope includes the systems that will hold your data.
- ☐ Record where each of your standard answers came from, for your own audit trail.

6. After the review

- ☐ Record the decision, the evidence relied on, and the reviewer.
- ☐ Set a reassessment date, and note which documents you expect to be refreshed by then.
- ☐ Confirm sensitive copies were deleted or access expired as agreed.
- ☐ Note the questions the supplier could not answer, for the next cycle.
- ☐ Share the reusable answers internally so the next team does not start again.