

Vendor Security Questionnaire

Everything needed to run a small-group roundtable before a supplier receives company information. The group walks the questionnaire: the program, the certificate, the data, access, incidents, subcontractors, and privacy. Includes a facilitator plan, agenda, discussion prompts, a four-stage tabletop, and a one-page handout.

Agenda

Time	Block	What happens
0:00 to 0:10	Welcome and hook	The person who owns suppliers opens. The facilitator tells one story about a payment sent to a new account after a supplier email. Ground rules.
0:10 to 0:25	Story round	Each person shares a questionnaire that came back too clean, a missing certificate, or a supplier they cannot explain. Capture themes on a flip chart.
0:25 to 0:50	Guided discussion	Work through 3 or 4 topics chosen from what the story round brought up.
0:50 to 1:10	Tabletop scenario	Groups of 3 or 4 work through The Friday Questionnaire, one stage at a time, then report back.
1:10 to 1:20	Gap check	Sticky notes: one supplier we could not explain today. Group them and rank them.
1:20 to 1:30	Commitments and close	Walk the handout. Each person names one questionnaire they will send or finish this week.

The Friday Questionnaire

Give each group one stage at a time, about 5 minutes apart. Groups answer each stage's question before seeing the next.

FRIDAY, 4 P.M.

A supplier returns the questionnaire with yes on every line. No certificate is attached. The contract is ready to sign on Monday, and the supplier will receive customer names.

Do you accept the questionnaire?

MONDAY, 9 A.M.

They send a certificate. The expiry date is last year. The place the data is stored is written as the cloud.

What do you ask for before any data moves?

MONDAY, 11 A.M.

On a call, they mention a second company that hosts the service and can see the data. That name is not on the questionnaire.

Is the questionnaire finished?

THE NEXT THURSDAY

An email from the supplier gives a new bank account for this month's invoice. The questionnaire said they would tell you about a security incident. This email does not say there was one.

Do you pay, and who do you call?

Debrief, after the groups report

- A yes with nothing attached is unfinished. Accepting it is a decision a named person makes, and the copy stays with the supplier record.
- Ask for a current certificate and a real location. The cloud is not enough to say where the data sits.
- A company that can see the data belongs on the questionnaire before access is turned on.
- A new bank account is confirmed with a number you already have. The number in the email is not that call.

2 weeks before

- Confirm the date, the room, and who is coming with the person who owns suppliers
- Bring one supplier whose questionnaire is missing, old, or all yes
- Send the invite with the ask to bring one story

Day of

- Print the handout, the scenario cards (one stage per card), and sticky notes
- Set up a flip chart with four columns: Certificate, Data, Access, Subcontractors

- Assign a note-taker

Within 1 week after

- Send a thank-you with the handout and the top 3 gaps raised
- Give the owner an action list: supplier, gap, suggested fix
- Log who came and which suppliers were named
- Schedule the quarterly refresher