FROM THE MAP, TRIAGE, HOLD FRAMEWORK

Vendor Due Diligence Question Bank

HOLD The questions to ask a vendor before you sign.

The questions that get the answers the scorecard needs, and the ones that surface the problem before you sign. Make them answer in writing. A verbal yes is not a commitment. Record each answer next to the question.

Data

1. Where is our data stored and hosted? _____
2. Who on your side can access it, and under what controls? _____
3. Can we export all of it, any time, in a usable format, without your help? _____
4. How long do you retain it, and how is it deleted when we leave? _____
5. Who are your sub-processors? _____
6. Is it encrypted in transit and at rest? _____

Security

1. What certifications do you hold, and can we see the report? _____
2. When were you last penetration tested, and by whom? _____
3. What is your breach history, and how fast do you notify us? _____

AI

1. Do you use our data to train or improve your models? Can we opt out, and is opt-out the default? _____
2. Is our data ever used to improve models other customers benefit from? _____
3. What model sits behind the AI, and where does it process our data? _____
4. Can we see how a given output was produced? _____
5. What happens when the AI is wrong, and what human oversight exists? _____

Integration and contract

1. How does it connect to our stack, and is the sync real-time or batch? _____
2. What happens to our integration when you ship an update? _____

3. What drives the price up, and is there a cap at renewal? _____
4. What are the termination terms, and how do we get our data back? _____

Red flags. A bad answer sounds like this.

“We may use your data to improve our services.” That usually means they train on it. Pin it down.

“SOC 2 in progress.” Not the same as holding it.

No clean way to export your own data without them.

Vague answers on where the AI processes your data.

Anything they will not put in writing.

Treat an evasive answer on data or AI as a finding, and often a dealbreaker.