

VIKRAM JHA - DEFENSIBLE AI QUESTION CARD

THE VENDOR QUESTION CARD

Version 1.0 - 23 August 2026

<https://vikramjha.work/artifacts/agent-vendor-question-card>

One question to ask every agent-platform vendor, asked identically each time, and the four answers you will get.

WHY IT EXISTS

Ask it exactly the same way each time. The value is not that the question is clever - it is that asking it identically makes the answers comparable across vendors, and the comparison is the finding. And ask it of yourself first: every question here applies to systems you have already built. If your own answer is the architecture diagram, the vendor's architecture diagram is not disqualifying, it is the industry.

WHAT IT CONTAINS

1. The single question, phrased for repetition rather than for cleverness
2. Two clarifications to have ready, because you will be asked for them
3. The four answers, and what each one actually tells you
4. Four follow-ups that escalate cleanly whatever the first answer was
5. Why using this as a gotcha costs you the information you came for

THE QUESTION

Then stop talking. Clarifications to have ready: 'Not the dashboard, and not the architecture - one action, and its authority record.' And: 'A real day, not a demo tenant.'

PICK A TUESDAY. LAST TUESDAY. SHOW ME ONE ACTION YOUR AGENT TOOK THAT DAY - AND EVERYTHING YOU WOULD HAND A REGULATOR WHO ASKED WHY IT WAS ALLOWED.

THE FOUR ANSWERS

THEY SHOW THE OBSERVABILITY PRODUCT - TRACES, SPANS, A TIMELINE, POSSIBLY VERY GOOD.

What it tells you: They have telemetry and are treating it as evidence. Telemetry records what happened; an authority record states what was permitted and by whom, and it has to exist at the moment of the action rather than be reconstructed afterward.

The follow-up: Does any line in that trace say what the human agreed to, or only what the system did afterward?

THEY EXPLAIN THE DESIGN - ROLES, POLICIES, A PERMISSIONS MODEL, POSSIBLY A WELL-BUILT ONE.

What it tells you: The control exists in the design. Whether it produced a record for that specific Tuesday is a separate and unanswered question. Design is a claim

about the general case; you asked for one instance.

The follow-up: I believe the design. I am asking what it emitted on Tuesday. Can you retrieve it?

THEY SAY THE RECORD DOES NOT EXIST IN THE FORM YOU ARE ASKING FOR.

What it tells you: More than the other three. You now know the true state, you know it before signing, and you are talking to someone who will tell you an inconvenient thing. Treat it as a positive signal about the relationship.

The follow-up: What would it take, on your side and mine, and would it be in the product or in my integration?

THEY HAND YOU THE RECORD. RARE - IT HAPPENS.

What it tells you: The product was built to be examined, which is a deliberate and expensive choice somebody made early. A record that exists can still fail to name a principal, an action, a boundary or an expiry.

The follow-up: Score it with the approval-record scoring worksheet, in the room, while you have their attention.

THE FOUR FOLLOW-UPS, IN ORDER

The same every time, whatever the first answer was.

WHO IS THE AGENT, TO THE SYSTEM, AT THE MOMENT IT ACTS?

What you are looking for: A principal - not an account, not a role.

WHAT WERE THE EDGES OF WHAT WAS APPROVED?

What you are looking for: A stated boundary, not the presence of assent.

IF I REVOKED IT RIGHT NOW, WHAT STILL LANDS?

What you are looking for: Whether anyone has measured it. 'Immediately' means nobody has.

COULD YOU ANSWER QUESTION ONE ABOUT A CALL FROM SIX MONTHS AGO?

What you are looking for: Retention that survives credential rotation.

HOW TO USE IT

1. Print it. Take it into the room. Ask the question in exactly the same words at every vendor meeting.
2. Record the answer type alongside whether a principal was named, a boundary stated, revocation measured, and six-month retention demonstrated.
3. Say out loud that this is not a gotcha. A vendor who cannot answer may be selling something that was never built to be examined - a fact about the product, legitimate to weigh, and not a verdict on the company or the people in the room.
4. Ask it of yourself before you ask it of anyone else.
5. Do not treat the answers as a ranking. They are a comparison of what each product can produce, which is a narrower and more useful claim.

Built from public standards and general practice. No client information appears

anywhere in this document. Regulatory instruments move - check anything cited here against its primary source on the day you rely on it.
Free to use and adapt; attribution welcome, not required.