

The Audit Readiness Test

Defensible governance. Defend any definition on demand.

Run the checklist against your own environment, not against a vendor's feature list. Work through it with the two or three people who would actually have to answer, and time the answers where noted. The time it takes to answer is usually the finding.

Score at the end of each one. The score tells you whether the problem is a workflow annoyance or an architecture gap, and the two need different budgets.

Every audit cycle becomes a project. Definitions get reconstructed from tribal knowledge, old emails, and whoever remembers the decision. The regulator asks when a field changed, who approved it, and what it meant at the time of a specific transaction.

SOX, GDPR, BCBS 239, CSRD, and the AI governance mandates now arriving all ask for documentation the estate cannot produce quickly. So the team assembles it by hand, before every window.

Section A: The questions an auditor asks

Answer each one for a single regulated metric, from the systems you have today. Record how long it takes.

- ☐ Name the metric and the regulation it falls under: [FILL IN]
- ☐ Who owns the definition, by name? [FILL IN]
- ☐ What did it mean on this date last year? [FILL IN]
- ☐ Who approved the last change to it, and when? [FILL IN]
- ☐ Every system it flows into, end to end: [FILL IN]
- ☐ Which policies apply at the point where it's consumed? [FILL IN]

Section B: Time the answers

- ☐ Time to answer all six questions above: [FILL IN]
- ☐ Person-days spent preparing for your last audit: [FILL IN]
- ☐ Number of separate systems you had to query to assemble the answer: [FILL IN]
- ☐ Findings or observations raised in your last audit related to data lineage or definitions: [FILL IN]

Section C: Requirements to test on any vendor call

- ☐ Is the whole metadata estate under version and configuration management, lineage, catalog entries, policies, and definitions together, so every change is logged, attributed, timestamped, and reversible?
- ☐ Can you query what a metric meant on an arbitrary past date, without restoring a backup?
- ☐ Does policy get applied where the data is used, and versioned where it changed?
- ☐ Is the lineage traceable to source code artifacts, at a standard an auditor accepts? Lineage by design, not by observation.
- ☐ For any metric compiled into a database or BI tool, is the enforced definition the same one under version control? The enforced definition should be the audited definition.
- ☐ Ask for the audit answer as a live query during the demo, using one of your own regulated metrics.

Score

1 point each for: over an hour to answer the six questions, more than 10 person-days on the last audit, three or more systems queried, an audit finding related to lineage or definitions, no named owner for the metric.

0 to 1. Audit readiness is a system state at your organization. Keep it there.

2 to 3. Readiness is a project you run before each window. It works until a regulator asks an unscheduled question.

4 to 5. The answers exist in people rather than in systems. Every audit carries the risk that the person who remembers has left.

Next step

Take the six questions in Section A into your next vendor conversation and ask for the answers as a live query against a sample of your own metadata. Every definition can defend itself.

Get in touch.

Request a demo to learn more about MetaKarta and how it helps you to be audit-ready.

[Request Demo](#)