

Audits shouldn't test your memory.

A self-assessment for DBAs, platform engineers, and compliance teams heading into audit season.

Every audit season brings the same request: show what changed in the database, when, where, and by whom, and prove it was approved. AI agents are making that harder. In Liquibase research, 96.5% of organizations report AI interacting with production databases, yet only 32% always or often create audit-ready change history.

The question isn't whether your team can rebuild the history.
It's whether they should have to.

ASSESS YOUR AUDIT EVIDENCE ACROSS FOUR AREAS

01

Visibility

Whether your evidence reaches the schema layer.

02

Change Evidence

Proof of what changed, when, where, and by whom.

03

Control Evidence

Proof that policies were enforced, not just written.

04

Audit Readiness

What your answers reveal about the effort audits demand.

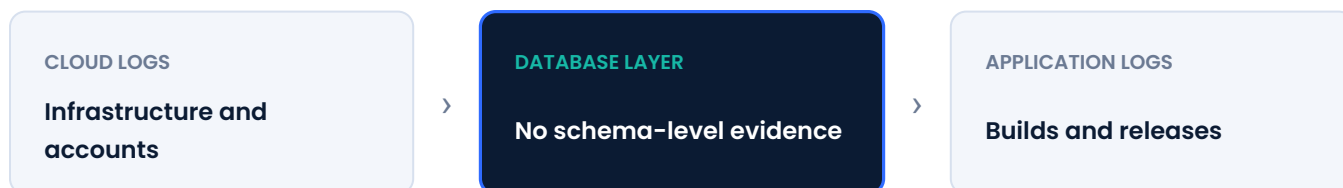
As you go, check every statement that describes your environment today. The goal is not a perfect score. It is to see where audit evidence depends on memory instead of a system of record.

The database layer is a compliance blind spot.

Most organizations have invested heavily in logging. Infrastructure changes are tracked, application releases are recorded, and cloud activity flows into a SIEM. None of those sources explain what happened inside the schema, which is exactly where auditors focus on regulated data.

CHECK EVERY STATEMENT THAT DESCRIBES YOUR ENVIRONMENT TODAY

- ☐ Infrastructure, application, and cloud logs are the primary evidence you rely on for database change.
- ☐ Schema changes, grants, and stored procedure updates are not captured in a single, queryable record.
- ☐ Changes made through a database console or ad hoc SQL leave little or no trace.
- ☐ AI agents or LLM tools touch production databases, but their activity isn't captured as its own record.
- ☐ You can't readily list every database that changed during the audit period, or what changed in each one.



Existing logs aren't wrong. They stop at the database boundary. They show that a deployment ran or a server was touched, not which table, column, permission, or procedure changed.

ASK ONE SIMPLE QUESTION

If an auditor picked a production table at random, could you show **every change made to it this year, who made it**, and how each one was approved, without asking a DBA to piece it together from memory?

Can you prove the change on demand?

Auditors don't accept recollection as evidence. They expect a record created when each change happened, whether a person or an AI agent made it, that no one could edit afterward.

CHECK EVERY STATEMENT THAT DESCRIBES YOUR ENVIRONMENT TODAY

- ☐ Answering an auditor's change request means searching scripts, tickets, email, and chat history.
- ☐ Change records live in spreadsheets, wikis, or files that can be edited after the fact.
- ☐ Tying a specific production change to the person who executed it requires asking around.
- ☐ You can't tell whether a production change was made by a person or an AI agent.
- ☐ Change populations for audit sampling are assembled by hand and hard to defend as complete.
- ☐ Preparing database change evidence takes days or weeks of DBA and compliance time.

THE STANDARD: UNALTERABLE EVIDENCE

Evidence you have to rebuild isn't evidence. It's a reconstruction.

Auditors want a system-generated record of every database change: what ran, when, where, and by whom. It should be captured automatically and protected from alteration, so it can be trusted on its own.

WHAT AUDITORS ASK FOR

What changed

The exact objects and statements that ran against each database.

When

A trustworthy timestamp tied to every deployment.

Where

The database, environment, and instance affected by each change.

By whom

The person, service account, or AI agent behind the change.

Can you prove the control, not just the change?

Showing that a change happened is only half the request. Auditors also need proof that your policies were strictly enforced every time, including for changes generated or deployed by AI agents.

CHECK EVERY STATEMENT THAT DESCRIBES YOUR ENVIRONMENT TODAY

- ☐ Change policies exist in writing, but enforcement depends on manual review.
- ☐ You can't show that every production change was approved before it was deployed.
- ☐ AI agents deploy changes through shared service accounts without dedicated controls.
- ☐ AI-generated SQL can reach production without the policy checks human changes receive.
- ☐ Emergency changes lack a consistent record linking approval to execution.
- ☐ Proving segregation of duties relies on screenshots, attestations, or manual reviews.

WHAT CONTINUOUS AUDIT EVIDENCE LOOKS LIKE

STAGE 1

Capture

Record every change as it runs.

STAGE 2

Attribute

Tie each change to a person or agent.

STAGE 3

Enforce

Apply policy before deployment.

STAGE 4

Detect

Surface out-of-process change.

STAGE 5

Protect

Keep records from being altered.

STAGE 6

Prove

Produce evidence on demand.

Audit evidence should be a byproduct of how database change happens, not a fire drill before every audit.

What did your answers reveal?

Count the statements you checked across the previous three sections. Use the result as a conversation starter, not a certification. Every checked statement is evidence someone will have to find, rebuild, or explain when the auditors arrive.

0 to 4 checked

AUDIT AWARE

Much of your database change is already captured. Close gaps in out-of-process change and control evidence before they surface in a sample.

5 to 10 checked

RECONSTRUCTING

Audit evidence depends on people and manual effort. Expect weeks of DBA and compliance time each audit season and a higher risk of exceptions.

11+ checked

BLIND SPOT

The database layer is largely invisible to your compliance program. Evidence is assembled from memory, and findings are likely to follow.

FIVE CAPABILITIES TO PRIORITIZE

- 01 Capture change at the source.** Record schema-level activity automatically as it happens.
- 02 Make evidence unalterable.** Protect change records from edits after the fact.
- 03 Attribute every change.** Tie each change to the person or AI agent behind it.
- 04 Enforce policy before deployment.** Prove controls ran, not just that they exist.
- 05 Keep evidence continuous.** Make audit readiness a standing state, not a seasonal project.

Make audit evidence continuous with Change Intelligence.

Liquibase Change Intelligence automatically captures database change activity, whether it comes from developers or AI agents, giving DBAs and compliance teams an unalterable record of what changed, when, where, and by whom, plus proof that policies were enforced.

[Explore Liquibase Change Intelligence](https://liquibase.com) · liquibase.com