

AI Audit Trail Checklist

Can you produce an audit trail for every AI action, today?

This is the question that decides whether AI reaches production in a regulated environment. If the answer is no, the runtime is the gap — not the policy.

CAPTURE

- ☐ Log every model call with actor, timestamp, model and version.
- ☐ Persist the prompt, the retrieved context and the response.
- ☐ Record tool and agent actions, including anything that writes to a system.
- ☐ Capture the permission decision that allowed the call.

RETAIN AND PROTECT

- ☐ Set a retention period that matches your regulatory obligation.
- ☐ Make logs tamper-evident and restrict who can delete them.
- ☐ Redact or tokenise personal data without losing traceability.
- ☐ Confirm logs survive vendor or model changes.

PRODUCE ON DEMAND

- ☐ Reconstruct any single AI action end to end within one working day.
- ☐ Report on evaluation results and failure rates over time.
- ☐ Show which actions were blocked, and why.
- ☐ Rehearse the request: run an internal audit drill before a real one.

A/DVNT Enterprise™ runs the operating layer that permissions, logs and evaluates every action — A/DVNT-managed or customer-operated. See advnt.ai/enterprise.