AI Agent Audit Log Checklist

What your AI agent should log, how long to keep it, who can read it, and how those logs become SOC 2 and EU AI Act evidence.

Checklist — Events Your Agent Must Log

Tick each item. If your agent does not capture it today, that is a gap to close.

- ■ Inputs and prompts: the user request and the full prompt sent to the model (redact sensitive fields where needed).
- ■ System context: the system prompt, instructions, and any retrieved documents used.
- ■ Tool calls: every tool or API the agent called, with the parameters it passed.
- ■ Tool results: what each tool returned to the agent.
- ■ Outputs: the agent's final response or action.
- ■ Model and version: the exact model name and version used for the run.
- ■ User / actor: the person or system that triggered the run, with their identity.
- ■ Timestamps: start and end time for the run and for each tool call.
- ■ Decisions and approvals: any decision made and any human approval or override.
- ■ Errors and retries: failures, timeouts, retries, and how they were handled.
- ■ PII access: a record whenever the agent read or wrote personal data, and which fields.
- ■ Session / trace ID: a unique ID that links every event in one run together.

Checklist — Retention Periods

- ■ Operational / debug logs: retain [30-90 days].
- ■ Security and access logs: retain [1 year] to support investigations.
- ■ Compliance evidence (decisions, approvals, PII access): retain [1-3 years] or as your regulator requires.
- ■ High-risk AI system logs (EU AI Act): retain at least the required period, often [6 months minimum] and longer by sector.
- ■ Deletion: automatically delete logs when their retention period ends, and log the deletion itself.
- ■ Minimization: do not store full PII in logs when a reference or hash will do.

Checklist — Access Controls on Logs

- ■ Role-based access: only named roles can read audit logs, and even fewer can export them.
- ■ Immutability: store logs so they cannot be edited or deleted before retention ends (write-once or append-only).
- ■ Separation of duties: the people who run the agents cannot alter the logs.
- ■ Encryption: encrypt logs at rest and in transit.
- ■ Meta-logging: log every access to the logs themselves.
- ■ Backups: back up logs and test that you can restore them.

Checklist — Review Cadence

- ■ Automated alerts: flag errors, unusual tool calls, and PII access in real time.
- ■ Weekly: review error and retry trends and any flagged events.
- ■ Monthly: sample agent runs and confirm decisions and approvals were logged correctly.
- ■ Quarterly: review access to the logs and confirm retention and deletion are working.

- After incidents: review the full trace and record lessons learned.

How Logs Map to SOC 2 Evidence

Trust Services Criteria	Evidence your logs supply
Security	Access logs and immutability show you control and monitor access.
Availability	Error, retry, and uptime logs show you monitor and respond to failures.
Processing integrity	Input, output, and decision logs show correct, complete processing.
Confidentiality	PII access logs and encryption show you protect sensitive data.
Monitoring	Review cadence and alerts show ongoing control operation auditors sample.

How Logs Map to EU AI Act Evidence

- Record-keeping: automatic logging over the system's lifetime supports the Act's logging requirement for high-risk AI.
- Traceability: session IDs and timestamps let you trace an outcome back to its inputs and model version.
- Human oversight: decision and approval logs show a human could review and override the AI.
- Transparency: model and version logs support your duty to document how the system works.
- Incident tracking: error and PII-access logs support reporting duties when something goes wrong.