

AI maintenance: what to include in a support scope

Assign ownership for quality tests, dependencies, incidents and data changes.

Updated October 29, 2026

An AI system can change when its code stays still. A hosted model, a source document or an upstream workflow can change its behaviour. Buy a maintenance process with named owners and evidence.

Keep a release record

Record the deployed model identifier, prompts, retrieval settings, dependencies and data sources. Store the test results used to approve the release. Require review before a material change reaches users. Keep a known working version and a documented rollback path.

The NCSC secure AI development guidance includes operation and maintenance. Use it to ask the supplier how it monitors deployed systems and responds to incidents. The NIST framework also treats risk management as ongoing work.

Monitor the business outcome

Track failure types that matter to the task. A support assistant may need checks for unsupported claims, leaked information and failed escalation. A document workflow may need checks for missing fields and incorrect routing. Compare current results against the accepted baseline. Review complaints and corrections as evidence, not just model scores.

Put support terms in writing

Name the incident contact and the person authorised to disable the system. Define severity by business impact. Specify coverage hours, response commitments, recovery steps and exclusions in the supplier agreement. Do not treat a response promise as a recovery promise.

Agree how usage costs are reported and who can change limits. Separate hosting, provider fees, planned improvements and defect fixes. Request deletion evidence when data is removed. Test export and recovery before you need them.

At renewal, inspect test history and incident records. Decide whether to continue, reduce scope or replace a dependency. A quiet dashboard is not enough evidence that the system is working.

Sources

- [NCSC, Guidelines for secure AI system development](#). Public page fetched 2026-10-29.
- [NIST, AI Risk Management Framework](#). Public page fetched 2026-10-29.

Frequently asked questions

Is this a supplier recommendation?

No. Use this guide to prepare a brief and check the supplier evidence yourself.