

Practical AI Adoption Workbook

Use this workbook to choose one limited AI pilot and decide whether it helps your team. Avoid promises about accuracy or return on investment until the pilot produces evidence.

Start with one measurable task

Pick a narrow, repeatable task with a human owner, such as drafting answers from approved support material. Record the current workflow and time spent. Define what a useful answer means and what must be escalated to a person.

Create an evaluation pack

Collect representative examples with permission. Include ambiguous questions, missing information and instructions that try to redirect the tool. Review outputs against a written rubric for correctness, relevance and appropriate refusal or escalation.

Limit data and authority

Map which information enters the model and who can retrieve it. Remove unnecessary personal or confidential data. Apply access checks to retrieval and downstream tools. Require human approval for consequential actions and define retention and deletion procedures.

Run a bounded pilot

Set limits for duration, users and cost. Track mistakes and the time reviewers spend correcting them alongside useful outcomes. Decide in advance when to pause the pilot. Compare results with the original workflow before expanding its scope.

Your project worksheet

Complete this with the people who will operate and support the system. Record evidence, owners and open questions before committing to a release.

Pilot task and human owner:

Current workflow / baseline:

Evaluation examples and success rubric:

Data sources, permissions and retention:

Escalation and approval boundaries:

Pilot duration, user and cost limits:

Decision: expand, revise or stop; evidence:

Primary reference

OWASP LLM application security project

Need help applying the checklist? Visit tawicode.in/contact. Keep passwords and secret keys out of this worksheet.