

CHECKLIST

20 REVIEW POINTS 10 MIN REVIEWED 10/08/2026

Start the AI pilot safely and measurably

Check use case, data, responsibility, quality limits and operational path before an AI pilot.

FOR WHOM

Departments, IT, data protection and project managers before the first use of AI with real work data.

WHEN TO USE IT

After an initial idea, but before choosing a provider, data sharing or productive access.

THE SHORT ANSWER

An AI pilot should only start when the purpose, permitted data, responsible persons, quality measurement, human control, cost framework and a safe exit path are determined.



Important boundary: This checklist is a practical initial check. It does not replace legal classification, data protection checks or risk assessments for the specific use of AI.

01 Purpose and suitability

The pilot needs a clear work task and a verifiable alternative to the current process.

☐ Describe a specific use case

Include input, expected output, user and today's processing.

☐ Separate benefits and consequences of errors

Evaluate time savings and quality as well as possible damage caused by incorrect results.

☐ Choose a suitable pilot scope

Start with frequent, limited processes and controllable error sequences.

☐ Eliminate unsuitable decisions

High-risk or difficult-to-verify decisions do not belong in an uncontrolled first attempt.

02 Data and provider path

Before the first test, it must be clear what information goes where and is created there.

☐ Record data types and origins

Mark personal, confidential, licensed and publicly available content.

☐ Set permitted test dates

Use reduced or synthetic data for early testing when real data has not yet been released.

☐ Check the provider's data paths

Clarify storage, model training, protocols, subcontractors, region and deletion.

☐ Protect access and secrets

API keys, roles, limits and separate environments are technically managed.

03

Role, risk and rules

Technical feasibility does not automatically answer the organizational and legal questions.

☐ **Name responsible people**

Technical responsibility, technology, data protection, security and approval are given clear responsibilities.

☐ **Classify your own role in the use of AI**

Document providers, operators, purpose, adjustments and affected persons.

☐ **Define human control**

Determine who reviews, corrects or rejects results and when.

☐ **Plan escalation and shutdown**

Errors, unexpected costs or data problems need an accessible decision-making path.

04

Quality and measurement

An impressive example is not a proof of quality for a recurring process.

☐

Collect test cases and edge cases

Use typical, difficult and deliberately unsuitable input from the real work context.

☐

Establish quality criteria

Define accuracy, completeness, traceability and permitted errors per task.

☐

Record initial value

Measure today's effort and typical mistakes so that the pilot can be compared.

☐

Determine go and no-go limits

Before the test, decide when to continue, improve or stop.

05

Operation and learning

A pilot already needs a limited operating route, even if it is not yet permanent production.

☐

Document versions and changes

Model, prompt, database and important parameters must be comprehensible for each test stand.

☐

Limit costs and usage

Budget, technical limits and warning thresholds prevent unnoticed expansion.

☐

Capture feedback and incidents

Users need an easy way to identify errors, impacts and suggestions for improvement.

☐

Schedule the next decision

Pilot, expansion, productive operation or stop are decided based on the previously defined criteria.

Result of the joint review

- ✔ A delineated and accountable AI use case
- ✔ Documented data paths and releases
- ✔ Measurable quality and termination criteria
- ✔ A limited pilot operation with human control

Related guidance

- AI readiness check →
- Classify the EU AI Act 2026 →
- AI consulting →

Sources and professional basis

This working aid translates general recommendations into a compact initial review. The primary sources and your specific context remain decisive.

- NIST: AI Risk Management Framework →
- NIST: AI RMF Playbook →
- EUR-Lex: Regulation EU 2024/1689 →

Frequently asked questions

Is the NIST AI RMF Playbook itself a checklist?



Can real customer data be used immediately in the pilot?



Browser checkmarks are not stored or transmitted to sudo/PORT.