

AI Act: audit checklist for your IT department

The AI Act classifies uses (not technologies) by risk level. Place each use case, then document it with the checklist.

The 4 risk levels

LEVEL	TYPICAL USES	OBLIGATION
Unacceptable	Social scoring, manipulation, sensitive biometrics.	Banned.
High risk	Employment (CV screening), credit, education, health, justice, critical infra.	Risk management, data, docs, human oversight, traceability.
Limited	Chatbots, generated content.	Transparency: disclose it's an AI.
Minimal	Summaries, writing, non-determining support.	No specific obligation (good practice).

Use-case audit checklist

- ☐ The use case is described (purpose, decision impacted, people affected).
- ☐ The risk level is determined and justified.
- ☐ The data used is qualified (source, quality, GDPR legal basis).
- ☐ Human oversight is planned wherever the decision matters.
- ☐ User transparency is ensured (people know an AI is involved).
- ☐ Traceability of decisions and model versions is in place.
- ☐ A compliance officer / DPO is involved.

Educational overview — not legal advice. Have high-risk uses validated by your DPO or a lawyer.