

AI ACT · READINESS 2026

Deploying AI is easy. Governing it is another story.

Only **13% of companies** are truly ready to deploy and govern AI — a figure that has held flat for three consecutive years. If your SME is among the 87% that haven't fully assessed their exposure, the clock is already running.

Source: Cisco AI Readiness Index 2025 — October 14, 2025



WHAT THE DATA SAYS

The 13% Figure — and the Widening Gap

13%

of companies are **fully ready** to deploy and govern AI — stable for 3 **consecutive years**, while adoption explodes.

Cisco AI Readiness Index 2025

The Gap in Numbers

20%

of EU companies use AI in 2025 — up from 13.5% in 2024, a **+6.5 point jump** in a single year.
(Eurostat)

83%

plan to deploy AI agents within the year — yet fewer than 1 in 8 have the governance to back it. *(Cisco)*

32%

have any process to measure the business impact of their AI investments.
(Cisco)

⚠️ Adoption is accelerating. Readiness is stalling. The gap is widening — and regulators are watching.



ADOPTION $\neq$ READINESS

These Are Two Different Realities

55% of large EU enterprises use AI. For SMEs, it's around 19%. But using is not governing. The AI Act doesn't ask **whether** you use AI — it asks whether you can **account for it** before a client, an auditor, or a market surveillance authority.

☒ Adoption

- Using an AI tool
- Deploying a model
- Having a use case
- Experimenting fast

✓ Readiness

- Governing an AI system
- Documenting its decisions
- Proving compliance
- Tracing, auditing, justifying

Source: Eurostat — Use of AI in enterprises, 2025 (SMEs 19%, large enterprises 55%)

The AI Act Is a **Binding Legal Framework** — Not a Best-Practice Guide

1

Art. 9 — Risk Management

A documented risk register, maintained **throughout the system's full lifecycle** — not a one-time exercise.

2

Art. 10 — Data Governance

Full documentation of training, validation, and test data sets used to build or fine-tune the system.

3

Art. 11 + Annex IV — Technical File

A complete technical documentation file must exist **before** placing the system on the market.

4

Art. 14 — Human Oversight

Mechanisms enabling a human to **control, correct, or interrupt** the AI system at any point.

5

Art. 17 — QMS

A dedicated, auditable Quality Management System covering the AI lifecycle end to end.



Penalty — Article 99

Up to **€35M or 7% of global turnover** for prohibited practices — **75% higher** than the GDPR ceiling of 4%. For SMEs, the lower amount applies (Art. 99(6)).



Enforcement Timeline

- **Feb. 2025:** Prohibited practices (Art. 5) — **already in force**
- **Aug. 2025:** GPAI obligations — **already in force**
- **Dec. 2, 2027:** High-risk systems (Annex III)
- **Aug. 2, 2028:** Embedded high-risk systems (Annex I)

Think You're "Just a User"? Article 25 Can Reclassify You Automatically.

The AI Act draws a sharp line between two roles carrying very different obligations. The trap: that line can shift without any notification — and your supplier contract won't protect you.



Deployer

Uses an AI system as intended → **limited obligations**.
Monitors, reports incidents, maintains logs.



Provider

Places a system on the market → **heavy obligations**: Art. 16, Annex IV file, conformity assessment, CE marking.

The 3 Reclassification Triggers — Art. 25(1)

→ Branding (White-Label)

You put your name or trademark on an existing high-risk system → you become a Provider.

→ Substantial Modification

You significantly modify a high-risk system — including fine-tuning — → you become a Provider.

→ Change of Intended Purpose

You repurpose a system (including a GPAI model) toward a high-risk use → you become a Provider.

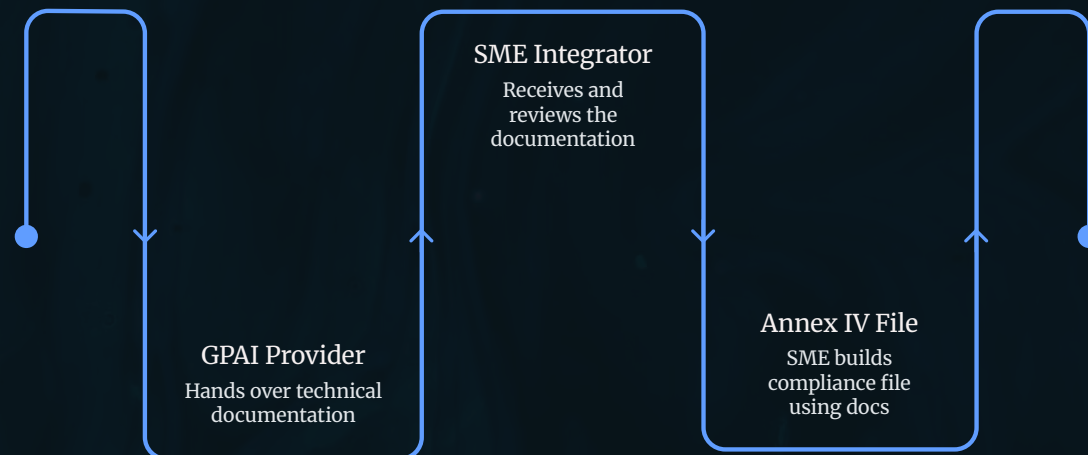
⊗ Reclassification is automatic. No notification, no registration. Your contract with your supplier does not protect you — this is a factual qualification, not a contractual one.

You Build **on Top** of a Foundation Model. That Changes Your Obligations.

What the Law Provides — Art. 53(1)(b) + Annex XII

Most SMEs don't develop foundation models (GPAI). They do **fine-tuning**, **RAG**, or deploy a **third-party API** on top of an existing model. The law anticipates this: the GPAI provider must pass downstream integrators the technical documentation needed to understand capabilities, limitations, and to meet their own compliance obligations.

This documentation **flows up the chain** — you use it to build part of your own Annex IV technical file.



⚠ The Open-Source Blind Spot

⚠ Art. 53(2) open-source exception: an open-source model provider is **not** required to supply downstream technical documentation.

If you build on an open-source model, you **inherit a documentation gap** that you must fill entirely on your own. The technical file obligations don't disappear — they fall squarely on you.

The choice of underlying model is therefore not just a technical decision. **It is a compliance decision.**

THE 3 DANGEROUS BELIEFS

What Most Leaders Think — And Why It's Wrong

✘ "We're GDPR-compliant, so we're covered."

GDPR protects **personal data**. The AI Act governs the **systems** that process it. Two scopes, two legal logics, two distinct types of enforceable proof. Strong GDPR maturity helps with data governance — but it does not satisfy a single AI Act obligation on its own.

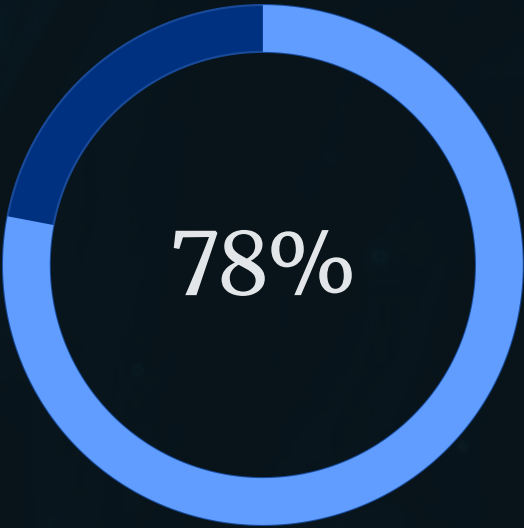
✘ "We're not big enough to be in scope."

The AI Act applies as soon as an AI system is **placed on the EU market** or produces effects within it — **regardless of company size**. An SME supplying an AI tool to a regulated sector (finance, healthcare, HR) is in scope as a Provider, with the full set of Provider obligations.

✘ "We do versioning and testing — we're solid."

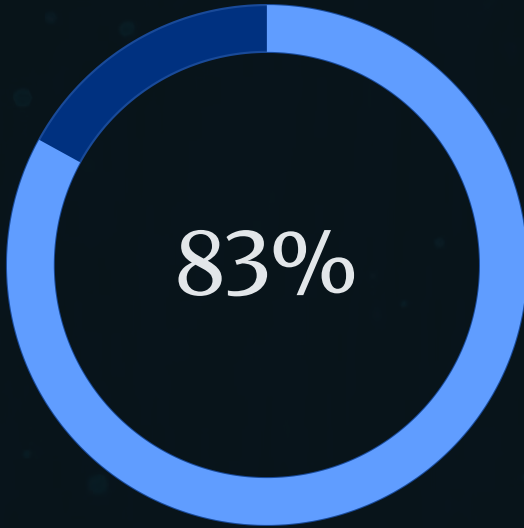
Code versioning and regression testing are good engineering. But before an auditor, **technique without a procedural framework** — QMS (Art. 17), risk register (Art. 9), Annex IV file — is worth nothing. Compliance is not a technical artifact. It is a **chain of enforceable evidence**.

The Gap Between Perceived Urgency and Actual Capacity



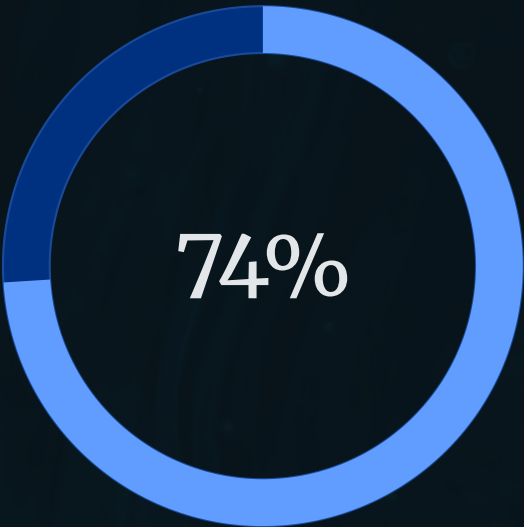
No Meaningful Steps

of organisations have taken no meaningful action toward AI Act compliance



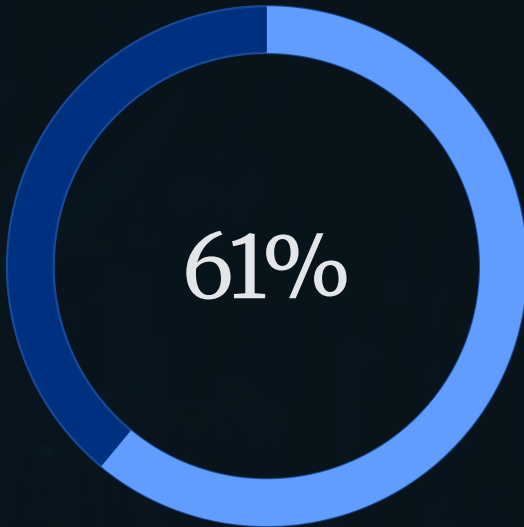
No AI Inventory

have no formal inventory of their active AI systems — shadow AI included



No Governance Owner

have designated no owner or governance body responsible for AI oversight



No Documentation Process

have no process to produce the technical documentation required for high-risk systems

Vision Compliance — EU AI Act Readiness Analysis, April 2026

⚠ The NIS2 parallel: in force since October 2024, yet only 16% of in-scope companies consider themselves fully compliant. Same root causes — budget gaps, lack of guidance, insufficient internal expertise. The AI Act is following the exact same trajectory.

It's Not About Ticking Boxes. It's About Producing Enforceable Evidence.

☒ Surface Compliance

- AI policy written
- One-off annual audit
- Training delivered to staff
- Declaration of conformity signed
- Governance documented on paper

✓ Operational Readiness

- Risk register maintained continuously (Art. 9)
- Runtime traceability of every AI decision
- Complete Annex IV technical file (Art. 11)
- Enforceable evidence per AI system
- Auditable QMS in place (Art. 17)

What Market Surveillance Authorities Can Request

- The complete technical documentation (Annex IV) for every high-risk system
- The risk register and its **full update history** since deployment

- Decision logs retained for a **minimum of 6 months** (Art. 19 — automatically generated logs)
- Direct access to the system itself for **testing and evaluation** by the authority

The Moment Non-Compliance Becomes Visible

Illustrative scenario — timeframes are examples, not statistics. The market dynamic below is sourced.

The Scenario

An AI SME signs a contract with a major account — a bank, insurer, or industrial player. Regulatory due diligence is triggered. **10 days** to produce the full documentation package.

What Is Requested

- Inventory of all AI systems supplied or in use
- Risk classification for each system
- Annex IV technical documentation for high-risk systems
- Risk register with update history
- Evidence of human oversight + Provider/Deployer role clarification (Art. 25)

What Happens Without Preparation

- Inventory missing or partial → **blocking**
- Regulatory role unclear (Art. 25?) → **blocking**
- Documentation scattered or absent → **blocking**
- Result: deal lost, or delayed by **3 to 6 months**

The Market Signal — This Is Not Theoretical

On NIS2, **42%** of companies have already been required to **prove** their compliance by partners. **41%** by investors. **36%** by clients. Proof is becoming a condition of market access — **before** official enforcement deadlines.

CyberSmart NIS2 Survey — April 2026

The Question Is Not *"If"* You'll Be Asked. It's *"When"* — and Whether You'll Be Ready.

Three diagnostic questions every SME leader should be able to answer with certainty — not approximation.

1

Inventory

Do you have a **complete, up-to-date inventory** of all active AI systems — including shadow AI, third-party tools, and external APIs?

2

Regulatory Role

Do you know whether you're a **Provider or Deployer** for each system — and whether fine-tuning or rebranding has already reclassified you under Art. 25?

3

Evidence

Could you **reconstruct an AI decision** — data, model version, output — and defend it before an auditor **today**?

📝 Answer in the comments: **Yes / No / In progress** — and tell us: on what basis do you answer "Yes"?

Slide 11/11 · AI Act Readiness Series · Week 1/12 · Next: The dangerous myth — "We're GDPR-compliant, so we're covered."