

FREE PRACTITIONER GUIDE · 2026 EDITION

EU AI Act Readiness Checklist

32 controls mapped to NIST AI RMF and ISO/IEC 42001. Built for CISOs, compliance officers, and heads of AI governance shipping AI systems into production in 2026.

Audience	CISOs · Compliance · AI Governance leads
Use case	Pre-audit gap analysis · vendor reviews · board reporting
Frameworks	EU AI Act · NIST AI RMF 1.0 · ISO/IEC 42001:2023
Updated	May 2026

How to use this checklist

Work through the seven sections below with the system owner for each AI use case in scope. Mark each control as **Met**, **Partial**, or **Gap**. Anything not Met becomes a remediation item with an owner and a date. Re-run quarterly, or after any material model change. Riskora customers automate steps 2 through 7 with continuous monitoring.

Risk-tier triage in 60 seconds

Before you score controls, classify the system: **Prohibited** (Art. 5), **High-risk** (Annex III or safety component of regulated product), **Limited-risk** (transparency obligations apply), or **Minimal-risk**. GPAI providers carry a separate track. Anything you classify as high-risk requires every control in sections 2 through 6.

1. Governance and AI literacy

Control	Article / Reference
<input type="checkbox"/> Documented AI literacy programme covering all staff who develop, deploy, or oversee AI systems.	Art. 4
<input type="checkbox"/> Named accountable owner for each AI system, with deputy and escalation path.	Art. 17
<input type="checkbox"/> AI inventory maintained with risk tier, lawful basis, data sources, and last review date.	Art. 17
<input type="checkbox"/> Prohibited-practice screen run on every new system before procurement or deployment.	Art. 5

2. Risk management system

Control	Article / Reference
<input type="checkbox"/> Iterative risk management lifecycle documented for each high-risk system.	Art. 9
<input type="checkbox"/> Foreseeable misuse scenarios identified, with mitigations and residual risk acceptance.	Art. 9
<input type="checkbox"/> Risks to vulnerable groups (minors, persons with disabilities) explicitly assessed.	Art. 9
<input type="checkbox"/> Fundamental Rights Impact Assessment (FRIA) completed for deployer obligations where applicable.	Art. 27

3. Data and data governance

	Control	Article / Reference
<input type="checkbox"/>	Training, validation, and test datasets documented with provenance and licensing.	Art. 10
<input type="checkbox"/>	Bias evaluation across protected characteristics performed and remediated.	Art. 10
<input type="checkbox"/>	Data-quality criteria (relevance, representativeness, accuracy) recorded.	Art. 10
<input type="checkbox"/>	Special-category data processing has Art. 10(5) lawful basis and safeguards documented.	Art. 10

4. Technical documentation and record keeping

	Control	Article / Reference
<input type="checkbox"/>	Annex IV technical documentation maintained and version controlled.	Art. 11
<input type="checkbox"/>	Automated event logging enabled for the system lifecycle, retained for at least 6 months.	Art. 12
<input type="checkbox"/>	Logs accessible to competent authorities on request, with retention policy enforced.	Art. 18
<input type="checkbox"/>	Model cards updated on every material retrain or fine-tune.	Art. 11

5. Transparency, oversight, accuracy

	Control	Article / Reference
<input type="checkbox"/>	Instructions for use provided to deployers, including known limitations and accuracy metrics.	Art. 13
<input type="checkbox"/>	Human oversight measures designed in, with stop, override, and review controls.	Art. 14
<input type="checkbox"/>	Accuracy, robustness, and cybersecurity targets defined and continuously measured.	Art. 15
<input type="checkbox"/>	End-user disclosure for AI interaction, deepfakes, and emotion-recognition where required.	Art. 50

6. Quality management, conformity, post-market

Control		Article / Reference
<input type="checkbox"/>	Quality management system covers design, development, testing, and change management for AI.	Art. 17
<input type="checkbox"/>	Conformity-assessment route selected (internal control or notified body) and evidence prepared.	Art. 43
<input type="checkbox"/>	EU declaration of conformity drafted for each high-risk system.	Art. 47
<input type="checkbox"/>	CE marking applied where the system is a regulated product or safety component.	Art. 48
<input type="checkbox"/>	Post-market monitoring plan operational, with metrics and review cadence.	Art. 72
<input type="checkbox"/>	Serious-incident reporting procedure to the market-surveillance authority within 15 days.	Art. 73

7. GPAI and third-party AI

Control		Article / Reference
<input type="checkbox"/>	GPAI provider responsibilities understood, including model card and copyright policy.	Art. 53
<input type="checkbox"/>	Systemic-risk thresholds tracked for any model exceeding 10^{25} FLOP training compute.	Art. 55
<input type="checkbox"/>	Downstream deployer obligations assessed for any third-party AI you embed.	Art. 25
<input type="checkbox"/>	Contractual flow-down of AI Act obligations included in vendor agreements.	Art. 25
<input type="checkbox"/>	Authorised representative appointed if you place AI on the EU market from outside the Union.	Art. 28
<input type="checkbox"/>	Voluntary code-of-conduct commitments documented for limited and minimal-risk systems.	Art. 95

Scoring and what to do with the result

Tally each section as a percentage of controls fully Met:

≥ 90%	Audit-ready. Schedule an external assurance review and lock evidence.
70 – 89%	Operationally sound. Close the remaining gaps inside one quarter.
40 – 69%	Material exposure. Stand up a remediation programme with executive sponsor.
< 40%	Stop deploying new high-risk systems until governance basics are in place.

Where Riskora helps

Riskora AI continuously monitors sections 2 through 7 against your live AI estate. Shadow-AI discovery, automated FRIAs, post-market monitoring, and incident reporting are wired in from day one, with evidence exported on demand for auditors and regulators.

Next step: Book a 20-minute walkthrough at riskoraai.com/demo and we will map this checklist to your environment.

Disclaimer: This checklist is educational guidance distilled from the EU AI Act (Regulation 2024/1689) and aligned frameworks. It is not legal advice. Confirm obligations with qualified counsel for your specific use case.