EU AI ACT
AUDIT CHECKLIST

3-Step Audit You Can Start This Week

Risk Classification · Compliance Gap Analysis · Vendor Due Diligence

Includes complete Vendor Compliance Checklist

REGULATION (EU) 2024/1689 | PRACTICAL EDITION | 2025

Table of Contents

OVERVIEW

Overview: The EU AI Act

The EU AI Act (Regulation 2024/1689) is the world's first comprehensive legal framework governing artificial intelligence systems. Adopted in May 2024 and entering force in August 2024, it applies a risk-based approach — imposing strict obligations on high-risk systems while allowing lower-risk AI to operate with lighter-touch requirements. Non-compliance carries fines of up to €35 million or 7% of global turnover.

Who Must Comply?

The Act has broad territorial scope — it applies to any organisation that places AI systems on the EU market or puts them into service within the EU, regardless of where the organisation is based. This means:

- **EU-based companies** developing or deploying AI systems of any kind
- **Non-EU companies** (US, UK, Asia-Pacific) whose AI output is used within the EU
- **AI providers** (developers/vendors) placing systems on the EU market
- **AI deployers** (organisations using third-party AI in their operations)
- **Importers and distributors** of AI systems within the EU supply chain

> **Even if your organisation is headquartered outside the EU, if your AI systems affect EU residents — customers, employees, or users — you are within scope and must comply.**

Key Deadlines & Timelines

Milestone	Date	What's Required
Act enters into force	1 August 2024	Regulation officially published
Prohibited practices ban	2 February 2025	All prohibited AI uses must cease
GPAI model obligations	2 August 2025	General Purpose AI rules apply
High-risk AI (Annex I)	2 August 2026	Full obligations for regulated-sector AI
High-risk AI (Annex III)	2 August 2027	Full obligations for other high-risk AI
Full application	2 August 2027	Complete framework in force

Table 1 — EU AI Act implementation timeline. Dates per Regulation (EU) 2024/1689.

Compliance KPIs at a Glance

€35M	€15M	€7.5M	2025	85+
Max Fine	**Prohibited AI**	**False Info**	**First Deadline**	**High-Risk Uses**
or 7% global turnover	or 3% for violations	or 1.5% of turnover	Feb 2 — banned uses	Annex III categories

RISK CLASSIFICATION FRAMEWORK

Risk Classification Framework

The EU AI Act organises AI systems into four risk tiers. Your obligations — and the penalties for non-compliance — differ dramatically depending on which tier your systems fall into. Correct classification is the essential first step of any compliance programme.

The Four-Tier Risk Model

Tier	Risk Level	Examples	Key Obligations	Penalty
Tier 1	UNACCEPTABLE — PROHIBITED	Social scoring, real-time biometric surveillance, subliminal manipulation	BANNED — must cease operations by Feb 2025	€35M or 7%
Tier 2	HIGH RISK	CV screening, credit scoring, medical devices, critical infrastructure AI	Full conformity assessment, registration, human oversight, documentation	€15M or 3%
Tier 3	LIMITED RISK	Chatbots, deepfakes, emotion recognition	Transparency obligations — users must be informed they interact with AI	€7.5M or 1.5%
Tier 4	MINIMAL RISK	Spam filters, AI in games, recommendation engines	No mandatory obligations; voluntary codes of conduct encouraged	None

Table 2 — EU AI Act risk tier classification overview.

Prohibited AI Practices (Tier 1 — Banned from Feb 2025)

- Subliminal or manipulative techniques that distort human behaviour beyond conscious awareness
- Exploitation of vulnerabilities of specific groups (age, disability) to distort behaviour
- Social scoring systems by public authorities based on personal characteristics or behaviour
- Real-time remote biometric identification in public spaces (with very limited exceptions)
- Biometric categorisation inferring race, political opinions, religion, sexual orientation
- Emotion recognition in workplace or educational settings
- Predictive policing based solely on profiling or personality trait assessment
- Facial recognition databases built by scraping internet or CCTV images

IMMEDIATE ACTION REQUIRED: If any current AI system falls into a prohibited category, it must be decommissioned or fundamentally redesigned before 2 February 2025. This is non-negotiable.

High-Risk AI Categories (Annex III — Key Examples)

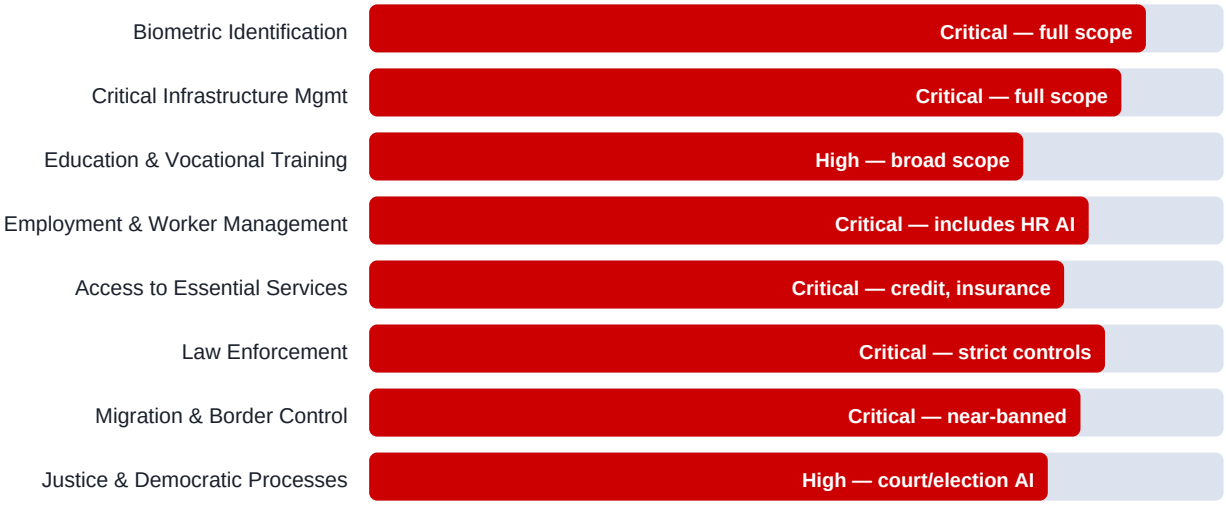

Figure 1 — High-risk AI categories (Annex III) with compliance criticality rating.

1

Map Your AI Inventory

Before you can comply, you need a complete picture of every AI system your organisation develops, deploys, or procures. Most organisations discover 40–60% more AI touchpoints than they expected during this step.

STEP 1 · MAP YOUR AI INVENTORY

Step 1 — AI System Discovery Checklist

Complete all items below for every AI system in scope. Aim to finish within 2 weeks. Use the classification worksheet on the next page to assign each system a risk tier.

- ☐ #01 **Identify all AI systems in use** — MANDATORY
  Audit all software, tools, APIs, and platforms using machine learning or automated decision-making.
- ☐ #02 **Include third-party and vendor AI** — MANDATORY
  Document all AI embedded in SaaS tools, ERP systems, HR platforms, and analytics dashboards.
- ☐ #03 **Map AI to business processes** — MANDATORY
  For each system, identify which business process it supports and what decisions it influences.
- ☐ #04 **Identify AI that affects EU persons** — MANDATORY
  Flag any system whose output affects EU-based employees, customers, or users.
- ☐ #05 **Document data inputs and outputs** — MANDATORY
  List data types consumed and decisions/outputs produced by each system.
- ☐ #06 **Identify the operator role** — MANDATORY
  Determine whether your organisation is the provider, deployer, importer, or distributor.
- ☐ #07 **Assess existing documentation** — RECOMMENDED
  Collect technical documentation, data sheets, and vendor agreements for each system.
- ☐ #08 **Interview business unit owners** — RECOMMENDED
  Conduct structured interviews with teams using AI to surface undisclosed or shadow AI.

☐ #09 **Check upcoming AI projects** — RECOMMENDED

Review roadmap and procurement pipelines to identify AI systems coming into scope.

☐ #10 **Create a centralised AI register** — BEST PRACTICE

Log all systems in a single register with owner, purpose, data types, and risk classification.

AI System Classification Worksheet

System Name	Purpose / Use Case	Data Types Used	Affects EU Persons?	Proposed Risk Tier	Owner
[System 1]			Yes / No	Unacceptable / High / Limited / Minimal	
[System 2]			Yes / No		
[System 3]			Yes / No		
[System 4]			Yes / No		
[System 5]			Yes / No		

Table 3 — AI System Inventory & Classification Worksheet. Complete one row per system.

2

Conduct Your Compliance Gap Audit

For each high-risk or limited-risk AI system identified in Step 1, work through the following checklists to identify compliance gaps. Prioritise by risk tier — start with any potential Tier 1 systems immediately.

STEP 2 · COMPLIANCE GAP AUDIT

Step 2 — Compliance Gap Audit Checklists

A. High-Risk System Requirements

All high-risk AI systems must satisfy the following requirements before deployment or by the applicable deadline. Use this checklist to assess current compliance and identify gaps.

- ☐ #11 **Technical documentation prepared** — MANDATORY
  Maintain Article 11 documentation: system description, design specs, training data, validation.
- ☐ #12 **Conformity assessment completed** — MANDATORY
  Conduct required conformity assessment (self-assessment or third-party notified body).
- ☐ #13 **CE marking applied (where required)** — MANDATORY
  Affix CE marking and issue EU Declaration of Conformity for applicable systems.
- ☐ #14 **Registration in EU database** — MANDATORY
  Register high-risk AI systems in the EU AI public database before deployment.
- ☐ #15 **Risk management system in place** — MANDATORY
  Implement a documented risk management system covering design, testing, and post-deployment.
- ☐ #16 **Quality management system established** — MANDATORY
  Establish QMS covering design, development, testing, deployment, and post-market monitoring.
- ☐ #17 **Automatic logging enabled** — MANDATORY
  Ensure system automatically logs events at a level that enables post-hoc traceability.
- ☐ #18 **Accuracy, robustness & cybersecurity** — MANDATORY
  Demonstrate the system meets appropriate accuracy thresholds and is resilient to adversarial inputs.

B. Transparency Obligations

- [ ] #19 **Users informed when interacting with AI** — MANDATORY
  Any system interacting with humans must clearly disclose it is an AI system in real time.
- [ ] #20 **Deepfake/synthetic content labelled** — MANDATORY
  AI-generated images, video, or audio must be marked as artificially generated.
- [ ] #21 **Emotion recognition disclosed** — MANDATORY
  Persons subjected to emotion recognition systems must be informed of that fact.
- [ ] #22 **Instructions for use provided** — MANDATORY
  Deployers must receive clear instructions for use, including limitations and foreseeable misuse.
- [ ] #23 **Plain language transparency notice** — RECOMMENDED
  Develop user-facing notices explaining AI decision-making in plain, accessible language.

C. Human Oversight Requirements

- [ ] #24 **Human oversight measures built in** — MANDATORY
  High-risk AI must be designed to allow human oversight during operation — not merely available.
- [ ] #25 **Override and stop capability** — MANDATORY
  Humans must be able to override, interrupt, or stop the system at any point.
- [ ] #26 **Trained oversight personnel assigned** — MANDATORY
  Individuals assigned to oversight roles must have capability, authority, and training to act.
- [ ] #27 **Oversight procedures documented** — MANDATORY
  Document exactly how, when, and by whom human oversight is exercised for each system.
- [ ] #28 **Oversight effectiveness tested** — RECOMMENDED
  Periodically test whether human oversight mechanisms are functioning as intended.

D. Data Governance Checklist

- [ ] #29 **Training data documented** — MANDATORY
  Document data sources, collection methods, labelling procedures, and known biases.

- [ ] #30 **Data quality assessment conducted** — MANDATORY
  Assess training and validation datasets for relevance, representativeness, and freedom from errors.

- [ ] #31 **GDPR alignment verified** — MANDATORY
  Confirm all data used for training and inference complies with GDPR lawful basis requirements.

- [ ] #32 **Bias and discrimination testing** — MANDATORY
  Test for discriminatory outputs across protected characteristics; document results and mitigations.

- [ ] #33 **Data minimisation applied** — RECOMMENDED
  Ensure only data necessary for the AI purpose is collected, used, and retained.

- [ ] #34 **Data retention policies set** — RECOMMENDED
  Define how long training data, logs, and outputs are retained and under what conditions deleted.

3

Remediate & Build Ongoing Governance

Gap audit complete — now fix what's broken and put structures in place so you don't drift out of compliance. Governance is not a one-time exercise; the Act requires continuous monitoring, incident reporting, and adaptation.

STEP 3 · REMEDIATE & GOVERN

Step 3 — Remediation & Governance

Remediation Priority Matrix

Gap Category	Risk Tier	Urgency	Typical Effort	Priority Score
Prohibited AI still in use	Tier 1	IMMEDIATE	High — decommission	P0 — Stop Now
Missing conformity assessment	Tier 2	CRITICAL	High — 4–12 weeks	P1
No EU database registration	Tier 2	CRITICAL	Low — 1–3 days	P1
Human oversight not in place	Tier 2	HIGH	Medium — 2–6 weeks	P2
Technical documentation gaps	Tier 2	HIGH	Medium — 2–8 weeks	P2
Transparency notices missing	Tier 3	MEDIUM	Low — 1–2 weeks	P3
Logging/monitoring absent	Tier 2	HIGH	Medium — 2–4 weeks	P2
Data governance deficiencies	Tier 2	HIGH	High — 4–16 weeks	P2
Vendor contracts not updated	Tier 2–3	MEDIUM	Medium — 2–6 weeks	P3
Incident reporting not set up	Tier 2	MEDIUM	Low — 1–2 weeks	P3

Table 4 — Remediation Priority Matrix. Address P0 immediately; schedule P1 within 30 days.

Building Your AI Governance Framework

Compliance is not just a checklist — it requires a governance structure that embeds accountability into your organisation. The following elements are required or strongly recommended:

☐ #35 **Appoint an AI Compliance Officer** RECOMMENDED

Designate a named individual responsible for EU AI Act compliance across the organisation.

- [ ] #36 **Establish an AI Governance Committee** — RECOMMENDED
  Form a cross-functional committee (legal, IT, risk, business) to oversee AI governance.

- [ ] #37 **Develop an AI Policy** — RECOMMENDED
  Create a formal AI policy covering acceptable use, risk classification, and compliance obligations.

- [ ] #38 **Implement AI impact assessments** — RECOMMENDED
  Before deploying new AI, conduct structured impact assessments covering risk, bias, and rights.

- [ ] #39 **Build a post-market monitoring process** — MANDATORY
  Establish mechanisms to monitor high-risk AI performance after deployment and log incidents.

- [ ] #40 **Set up serious incident reporting** — MANDATORY
  Create a process to report serious incidents and malfunctions to competent authorities within 15 days.

- [ ] #41 **Train employees on AI Act obligations** — RECOMMENDED
  Ensure all teams using or developing AI are trained on their obligations under the Act.

- [ ] #42 **Conduct annual compliance review** — BEST PRACTICE
  Schedule a formal annual review of all AI systems, governance structures, and compliance status.

VENDOR COMPLIANCE CHECKLIST

Vendor Compliance Checklist

When your organisation uses AI systems built by third-party vendors, you remain responsible — as the deployer — for compliance with the EU AI Act. This section gives you the complete due diligence and contractual framework to manage that responsibility effectively.

Pre-Procurement Due Diligence

- [ ] #43 **Request vendor risk classification** — MANDATORY
  Ask the vendor to confirm the risk classification of their AI system under the EU AI Act.
- [ ] #44 **Obtain technical documentation** — MANDATORY
  For high-risk systems, request Article 11 technical documentation before contracting.
- [ ] #45 **Verify conformity assessment** — MANDATORY
  Confirm the vendor has completed the required conformity assessment for Tier 2 systems.
- [ ] #46 **Check EU database registration** — MANDATORY
  Verify the system is registered in the EU AI public database (for high-risk systems).
- [ ] #47 **Review data practices** — MANDATORY
  Understand what data the vendor's AI uses, how it is processed, and where it is stored.
- [ ] #48 **Assess human oversight capability** — MANDATORY
  Confirm the vendor's system supports meaningful human oversight and override functions.
- [ ] #49 **Evaluate vendor AI governance maturity** — RECOMMENDED
  Assess whether the vendor has an AI policy, governance committee, and incident reporting process.
- [ ] #50 **Request bias and accuracy testing results** — RECOMMENDED
  Ask for evidence of bias testing and accuracy validation across relevant demographic groups.

Contract Clauses Checklist

Ensure the following provisions are included in all contracts with AI vendors whose systems are used in EU-affecting operations:

Contract Provision	Risk Tier	Priority
Vendor confirms EU AI Act compliance and risk classification	All tiers	MANDATORY
Vendor provides and maintains updated technical documentation	Tier 2	MANDATORY
Vendor notifies you of any compliance status changes within 5 business days	Tier 2	MANDATORY
Vendor supports your right to audit or inspect AI systems	Tier 2	MANDATORY
Vendor notifies you of serious incidents affecting your deployment within 24 hours	Tier 2	MANDATORY
Vendor provides human oversight and override capabilities	Tier 2	MANDATORY
Vendor indemnifies you for fines arising from their non-compliance	Tier 2–3	RECOMMENDED
Vendor provides training materials and compliance documentation for your staff	All tiers	RECOMMENDED
Right to terminate if vendor falls out of EU AI Act compliance	All tiers	RECOMMENDED
Vendor maintains GDPR-compliant data processing under DPA	All tiers	MANDATORY
Vendor provides GDPR-compliant data processing addendum (DPA)	All tiers	MANDATORY
Service levels for incident response and remediation	Tier 2	RECOMMENDED

Table 5 — Required and recommended contract provisions for AI vendors.

Vendor Compliance Scoring Scorecard

Use this scorecard during procurement and annual vendor reviews. Score each vendor 0–3 per criterion. Total score guides procurement decision.

Assessment Area	0 — None	1 — Partial	2 — Good	3 — Excellent	Score
AI Act risk classification documented	No documentation	Claims compliance — no evidence	Classification with basic evidence	Full documented assessment	/3
Technical documentation available	None provided	Summary only	Partial Annex IV docs	Complete Article 11 docs	/3
Conformity assessment status	None / unknown	Self-assessment only	Completed self-assessment	Third-party notified body	/3
Human oversight built in	No override capability	Manual override only	Oversight + logging	Full oversight + audit trail	/3
Bias & accuracy testing evidence	None	Internal claims only	Test results on request	Published results + methodology	/3

Assessment Area	0 — None	1 — Partial	2 — Good	3 — Excellent	Score
Incident reporting process	None	Ad-hoc process	Defined process, limited SLA	Formal process, 24hr SLA, tested	/3
Data governance and GDPR compliance	No DPA / policies	Basic DPA available	DPA + data map	DPA + data map + audit rights	/3
AI governance maturity	No policy/owner	Basic policy only	Policy + designated owner	Governance committee + annual review	/3

Table 6 — Vendor Compliance Scorecard. Scoring guide: 20–24 = Strong; 14–19 = Acceptable with conditions; 8–13 = Requires improvement plan; 0–7 = Do not procure.

APPENDICES

Appendices

A — Penalty & Enforcement Summary

Violation Category	Maximum Fine	% of Global Turnover
Prohibited AI practices (Tier 1)	€35,000,000	7% — whichever is higher
High-risk system non-compliance (Tier 2)	€15,000,000	3% — whichever is higher
Providing false information to authorities	€7,500,000	1.5% — whichever is higher
SME / start-up (lower cap applies)	Lower of above	Or above %, whichever is lower

Table A.1 — EU AI Act penalty structure. Per Article 99.

Enforcement begins with national market surveillance authorities. The European AI Office handles GPAI model violations. Regulators can demand access to documentation, conduct audits, and impose interim measures including system suspension.

B — Key Definitions

Term	Definition
AI System	A machine-based system that infers from inputs how to generate outputs such as predictions, content, recommendations, or decisions that influence real or virtual environments.
Provider	Entity that develops or has an AI system developed and places it on the EU market or puts it into service.
Deployer	Entity that uses an AI system under its authority except for personal non-professional use.
High-Risk AI	AI system posing significant risks to health, safety, or fundamental rights, as listed in Annex III or embedded in regulated products (Annex I).
GPAI Model	General Purpose AI model trained with large amounts of data, capable of a wide range of tasks — includes large language models.
Conformity Assessment	Process by which a provider verifies a high-risk AI system meets mandatory requirements.
Technical Documentation	Documentation under Article 11 / Annex IV demonstrating a high-risk system's design, training, testing, and compliance.
Notified Body	Third-party conformity assessment body designated by an EU member state to assess certain high-risk AI systems.
Post-Market Monitoring	Ongoing process to collect and analyse data on high-risk AI performance after deployment.

Term	Definition
Serious Incident	Incident causing death, serious injury, significant property damage, or fundamental rights violations attributable to an AI system.

C — Useful Resources & References

Resource	Description	Source
Regulation (EU) 2024/1689	Full text of the EU AI Act	eur-lex.europa.eu
EU AI Office	Official EU AI Act guidance and enforcement body	digital-strategy.ec.europa.eu
AI Act Explorer	Interactive browser of AI Act obligations by role/risk	artificialintelligenceact.eu
NIST AI RMF	AI Risk Management Framework — useful companion standard	nist.gov/ai
ISO/IEC 42001	AI management system standard — maps to AI Act requirements	iso.org
ENISA AI Security Guidelines	Cybersecurity guidance for AI systems	enisa.europa.eu
ICO AI Auditing Framework	Practical AI audit methodology	ico.org.uk
BSI AI Act Readiness Tool	Self-assessment readiness tool	bsigroup.com

EU AI Compliance Institute | www.euaiaudit.eu | compliance@euaiaudit.eu

This checklist is provided for informational purposes only and does not constitute legal advice. Consult qualified legal counsel for compliance decisions specific to your organisation. Regulation (EU) 2024/1689 is the authoritative source of obligations.