EU AI ACT AUDIT Checklist 2026

A 3-Step Compliance Audit You Can Start This Week

- [x] Includes Vendor Compliance Checklist

Executive Summary

The **EU AI Act** is the **world's first comprehensive AI regulation** and introduces a risk-based framework governing the development, deployment, and use of artificial intelligence systems.

The Act applies not only to organizations established within the European Union but also to providers and deployers whose AI systems or outputs are used in the EU.

Organizations that wait until enforcement deadlines arrive may discover significant compliance gaps in governance, documentation, vendor management, and risk oversight.

This guide provides a practical three-step audit that organizations can begin immediately to assess readiness and identify compliance risks.

Why This Matters

The EU AI Act establishes obligations based on risk classification.

Organizations must first determine:

- Whether they are an **AI provider, deployer, importer, distributor, or authorized representative**.
- Whether their systems fall into prohibited, high-risk, limited-risk, or minimal-risk categories.
- Whether they are using **General-Purpose AI (GPAI)** models that carry additional obligations.

Without a complete inventory of AI systems and vendors, organizations cannot accurately determine their compliance obligations.

Source:

- EU AI Act, Articles 3, 6, 16, 26
- European Commission GPAI Obligations Guidance

Step 1: Audit Your AI Inventory

Objective

Identify every AI system currently developed, purchased, deployed, or used within the organization.

Many organizations cannot answer a simple question:

"Where is AI currently being used?"

Without this visibility, compliance is impossible.

Audit Questions

- ☐ Do we maintain a centralized inventory of AI systems?
- ☐ Have we identified all externally purchased AI solutions?
- ☐ Have we identified internally developed AI systems?
- ☐ Do we know which systems affect employees, customers, candidates, or citizens?
- ☐ Have we classified each system according to EU AI Act risk categories?
- ☐ Have we documented the purpose, owner, and business function of each system?

Evidence to Collect

- AI asset inventory
- Procurement records
- Vendor lists
- AI system register
- Data flow diagrams

Audit Outcome

By the end of Step 1, every AI system should have:

- Owner
- Business purpose
- Risk classification
- Vendor information
- Data sources

Step 2: Audit Governance & Risk Controls

Objective

Verify that governance mechanisms exist for AI oversight.

The EU AI Act places significant emphasis on:

- **Risk management**
- **Human oversight**
- **Documentation**
- **Record keeping**
- **Transparency**

For high-risk systems, providers must maintain risk management systems, documentation, logging mechanisms, and quality management processes.

Deployers must implement human oversight and maintain logs under their control.

Audit Questions

Governance

- ☐ Is there an assigned AI governance owner?
- ☐ Is AI oversight assigned to a committee or executive sponsor?
- ☐ Are AI policies documented and approved?

Human Oversight

- ☐ Can humans review, intervene, or override AI decisions?
- ☐ Is human oversight documented?
- ☐ Have responsible personnel received training?

Documentation

- ☐ Do we maintain documentation for AI systems?
- ☐ Are decisions, outputs, and changes logged?
- ☐ Can compliance evidence be produced during an audit?

Risk Management

- ☐ Are AI risks assessed before deployment?
- ☐ Are privacy, bias, cybersecurity, and operational risks evaluated?
- ☐ Is there a process for incident reporting?

Evidence to Collect

- AI governance policies
- Risk assessments
- Oversight procedures
- Audit logs
- Training records
- Incident management records

Audit Outcome

Every AI system should have:

- Documented ownership
- Defined oversight
- Risk assessment records
- Monitoring controls
- Audit trail capability

Step 3: Audit Vendor Compliance

Objective

Determine whether AI vendors can provide evidence necessary for compliance.

Many organizations assume compliance responsibilities belong entirely to the vendor.

The EU AI Act places obligations on both providers and deployers.

Organizations therefore need a structured vendor assessment process.

Vendor Compliance Checklist

Documentation

- ☐ Has the vendor provided technical documentation?
- ☐ Has the vendor documented intended use cases?
- ☐ Has the vendor documented system limitations?
- ☐ Can the vendor explain model behavior and outputs?

Risk Management

- ☐ Does the vendor maintain an AI risk management framework?
- ☐ Has the vendor conducted risk assessments?
- ☐ Are model updates governed by documented procedures?
- ☐ Does the vendor maintain incident reporting processes?

Security

- ☐ Does the vendor conduct cybersecurity testing?
- ☐ Are access controls documented?
- ☐ Is model monitoring implemented?
- ☐ Are vulnerabilities tracked and remediated?

Transparency

- ☐ Can the vendor explain training data sources?
- ☐ Are AI-generated outputs disclosed where required?
- ☐ Are users informed when interacting with AI?

Human Oversight

- ☐ Does the solution support human review?
- ☐ Can decisions be challenged or overridden?
- ☐ Are escalation procedures documented?

Compliance Readiness

- ☐ Can the vendor demonstrate alignment with the EU AI Act?
- ☐ Can the vendor provide audit evidence upon re
- ☐ Has the vendor designated compliance contacts?
- ☐ Are contractual compliance obligations defined?

Red Flags That Require Immediate Review

Organizations should escalate review if:

- No AI inventory exists.
- No AI governance owner has been assigned.
- AI decisions cannot be explained.
- Human oversight is absent.
- Vendor documentation is unavailable.
- AI outputs are not logged.
- Risk assessments have never been performed.
- High-risk use cases have not been identified.

Final Readiness Scorecard

AI Inventory

☐ Complete ☐ Partial ☐ Not Started

Governance

☐ Complete ☐ Partial ☐ Not Started

Risk Management

☐ Complete ☐ Partial ☐ Not Started

Documentation

☐ Complete ☐ Partial ☐ Not Started

Vendor Compliance

☐ Complete ☐ Partial ☐ Not Started

Human Oversight

☐ Complete ☐ Partial ☐ Not Started

Key Takeaway

The first organizations to succeed under the **EU AI Act** will not be those with the most **advanced AI systems**. They will be those with the **strongest governance**, **documentation**, **oversight**, and **risk management practices**.

A complete AI inventory, documented governance framework, and structured vendor review process are the most practical actions organizations can begin this week.

Sources

- European Union, Regulation (EU) 2024/1689 (EU AI Act), Articles 16, 26, and 27. (EU AI Act)
- European Commission — General-Purpose AI Obligations Guidance. Requirements include technical documentation, copyright policies, training-data summaries, risk mitigation, incident reporting, and cybersecurity obligations for GPAI providers. (Digital Strategy)
- National Institute of Standards and Technology (NIST) — AI Risk Management Framework (AI RMF 1.0). Provides a recognized framework for AI governance, risk identification, monitoring, and oversight. (NIST)
- European Commission draft guidance on classification of high-risk AI systems under the EU AI Act. (IT Pro)
- IBM Global CIO/CTO Survey (2026): only 11% of leaders feel fully prepared for large-scale AI deployment and 77% report current governance frameworks are inadequate. (IT Pro)