EU EU AI Act Compliance Guide

Practical guide to EU AI Act requirements for AI system providers and deployers | TeraSystemsAI Governance Toolkit

> **Legal Disclaimer:** This guide is designed to help teams understand EU AI Act process and documentation expectations. It does **not** constitute legal advice. Organizations should consult qualified legal counsel for regulatory compliance decisions.

Overview of the EU AI Act

The **EU Artificial Intelligence Act** (Regulation (EU) 2024/1689) is the world's first comprehensive legal framework for AI systems. It takes a risk-based approach, imposing different obligations depending on the level of risk an AI system poses to health, safety, and fundamental rights.

> **Key Principle:** The higher the risk posed by an AI system, the more stringent the regulatory requirements. The Act categorizes AI systems into four risk levels: Unacceptable, High, Limited, and Minimal.

Risk Classification Framework

Understanding which risk category your AI system falls into is the **first and most critical step** in determining compliance obligations.

Risk Level	Description	Examples	Compliance Requirement
UNACCEPTABLE RISK	AI systems that pose a clear threat to safety, livelihoods, or rights	• Social scoring by governments • Real-time biometric identification in public spaces (with exceptions) • Manipulation of behavior causing harm • Exploitation of vulnerabilities	**PROHIBITED**
HIGH RISK	AI systems used in critical areas affecting safety or fundamental rights	• Medical devices (diagnostics, treatment) • Critical infrastructure management • Employment decisions (hiring, termination) • Law enforcement applications • Credit scoring and loan decisioning • Educational assessment and admissions	**STRICT REQUIREMENTS** (Conformity assessment, documentation, monitoring)
LIMITED RISK	AI systems where transparency concerns exist	• Chatbots and conversational AI • Emotion recognition systems • Deepfake generators • Biometric categorization systems	**TRANSPARENCY OBLIGATIONS** (Disclosure to users that they interact with AI)
MINIMAL RISK	AI systems with low or no impact on rights and safety	• AI-powered spam filters • AI-enabled video games	**VOLUNTARY COMPLIANCE** (Best practices encouraged)

Risk Level	Description	Examples	Compliance Requirement
		• Recommendation systems (non-critical)	

Requirements for High-Risk AI Systems

Most organizations deploying AI in regulated or high-stakes environments will fall into the **High-Risk** category. The following sections outline key obligations.

1. Risk Management System (Article 9)

- ☐ Establish a continuous risk management process throughout the AI system lifecycle
- ☐ Identify and analyze known and reasonably foreseeable risks
- ☐ Estimate and evaluate risks that may emerge during use
- ☐ Adopt suitable risk management measures
- ☐ Test and document residual risks
- ☐ Update risk assessments based on post-market monitoring data

2. Data and Data Governance (Article 10)

- ☐ Ensure training, validation, and testing datasets are relevant, representative, and free from errors
- ☐ Take into account characteristics of the intended operational context
- ☐ Apply appropriate data governance and management practices
- ☐ Examine datasets for possible biases that could lead to discrimination

- ☐ Implement measures to detect, prevent, and mitigate bias
- ☐ Document data provenance and preprocessing steps

3. Technical Documentation (Article 11, Annex IV)

- ☐ General description of the AI system and its intended purpose
- ☐ Design specifications, architecture, and development process
- ☐ Detailed description of data requirements and data used
- ☐ Computational resources used for training and operation
- ☐ Testing and validation procedures, including metrics
- ☐ Risk management documentation
- ☐ Performance metrics and limitations
- ☐ Information about human oversight measures
- ☐ Cybersecurity measures
- ☐ Instructions for use

4. Record-Keeping and Logging (Article 12)

- ☐ AI systems must keep automatic logs of their operation
- ☐ Logs should enable traceability throughout the system lifecycle
- ☐ Record events relevant to identifying risks and non-conformity
- ☐ Ensure logs are protected against tampering and unauthorized access

- ☐ Retain logs for an appropriate period (minimum duration determined by risk level)

5. Transparency and User Information (Article 13)

- ☐ Provide clear, concise, and accessible instructions for use
- ☐ Specify the AI system's intended purpose and limitations
- ☐ Include information on expected accuracy, robustness, and cybersecurity
- ☐ Disclose known or foreseeable circumstances that may lead to risks
- ☐ Describe human oversight requirements and capabilities
- ☐ Document expected operational lifetime and maintenance needs

6. Human Oversight (Article 14)

- ☐ Design AI systems to enable effective human oversight
- ☐ Ensure humans can fully understand the system's capacities and limitations
- ☐ Enable humans to monitor the system's operation, including anomaly detection
- ☐ Provide mechanisms to intervene, interrupt, or override AI decisions
- ☐ Define roles, responsibilities, and training for oversight personnel

7. Accuracy, Robustness, and Cybersecurity (Article 15)

- ☐ Achieve appropriate levels of accuracy as stated in instructions for use
- ☐ Ensure robustness against errors, faults, and inconsistencies
- ☐ Implement measures to ensure resilience against attempts to alter use or performance

☐ Apply cybersecurity measures to protect against unauthorized access

☐ Test system behavior under adversarial conditions

Conformity Assessment Process

Conformity Assessment: High-risk AI systems must undergo a conformity assessment before they can be placed on the EU market or put into service. This can be done through internal assessment or third-party verification, depending on the risk level.

Conformity Assessment Pathways

Assessment Type	When Applicable	Process
Internal Control (Annex VI)	Most high-risk AI systems	• Provider conducts internal assessment • Prepares technical documentation • Establishes quality management system • Issues EU Declaration of Conformity • Affixes CE marking
Third-Party Assessment (Annex VII)	Specific high-risk categories (e.g., biometric systems, critical infrastructure)	• Notified Body reviews technical documentation • Audits quality management system • Issues conformity certificate • Provider issues EU Declaration of Conformity • Affixes CE marking

Steps for Conformity Assessment

1. **Classify your AI system** – Determine if it is high-risk based on Annex III criteria
2. **Establish a quality management system** – Document processes, risk management, and governance
3. **Prepare technical documentation** – Compile all required documentation per Annex IV
4. **Conduct risk assessment** – Identify, evaluate, and mitigate risks
5. **Implement data governance** – Ensure datasets meet quality and bias requirements
6. **Test and validate** – Demonstrate accuracy, robustness, and safety
7. **Set up human oversight** – Define oversight mechanisms and responsibilities
8. **Enable logging and traceability** – Implement automatic event recording
9. **Prepare instructions for use** – Provide clear, comprehensive user documentation
10. **Issue EU Declaration of Conformity** – Formally declare compliance
11. **Affix CE marking** – Apply the CE mark to indicate conformity
12. **Register in EU database** – Submit required information to EU AI system database

Implementation Timeline

August 1, 2024

Act Entry into Force
EU AI Act officially entered into force

February 2, 2025

Prohibited AI Practices
Ban on unacceptable risk AI systems takes effect (6 months after entry into force)

August 2, 2025

Codes of Practice & Governance
AI Office operational; codes of practice for general-purpose AI developed (12 months)

August 2, 2026

General-Purpose AI Obligations
Requirements for general-purpose AI models take effect (24 months)

> **August 2, 2027**
>
> **Full Application for High-Risk AI**
>
> **All high-risk AI system requirements fully apply (36 months)**

Compliance Readiness Checklist

> **Action Required:** Organizations deploying high-risk AI systems should begin compliance preparations **immediately** to meet the August 2027 deadline.

Phase 1: Assessment & Planning (Months 1-3)

- ☐ Inventory all AI systems in development and production
- ☐ Classify each system according to EU AI Act risk categories
- ☐ Identify gaps between current practices and EU AI Act requirements
- ☐ Assign roles and responsibilities for compliance
- ☐ Develop a compliance roadmap with milestones
- ☐ Allocate budget and resources for compliance activities

Phase 2: Documentation & Governance (Months 3-9)

- ☐ Establish a quality management system (QMS)
- ☐ Develop risk management processes and documentation
- ☐ Create technical documentation templates aligned with Annex IV
- ☐ Implement data governance policies and procedures

- ☐ Document model development, training, and validation processes
- ☐ Prepare instructions for use and user-facing documentation

Phase 3: Technical Implementation (Months 6-18)

- ☐ Implement logging and traceability mechanisms
- ☐ Develop or enhance human oversight capabilities
- ☐ Conduct bias assessments and implement mitigation measures
- ☐ Perform accuracy, robustness, and cybersecurity testing
- ☐ Set up post-market monitoring systems
- ☐ Establish incident reporting and response procedures

Phase 4: Conformity Assessment & Certification (Months 18-30)

- ☐ Engage a notified body (if third-party assessment required)
- ☐ Complete all technical documentation
- ☐ Finalize risk assessments and mitigation plans
- ☐ Conduct conformity assessment procedure
- ☐ Issue EU Declaration of Conformity
- ☐ Affix CE marking to AI systems

Phase 5: Registration & Ongoing Compliance (Months 30+)

- ☐ Register AI systems in EU AI database

- ☐ Implement continuous monitoring and reporting
- ☐ Conduct periodic reviews of risk assessments
- ☐ Update documentation as system evolves
- ☐ Train personnel on compliance obligations
- ☐ Prepare for regulatory audits and inspections

Key Compliance Pitfalls to Avoid

Common Mistake	Why It's Problematic	Recommended Action
Treating compliance as a one-time activity	EU AI Act requires ongoing monitoring, updates, and documentation throughout the lifecycle	Establish continuous compliance processes, not just pre-deployment checks
Inadequate technical documentation	Incomplete documentation can result in failed conformity assessments and regulatory penalties	Follow Annex IV requirements meticulously; use comprehensive templates
Ignoring data governance	Biased or unrepresentative datasets can lead to non-compliance and discrimination risks	Implement rigorous data quality, bias detection, and mitigation practices
Weak human oversight mechanisms	Lack of meaningful human control violates Article 14 and increases liability exposure	Design AI systems with built-in oversight capabilities; train oversight personnel
No post-market monitoring	Failing to monitor AI systems in production can miss performance degradation and emerging risks	Set up automated monitoring, alerting, and incident response workflows

Common Mistake	Why It's Problematic	Recommended Action
Waiting until 2027 to start	Compliance requires significant upfront work; last-minute efforts are high-risk and costly	Begin compliance activities now; aim to be ready 6-12 months before deadline

Additional Resources

- **Official EU AI Act Text:** Regulation (EU) 2024/1689 (available on EUR-Lex)
- **European Commission AI Office:** Official guidance and FAQs
- **AI Pact:** Voluntary commitments and best practices
- **Notified Bodies:** List of third-party conformity assessment organizations
- **TeraSystemsAI Governance Toolkit:** Additional templates and frameworks for compliance

---

TeraSystemsAI

This guide is provided as part of the AI Governance Toolkit.

For more resources, visit **terasystems.ai/governance-toolkit**