

What does Annex I of EU AI Act cover?



A

Section A:

Covers product safety directives and regulations requiring third-party conformity assessments (such as toys, lifts, medical devices, and machinery).

B

Section B:

Covers other Union harmonisation legislation addressing specific transport, marine, and civil aviation security frameworks.

Covered sectors and products in Annex I

- Machinery
- Toy safety
- Recreational craft
- Lift safety
- Explosive equipment
- Radio equipment
- Pressure equipment
- Cableway installations
- Protective equipment
- Gas appliances
- Medical devices
- In-vitro diagnostics
- Aviation security
- Two-wheel vehicles
- Agricultural vehicles
- Marine equipment
- Rail interoperability
- Motor vehicles
- Vehicle safety
- Civil aviation

What does Annex III of EU AI Act cover?

**Systems classified as
high-risk AI systems
under Article 6(2).**

**If an AI system
operates within these
designated areas, it
faces strict
compliance
obligations regarding
data governance,
documentation,
transparency, and
human oversight.**

Annex III

Covered areas

- **Remote biometric identification of individuals in public spaces for the targeted search of a person suspected or convicted of having committed a criminal offence**
- **Biometric categorisation using sensitive personal characteristics**
- **Emotion recognition systems for individuals**

- **AI managing critical infrastructure and utilities**
- **AI determining educational admissions and access**
- **AI evaluating students' learning outcomes**
- **AI assessing appropriate education level**
- **AI monitoring students during examinations**
- **AI supporting recruitment and candidate selection**

- **AI managing employment and workplace decisions**
- **AI determining eligibility for public benefits**
- **AI assessing creditworthiness and credit scores**
- **AI pricing life and health insurance risks**
- **AI prioritising emergency calls and dispatch**
- **AI assessing crime victimisation risk**

- **AI polygraphs supporting law enforcement investigations**
- **AI evaluating reliability of criminal evidence**
- **AI assessing offending or reoffending risks**
- **AI profiling individuals during criminal investigations**
- **AI assessing migration and security risks**

- **AI supporting asylum, visa and residence decisions**
- **AI identifying individuals at border control**
- **AI assisting judicial decision-making and dispute resolution**
- **AI influencing election outcomes or voting behaviour**

EU AI Act

Article 17

Quality Management System

**13 Requirements
for the QMS of high-risk AI**

Requirements 1–5

01 **Regulatory Compliance Strategy**

A strategy for regulatory compliance, including conformity with conformity assessment procedures and management of changes to the high-risk AI system.

02 **Design Control and Verification**

Techniques, procedures and systematic actions for design, design control and design verification of the high-risk AI system.

03 **Development and Quality Assurance**

Techniques, procedures and systematic actions for development, quality control and quality assurance of the high-risk AI system.

04 **Testing and Validation**

Procedures and systematic actions for testing, verification and validation of the high-risk AI system, including pre- and post-market activities.

05 **Technical Specifications**

Data and data governance, including data collection, analysis, labelling, storage, filtration, mining, aggregation, retention and any other operation regarding the data.

Requirements 6–9

06

Data Management

The risk management system referred to in Article 9.

07

Risk Management

The setting-up, implementation and maintenance of a post-market monitoring system, in accordance with Article 72.

08

Post-Market Monitoring

Procedures related to the reporting of a serious incident in accordance with Article 73.

09

Incident Reporting

Communication with national competent authorities, other relevant authorities, including those providing or supporting access to data, notified bodies, other operators, customers or other interested parties.

Requirements 10–13

10 Stakeholder Communication

Systems and procedures for record-keeping of all relevant documentation and information.

11 Record-Keeping

Resource management, including security-of-supply related measures.

12 Resource Management

An accountability framework setting out the responsibilities of the management and other staff with regard to all the aspects listed in this paragraph.

13 Accountability Framework

Clear assignment of responsibilities and accountabilities across the organisation.

**Don't miss out on
the latest
updates on AI,
technology and
compliance**

**Follow me on
LinkedIn!**