AI
ARTIFICIAL
INTELLIGENCE

EXCELLENCE
& TRUST

DG CNECT, European Commission

Risk management logic of the AI Act and related standards
30 May 2024

EUROPEAN ARTIFICIAL INTELLIGENCE OFFICE

Agenda

1. Opening remarks

2. AI Act’s risk management and QMS logic

3 Analysis of the AI standardisation landscape from the lens of the AI Act

4. Q&A

AI
ARTIFICIAL
INTELLIGENCE

EXCELLENCE
& TRUST

AI Act’s risk management and QMS logic

Dr. Tatjana Evas, DG CNECT, European Commission

EUROPEAN ARTIFICIAL
INTELLIGENCE OFFICE

The AI Act – the main principles

Enhanced Product regulation: risks to health, safety and fundamental rights

AI system and risks that may be generated by an AI system – is the focus of the requirements for high risk

Risk-based and lifecycle approach: regulate according to risk, pre and post-market monitoring

Trust across entire value chain: rules for AI systems and GPAI models

Responsible innovation: encourage the development of trustworthy and human-centric AI

Harmonized rules across EU – Ensuring trustworthy AI

Consistent legal framework in 27 EU Member States

1. The AI Act – the legislative rationale and logic

- The **purpose of the AIA** is set out in **Article 1** →

  "ensuring **a high level of protection of health, safety, fundamental rights** enshrined in the Charter of FR, including democracy, the rule of law and environmental protection, **against the harmful effects of the AI systems** in the Union"

- **Product legislation logic → focus on trustworthiness of an AI system**

  *(recital 47) Consistent with the objectives of Union harmonisation legislation to facilitate the free movement of products in the internal market and to ensure that **only safe and otherwise compliant products find their way into the market, it is important that the safety risks that may be generated by a product as a whole due to its digital components, including AI systems, are duly prevented and mitigated.***

- **AI Act is a part of the New Legislative Framework (NLF)** system

  *(recital 9) The harmonised rules laid down in this Regulation should apply across sectors and**, in line with the New Legislative Framework**, should be without prejudice to existing Union law, in particular on data protection, consumer protection, fundamental rights, employment, and protection of workers, and product safety, to which this Regulation is complementary.*

2. New Legislative Framework – key concepts

- **NLF building blocks**

  Regulation (EC) 765/2008; Decision 768/2008; Regulation (EU) 2019/1020 + The Blue Guide

- **NLF = 26 EU legal act**

  (e.g. Machinery Regulation, Medical Device Regulation, Toys Safety)

- **The key elements of the NLF**

  - shared key definitions, procedures and the structure (to enhance consistency and ease applicability) for placing a product on the market, conformity assessment, CE marking and market surveillance

  - legislation focuses on

    → **public protection objectives** of the product concerned and outlines **basic safety characteristics**

    → **essential requirements** → operationalized through **technical standards**

    → **EU product 'quality chain'** – meaning that the quality of the product must be ensure by all actors in the lifecycle of the product, where quality means – ability of a product to meet the level of safety and other policy objectives aimed by the Union legislation.

3. New Legislative Framework – The Blue Guide

The Blue guide *(para 1.2.3)*

The evolution of EU legislative techniques in this area has been progressive, tackling issues one after another, although sometimes in parallel, culminating in the adoption of **the New Legislative Framework: essential or other legal requirements, product standards, standards and rules for the competence of conformity assessment bodies as well as for accreditation, standards for quality management, conformity assessment procedures, CE marking, accreditation policy, and lately market surveillance policy including the control of products from third countrie**s.

The New Legislative Framework now constitutes a complete system bringing together all the different elements that need to be dealt with in product safety legislation in a coherent, comprehensive legislative instrument that can be used across the board in all industrial sectors, and even beyond (environmental and health policies also have recourse to a number of these elements), whenever EU legislation is required.
In this system, the legislation has to set the levels of public protection objectives of the products concerned as well as the basic safety characteristics, it should set the obligations and requirements for economic operators, it has to set-where necessary-the level of competence of the third party conformity assessment bodies who assess products or quality management systems, as well as the control mechanisms for these bodies (notification and accreditation), it must determine which are the appropriate conformity assessment processes (modules which also include the manufacturer's Declaration of Conformity) to be applied, and finally it must impose the appropriate market surveillance mechanisms (internal and external) to ensure that the whole legislative instrument operates in an effective and seamless manner.

All these different elements are interlinked, operate together and are complementary, forming an EU quality (20) chain. The quality of the product depends on the quality of the manufacturing, which in many instances is influenced by the quality of testing, internal or carried out by external bodies, which depends on the quality of the conformity assessment processes, which depends on the quality of the bodies which in turn depends on the quality of their controls, which depends on the quality of notification or accreditation; the entire system depending on the quality of market surveillance and controls of products from third countries.
The word « quality » is used to designate the level of safety and other public policy objectives which are aimed by the Union harmonisation legislation.

4. The AIA - The Risk-Based Approach

General-purpose AI models

Transparency rules
for all models

Risk management
in case of systemic risk

AI systems – risk classification

Unacceptable risk e.g. social scoring	**Prohibited**
High risk e.g. recruitment, medical devices	**Permitted** subject to requirements, conformity assessment
'Transparency' risk e.g. chatbots, deep fakes	**Permitted** subject to information/transparency obligations
Minimal or no risk	**Permitted** with no restrictions

Mandatory Requirements for all high-risk AI system before they can be used and strong system of enforcement and post-market monitoring

8

5. Key definitions

'risk' means the combination of the probability of an occurrence of harm and the severity of that harm;

This definition aligns with the definition of risk in other NLF legislation and e.g. with Safety Risk Management per ISO Guide 51.

This stands in contrast to other definitions of risk such as "the effect of uncertainty on an expected result", meaning a (positive or negative) deviation from the expected

(not defined in the AIA, but standard in the NLF legislation)

Harm – injury or damage
Hazard - potential source of harm

6. Type of Risks Covered

Type of risks covered in the AI Act

Providers will have to covered **health and safety risks** as well as **risks to fundamental rights**, including

Article 10.2 (f) "biases that are likely to affect the health and safety of persons, have a negative impact on fundamental rights or lead to discrimination prohibited under Union law, especially where data outputs influence inputs for future operations"

Article 9.9 adverse impacts on persons under the age of 18 and, other vulnerable groups

Article 14.4 (b) Automation bias (e.g. users automatically relying or over-relying on the output produced by the AI)

Article 15.4 for systems that continue to learn "the risk of possibly biased outputs influencing input for future operations (feedback loops), and as to ensure that any such feedback loops are duly addressed with appropriate mitigation measures"

Article 15.5 Cybersecurity risks specific to AI systems

7. The Legal Basis

Main legal basis for **high-risk AI systems**

for RMS: **Article 1 + Article 8 + Article 9 (+ relevant recitals)**

for QMS: **Article 1, Article 16, Article 17, Annex VII (+ relevant recitals**)

+

Legal rules (unless provided otherwise) included in the Regulation (EC) No 765/2008, Decision No 768/2008/EC and Regulation (EU) 2019/1020 (New Legislative Framework) and interpretative guidelines adopted, including Commission notice The 'Blue Guide' on the implementation of EU product rules 2022 (Text with EEA relevance) 2022/C 247/01

RMS + QMS are mandatory for all high-risk AI systems!

8. RMS for high-risk AI systems

Article 8: Compliance with the requirements

1. High-risk AI systems shall comply with the requirements laid down in this Section, taking into account their intended purpose as well as the generally acknowledged state of the art on AI and AI-related technologies. The risk management system referred to in Article 9 shall be taken into account when ensuring compliance with those requirements.

9. RMS for high-risk AI systems

Article 9 Risk management system - logic

Comprehensive system – continuous and covering all stages of the lifecycle + obligatory testing + adjusted based on data from post-market monitoring

- Obligation to set, implement, **document** and maintain RMS (para 1)

- Concept of the RMS → **continuous process run through entire lifecycle, comprising the following steps (para 2)**
  - identification and analysis of the known and the reasonably foreseeable risks that the high-risk AI system can pose to health, safety or fundamental rights
  - estimation and evaluation of risks,
  - evaluation of risks including based on the data from post-market monitoring
  - adoption of **appropriate and targeted risk management measures**

10. RMS for high-risk AI systems

Article 9 Risk management system - identification of the most appropriate risk management measures (para 5)

[risk control] In identifying the most appropriate risk management measures, the following shall be ensured:

(a) [safety by design] elimination or reduction of risks identified and evaluated pursuant to paragraph 2 in as far as technically feasible through **adequate design and development of the high-risk AI system**;

(b) [protective measures] where appropriate, **implementation of adequate mitigation and control measures** addressing risks that cannot be eliminated;

(c) [information for safety] provision of information required pursuant to Article 13 and, where appropriate, training to deployers.

11. RMS for high-risk AI systems

Article 9 Risk management system – Testing! (paras 6, 7 and 8)

[testing is a key for identification of the appropriate risk management measures and compliance for all the requirements (Article 8 – 15) applicable to high-risk AI systems]

6. High-risk AI systems **shall be tested for the purpose of identifying the most appropriate and targeted risk management measures**. Testing shall ensure that high-risk AI systems perform consistently for their intended purpose and that they are in **compliance with the requirements set out in this Section**.

8. The testing of high-risk AI systems shall be performed, as appropriate, at any time throughout the development process, and, in any event, prior to their being placed on the market or put into service. **Testing shall be carried out against prior defined metrics and probabilistic thresholds that are appropriate to the intended purpose of the high-risk AI system.**

12. RMS for high-risk AI systems

Article 9 Risk management system – risks covered (para 9)

in implementing the RMS – focus on risks to health, safety and fundamental rights, in particular impact on persons under the age of 18 and, as appropriate, other vulnerable groups.

> 9. When implementing the risk management system as provided for in paragraphs 1 to 7, providers shall give consideration to whether in view of its intended purpose the high-risk AI system is likely to have an adverse impact on persons under the age of 18 and, as appropriate, other vulnerable groups.

13. RMS for high-risk AI systems

Article 9 Risk management system – Principle of complementarity (para 10)

- For providers of high-risk AI systems that are subject to requirements regarding internal risk management processes under other relevant provisions of Union law, the aspects provided in paragraphs 1 to 9 may be part of, or combined with, the risk management procedures established pursuant to that law.

14. QMS – main elements

The word « quality » is used to designate the level of safety and other public policy objectives which are aimed by the Union harmonisation legislation. (The Blue Guide)

Article 17 - QMS is mandatory for high-risk AI systems

- QMS – must ensure compliance with the AI Act and should be documented in the form of written polices, procedures and instructions

- Covers lifecycle of the AI systems, at least following elements must be included

  Pre-market: strategy for regulatory compliance; design control and verification; examination, test and validation of AI system; technical specifications

  Post-Market: quality control; reporting of serious incidents; post-market monitoring system

  Continuously: data management systems and procedures; RMS; communication with authorities; document and record keeping, including logging; resource management (including security of supply); accountability framework

  + For systems that continue to learn (Annex IV (2f) ‘ technical solutions adopted to ensure continuous compliance’

15. QMS - Conclusions

QMS is mandatory and must ensure compliance with AI Act

QMS must be documented

QMS covers,
- Quality during design and development of AI system
- Quality in the post market stages
- For continuously learning systems – technical solutions adopted to ensure continuous compliance of the AI system with the requirements set (Art. 8 – 15)

AI
ARTIFICIAL
INTELLIGENCE

EXCELLENCE
& TRUST

Analysis of the AI standardisation landscape from the lens of the AI Act

Josep Soler Garrido, Joint Research Centre, European Commission

EUROPEAN ARTIFICIAL INTELLIGENCE OFFICE

AI standards for the AI Act

- AI: a very active area of standardisation
- The European Commission issued a standardisation request to support AI Act
- International standards address various aspects of AI, relevant for AI Act
- However, current coverage is partial and often not aligned with the regulation
- Additional standards are required to cover essential gaps

Practical example: AI risk and quality management

- ISO/IEC standards recently published
- Detailed analysis from the lens of AI Act shows key areas of misalignment, such as:
  - Objectives and terminology, such as risk definition
  - Focus on organisational aspects – limited product orientation
  - Focus on guidance – limited requirements
  - Gaps in technical coverage of various AI Act requirements

ISO/IEC 23894:2023

Information technology

Artificial Intelligence

Guidance on risk management

ISO/IEC 42001:2023

Information technology

Artificial Intelligence

Management System

Qualities of harmonised AI standards

- Tailored to the risks addressed by the AI Act
- AI system- and product-oriented
- Sufficiently prescriptive & with clear requirements
- Applicable across sectors and types of AI system
- Aligned with the state of the art of Artificial Intelligence
- Cover all trustworthiness requirements and their interplay

References

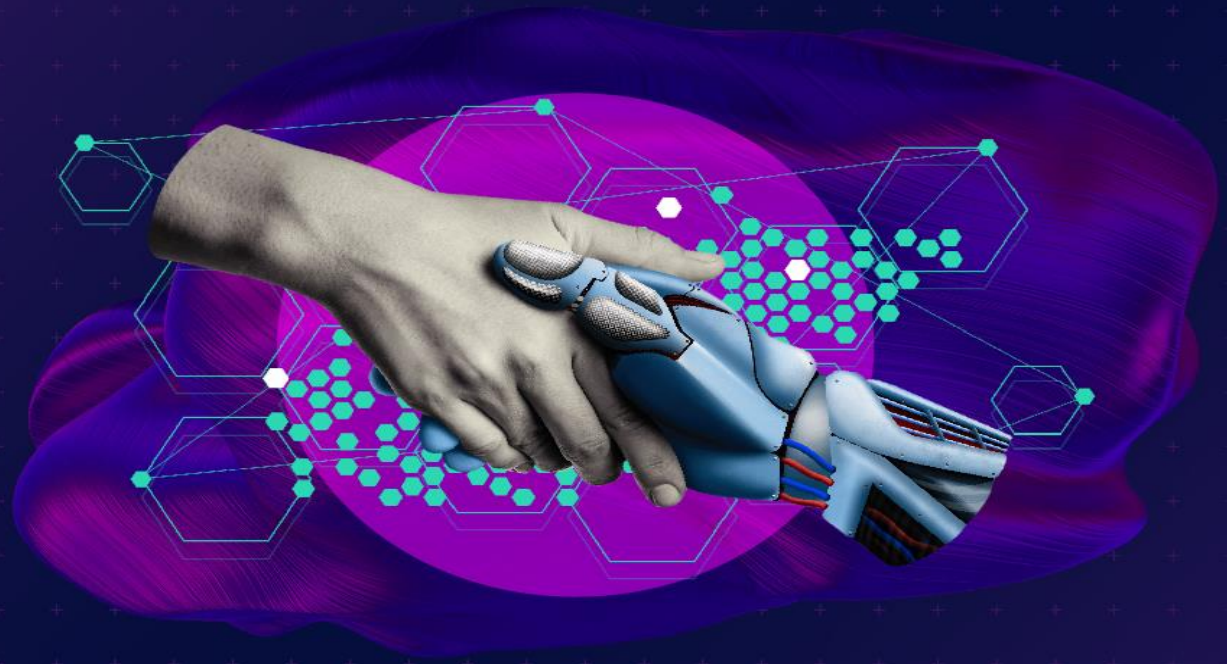
- **Analysis of the preliminary AI standardisation work plan in support of the AI Act**
  Publications Office of the European Union
  https://publications.jrc.ec.europa.eu/repository/handle/JRC132833

- **Cybersecurity of artificial intelligence in the AI Act**
  Publications Office of the European Union
  https://publications.jrc.ec.europa.eu/repository/handle/JRC134461

- **AI Watch: Artificial Intelligence Standardisation Landscape Update**
  Publications Office of the European Union
  https://publications.jrc.ec.europa.eu/repository/handle/JRC131155

- **The role of explainable AI in the context of the AI Act**
  2023 ACM Conference on Fairness, Accountability and Transparency
  https://dl.acm.org/doi/pdf/10.1145/3593013.3594069

- **Documenting High-Risk AI: A European Regulatory Perspective**
  IEEE Computer Magazine, May 2023
  https://ieeexplore.ieee.org/document/10109295



EUROPEAN AI OFFICE

THE CENTRE OF AI EXPERTISE IN EUROPE

#DigitalEU