Luxembourg House of Cybersecurity

Dr. Emilia Tantar

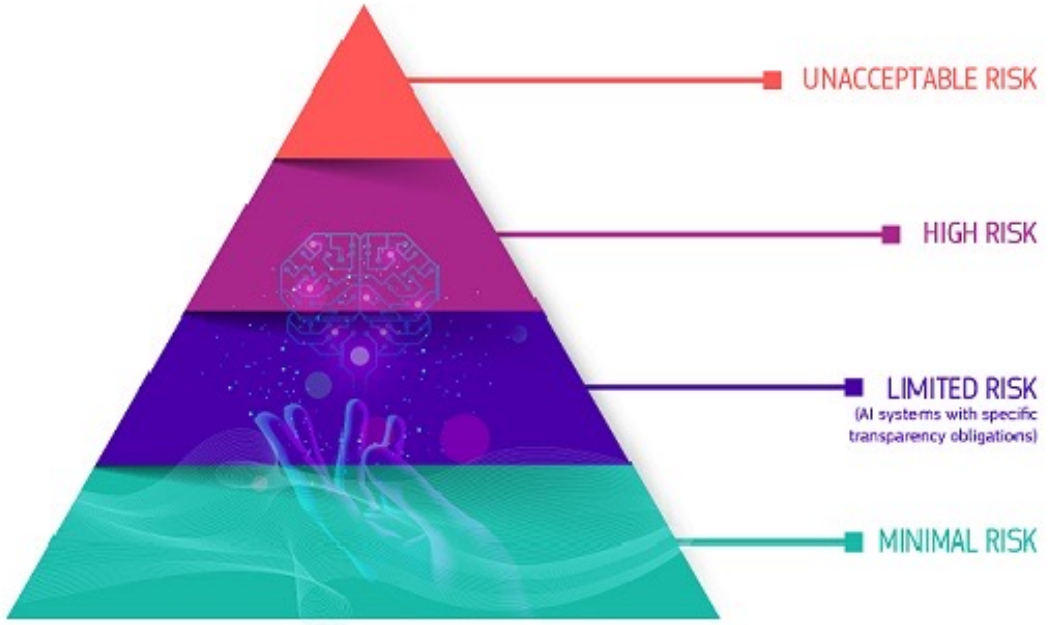
Chief AI Officer and Head of Departmernt Cybersecurity Factory
Luxembourg House of Cybersecurity
Convenor WG2 Operational aspects in CEN/CLC JTC 21
President and Head of Delegation of Luxembourg NMC AI

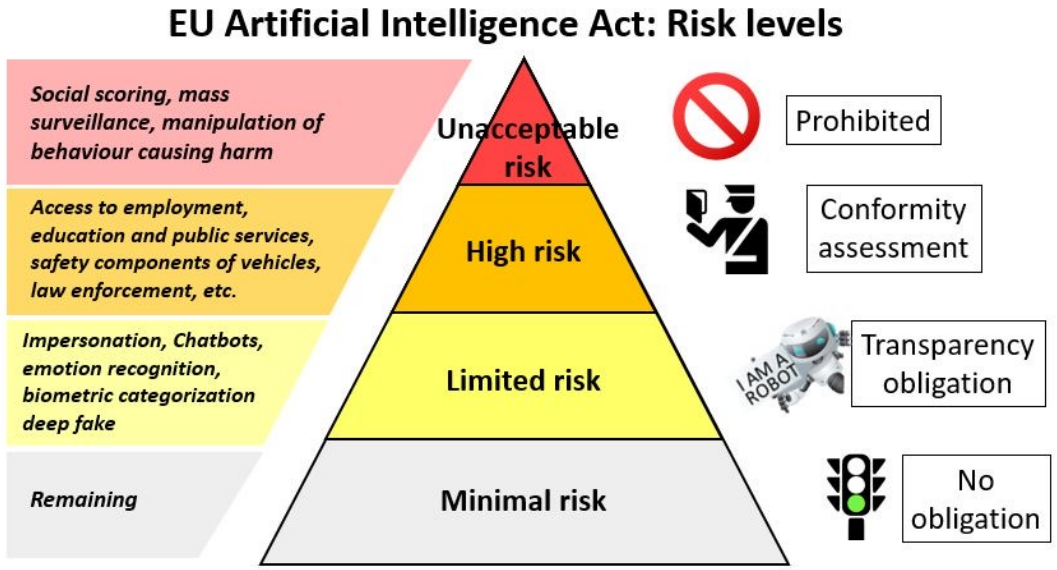
# *Conformity Assessment for High-Risk AI system providers*

# STATEMENT OF PURPOSE

Luxembourg House of Cybersecurity

*The purpose of the herein document is to offer a high-level view on aspects within AI standardisation and EU AI legislative framework [compiling a number of normative documents and articles on AI], with a main focus on societal and business-related implications. The presentation is intended for dissemination within the limits of the* **Driving Trustworthy AI through Design and Regulation** *participants. Where applicable, [public domain] external materials are credited, and links are provided to allow referring to the respective originating works.*




# EU AI Act regulation – a risk based approach

Sources:

https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

https://www.telefonica.com/en/communication-room/blog/a-fit-for-purpose-and-borderless-european-artificial-intelligence-regulation/

Assess the risk class of your AI system according to the AI Act:
https://ai-act-service-desk.ec.europa.eu/en/eu-ai-act-compliance-checker

Luxembourg House of Cybersecurity

# What are the obligations?
## *Obligations of providers*

| | High-risk AI system | Limited-risk AI system | Minimal-risk AI system | Systemic-risk GPAI model |
|---|---|---|---|---|
| AI Literacy | Art. 4 | Art. 4 | Art. 4 | Art. 4 |
| Transparency and provision of information | Art. 13 | Art. 50(1), (2) | | Art. 53(1)b |
| Data and data gouvernance | Art. 10 | | | Art. 53(1)c, d |
| Technical documentation | Art. 11 | | | Art. 53(1)a |
| Cooperation with competent authorities | Art. 21 | | | Art. 53(3) |
| Risk management | Art. 9 | | | Art. 55(1)a, b |
| Accuracy, robustess, cybersecurity | Art. 15 | | | Art. 55(1)d |
| Registration | Art. 49 | | | Art. 52(1) |
| Reporting of serious incidents | Art. 73 | | | Art. 55(1)c |
| Record keeping | Art. 12 | | | |
| Human oversight | Art. 14 | | | |
| Labeling | Art. 16(b) | | | |
| Accessability | Art. 16(l) | | | |
| Quality Management System | Art. 17 | | | |
| Documentation keeping | Art. 18, 19 | | | |
| Correctives measures | Art, 20 | | | |
| Conformity assessment and declaration | Art. 43, 47, 48 | | | |

# Obligations for providers (various layers)

| | High-risk AI systems | Limited risk AI systems | Minimal risk AI systems | Systemic risk GPAI model |
|---|---|---|---|---|
| **AI Literacy** | Art. 4 | Art. 4 | Art. 4 | Art. 4 |
| Risk management | Art. 9 | | | Art. 55(1)a, b |
| Data quality and data governance | Art. 10 | | | Art. 53(1)c, d |
| Technical documentation | Art. 11 | | | Art. 53(1)a |
| Record keeping/logging | Art.12 | | | |
| Transparency and provision of information | Art. 13 | Art. 50(1), (2) | | Art. 53(1)b |
| Human oversight | Art. 14 | | | |
| Accuracy, robustness, cbyersecurity | Art. 15 | | | Art. 55(1)d |
| Labeling | Art. 16(b) | | | |
| Accessibility | Art. 16 (l) | | | |
| Quality management system | Art. 17 | | | |
| Documentation keeping | Art. 18, 19 | | | |
| Correctives measures | Art. 20 | | | |
| Cooperation with competent authorities | Art. 21 | | | Art. 53(3) |
| Conformity assessment and declaration | Art. 43, 47 and 48 | | | |
| Registration | Art. 49 | | | Art. 52(1) |
| Reporting of serious incidents | Art. 73 | | | Art. 55(1)c |

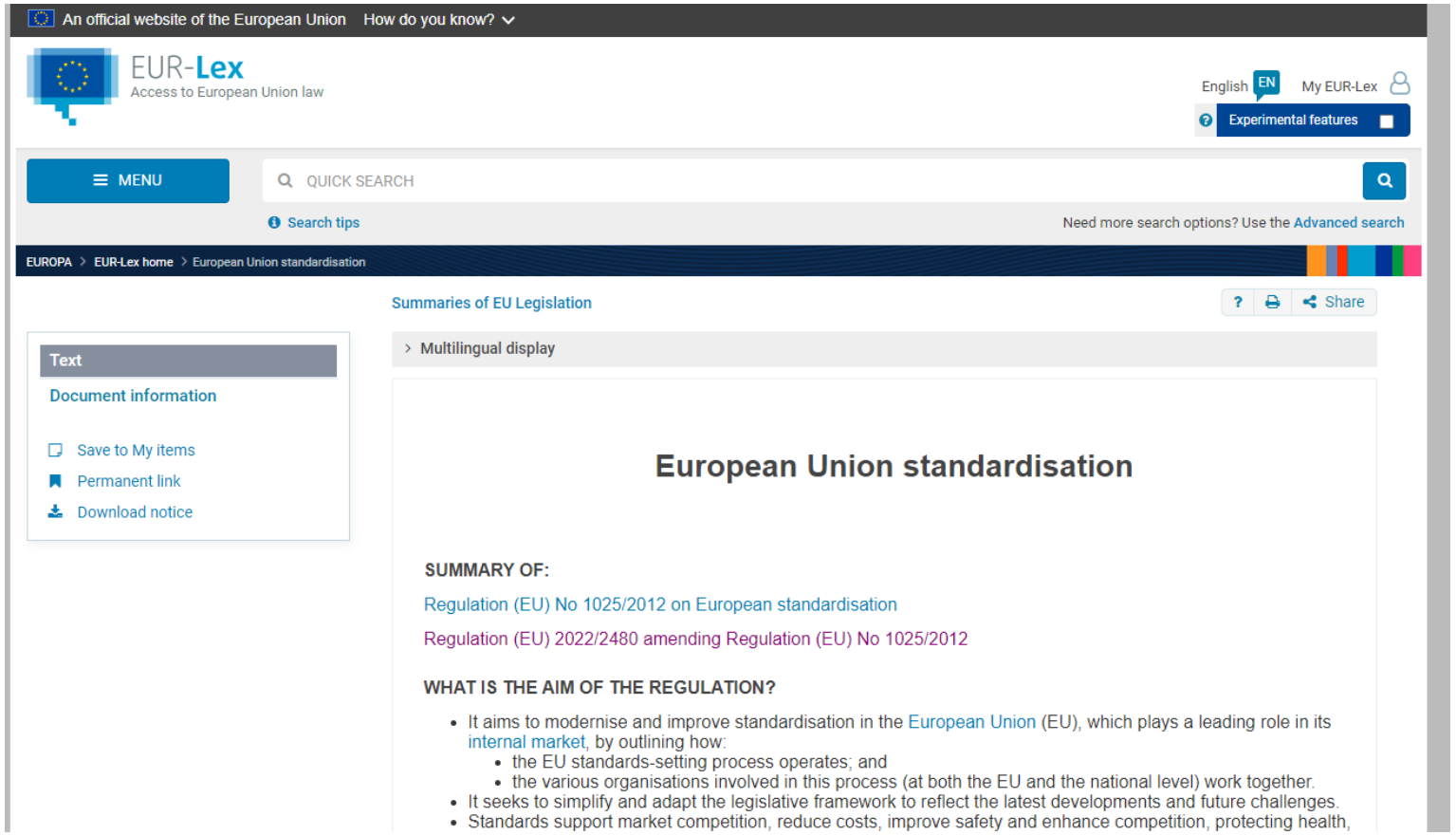
Luxembourg House of Cybersecurity

# What are the obligations?
## *Obligations of deployers*

| | High-risk AI system | Limited-risk AI system | Minimal-risk AI system |
|---|---|---|---|
| AI Literacy | Art. 4 | Art. 4 | Art. 4 |
| Transparency and provision of information | Art. 26(11) | Art. 50(3), (4) | |
| Use of the SIA according to the instructions for use | Art. 26(1), (3) | | |
| Human oversight | Art. 26(2) | | |
| Monitoring | Art. 26(5) | | |
| Reporting of serious incidents | Art. 26(5), 73(2) | | |
| Record keeping | Art. 26(6) | | |
| Cooperation with competent authorities | Art. 26(12) | | |
| Explanation of individual decision-making | Art. 86(1) | | |
| *Impact analysis* | Art. 26(9), 27 | | |
| *Registration obligations* | Art. 26(8) | | |
| *Employees information* | Art. 18, 19 | | |

# Standards and the Role of European standardization organisations

**Definition of a standard :**
A technical specification, adopted by a recognized standardization body, for repeated or continuous application, with which compliance is not compulsory.




Source: Regulation (EU) No 1025/2012 (revised in 2015) https://eur-lex.europa.eu/EN/legal-content/summary/european-union-standardisation.html#:~:text=It%20seeks%20to%20simplify%20and,safety%2C%20security%20and%20the%20environment

Luxembourg House of Cybersecurity

(4) European standards are adopted by the European standardisation organisations, namely CEN, Cenelec and ETSI.

(5) European standards play a very important role within the internal market, for instance through the use of harmonised standards in the presumption of conformity of products to be made available on the market with the essential requirements relating to those products laid down in the relevant Union harmonisation legislation. Those requirements should be precisely defined in order to avoid misinterpretation on the part of the European standardisation organisations.

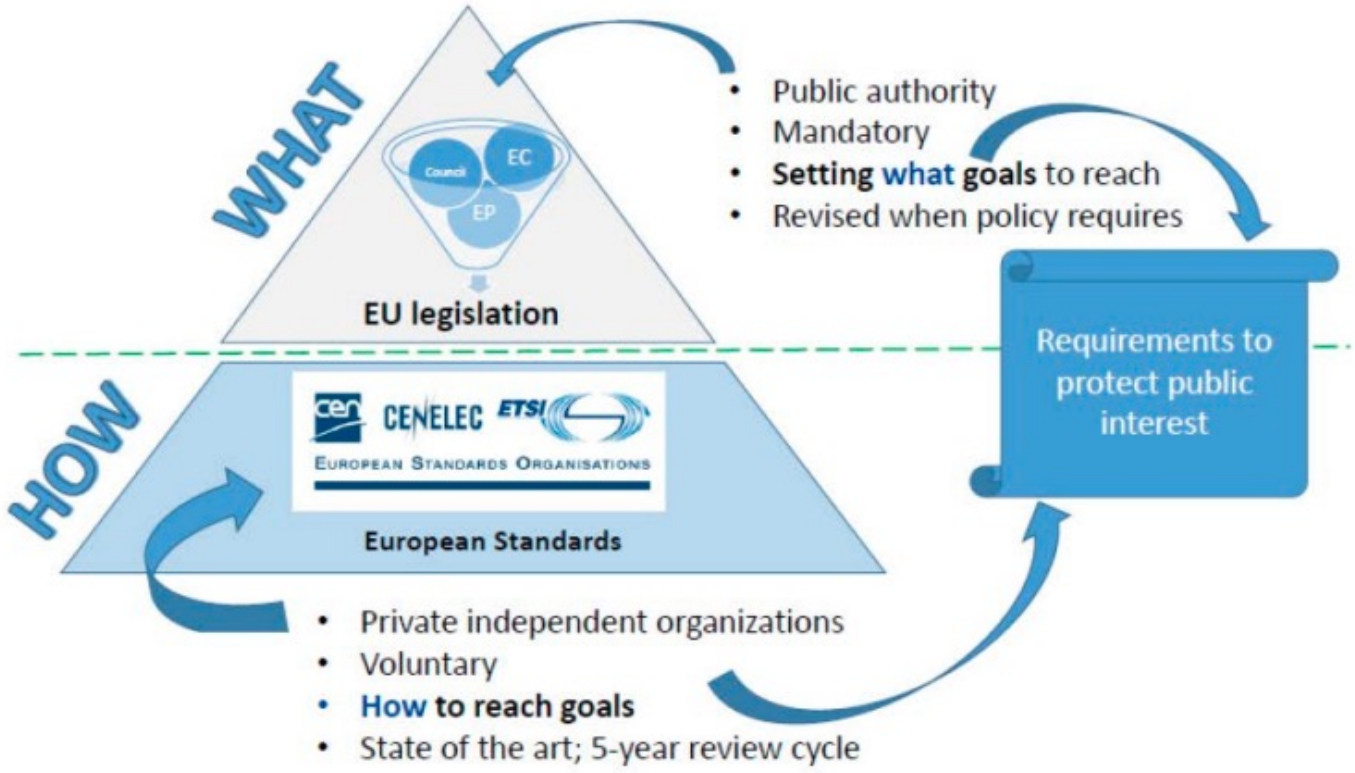
(6) Standardisation plays an increasingly important role in international trade and the opening-up of markets. The Union should seek to promote cooperation between European standardisation organisations and international standardisation bodies. The Union should also promote bilateral approaches with third countries to coordinate standardisation efforts and promote European standards, for instance when negotiating agreements or by seconding standardisation experts to third countries. Furthermore the Union should encourage contact between European standardisation organisations and private forums and consortia, while maintaining the primacy of European standardisation.

# Empowered by the European Publications Office

Source:

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32012R1025

# ENs in support of EU legislation



# Standards versus Legislation

## Standards

- Voluntary
- Consensual
- Developed by independent organizations
- Revised every 5 years
- Provide specifications and test methods (interoperability, safety, quality, etc.)

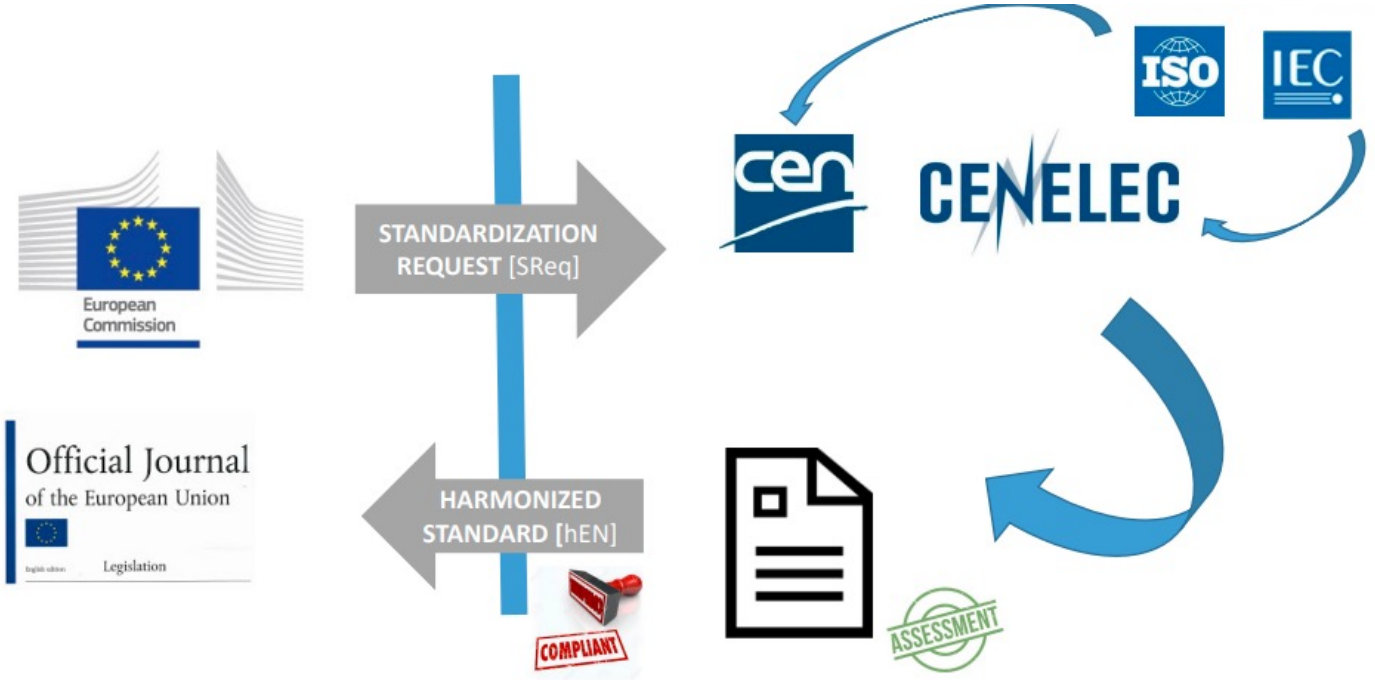
## Legislation

- Mandatory
- Imposed by Law
- Established by public authorities
- Revised when legislators decide
- Sets requirements to protect public interests

Luxembourg House of Cybersecurity

# How harmonized standards support legislation

Process defined in Regulation (EU) 1025/2012, amended by Regulation (EU) 2022/2480




> 3000 harmonized Standards listed in the OJEU

Luxembourg House of Cybersecurity

# EU AI systems requirements from the European Commission C(2023)3215 – Standardisation request M/593 to CEN and CLC JTC 21

https://ec.europa.eu/transparency/documents-register/detail?ref=C(2023)3215&lang=en

| Reference information | | Deadline for the adoption by CEN and CENELEC |
|---|---|---|
| 1. | European standard(s) and/or European standardisation deliverable(s) on risk management system for AI systems | 31/01/2025 |
| 2. | European standard(s) and/or European standardisation deliverable(s) on governance and quality of datasets used to build AI systems | 31/01/2025 |
| 3. | European standard(s) and/or European standardisation deliverable(s) on record keeping through logging capabilities by AI systems | 31/01/2025 |
| 4. | European standard(s) and/or European standardisation deliverable(s) on transparency and information provisions to the users of AI systems | 31/01/2025 |
| 5. | European standard(s) and/or European standardisation deliverable(s) on human oversight of AI systems | 31/01/2025 |
| 6. | European standard(s) and/or European standardisation deliverable(s) on accuracy specifications for AI systems | 31/01/2025 |
| 7. | European standard(s) and/or European standardisation deliverable(s) on robustness specifications for AI systems | 31/01/2025 |
| 8. | European standard(s) and/or European standardisation deliverable(s) on cybersecurity specifications for AI systems | 31/01/2025 |
| 9. | European standard(s) and/or European standardisation deliverable(s) on quality management system for providers of AI systems, including post-market monitoring process | 31/01/2025 |
| 10. | European standard(s) and/or European standardisation deliverable(s) on conformity assessment for AI systems | 31/01/2025 |

Black Swan LUX

Luxembourg House of Cybersecurity

# Maping of hEN candidate standards to EU AI Act articles

| Standardisation Request | AI Act* | Primary project*** | Supporting normative references** | |
|---|---|---|---|---|
| SR 1 – Risk | Art 9 - Risk | AI Risk Management | | |
| SR 2 - Data | Art 10 - Data | Quality and governance of datasets in AI | | |
| | | Concepts, measures and requirements for managing bias in AI systems | | |
| SR ALL - Docs | | | | |
| SR 3 - Records | Art 12 - Records | AI trustworthiness framework | ISO/IEC 12791 | ISO/IEC WD 4213 |
| SR 4 - Transparency | Art 13 - Transparency | | ISO/IEC WD 23281 | ISO/IEC FDIS 9868 |
| SR 5 - Oversight | Art 14 - Oversight | | ISO/IEC WD 23282 | ISO/IEC 29119-x |
| SR 6 - Accuracy | Art 15 – Accuracy, Robustness, Cybersecurity | | ISO/IEC FDIS 12792 | ISO/IEC 24029-x |
| SR 7 - Robustness | | | ISO/IEC WD 24970 | Computer Vision |
| SR 8 - Cyber | | Cybersecurity specifications for AI Systems | | |
| SR 9 – Quality MS | Art 17 – Quality MS | Quality management system for EU AI Act regulatory purposes | ISO/IEC 42001 | |
| | Art 72 - Monitoring | | | |
| SR 10 – Conformity | Art 72 - Monitoring | AI Conformity assessment framework | ISO/IEC 17000 | |

Black Swan LUX

Luxembourg House of Cybersecurity

# Compliance framework
# Resulting obligations

Luxembourg House of Cybersecurity

# 1. What is Conformity Assessment?

Conformity assessment ensures that products, services, or processes meet defined standards or regulations.

01

Verification that a product/service/process meets defined standards (e.g., ISO, IEC).

02

•Involves Testing, Inspection, Certification, and Surveillance.

Current process: human led. Potential for AI conformity assessment: HMT used throughout the activities.

03

Ensures safety, quality, compliance with regulations.

# Conformity assessment considerations

Identification of purpose and scope of the scheme

**Object of conformity assessment:**

- Product
- Service
- Process
- System
- **Person**
- Management system
- Body
- Organisation

## Conformity assessment can be conducted by:

**1st party:** a manufacturer or supplier, the person or organization that provides the object

**2nd party:** a user or purchaser

**3rd party**: an independent body, a person or body that is independent of the person or body that provides the object.

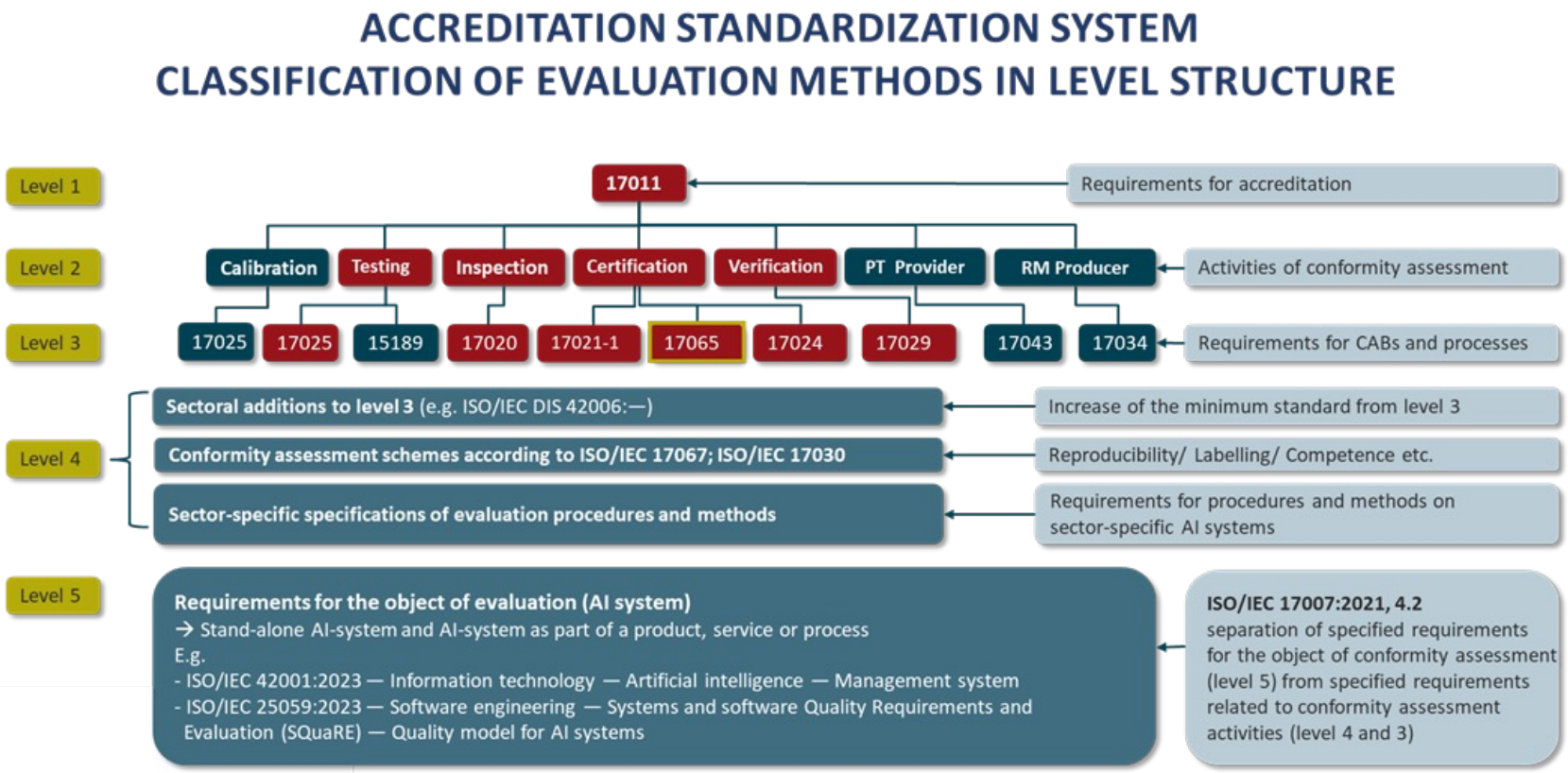
Schemes should be developed in accordance with ISO/IEC 17067:2013, Conformity assessment -Fundamentals of product certification and guidelines for product certification schemes.

Conformity assessment schemes can be setup as voluntary (“self-regulation”)

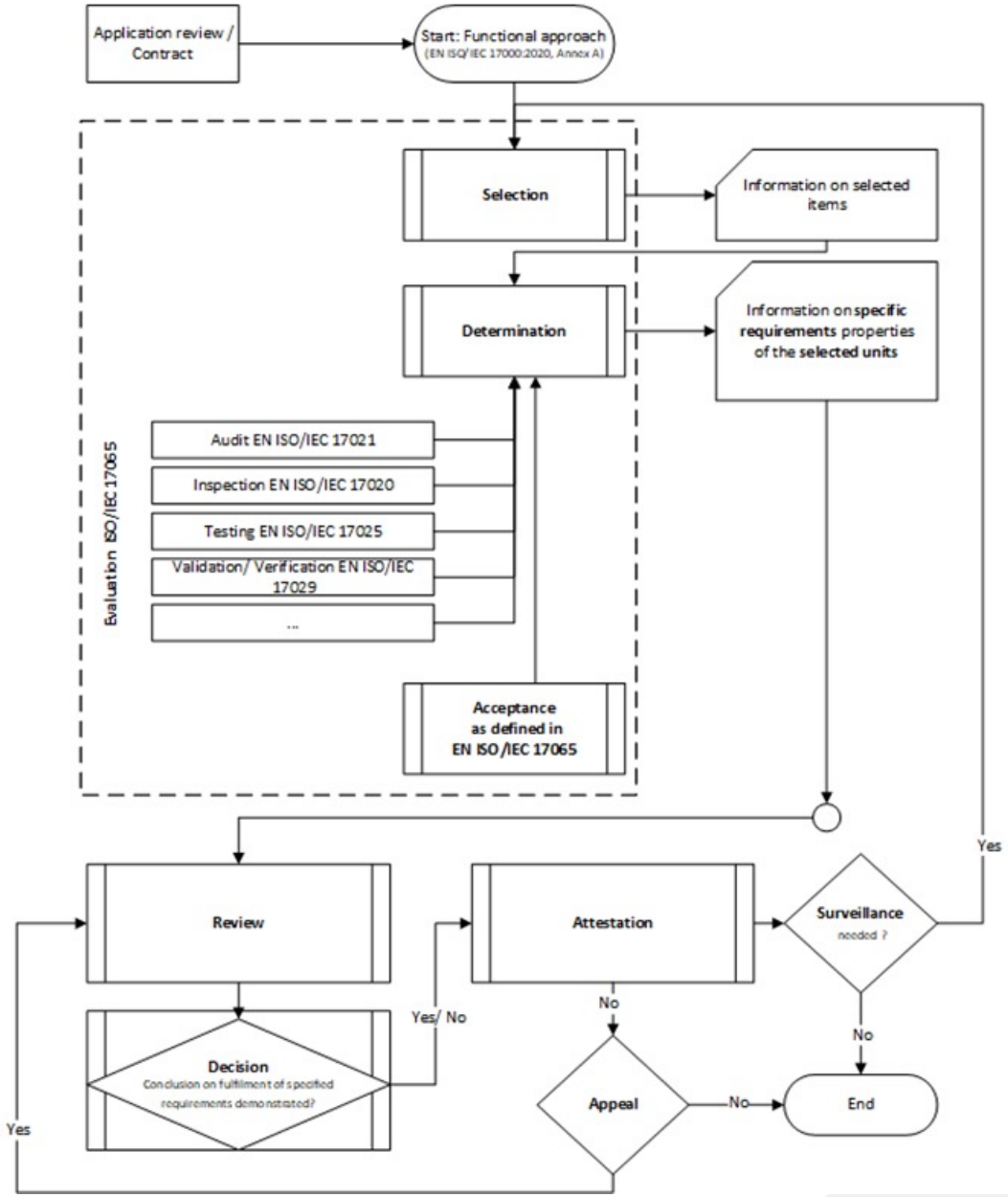
*Accreditation applies only to 3rd party Conformity Assessment Bodies (CABs)*

**High-risk cases require 3rd party Conformity Assessment, as seen for machines listed in Annex 4 of the Machinery Directive 2006/42/EC or for the certified category of civil drones.**

# CEN/CLC TR 17894 AI conformity assessment



# Functional view of AI conformity assessment




Luxembourg House of Cybersecurity

# 2. Workflow in ISO 17025 (testing)

• Application → Scrutiny → On-site Audit → Reporting → Accreditation.

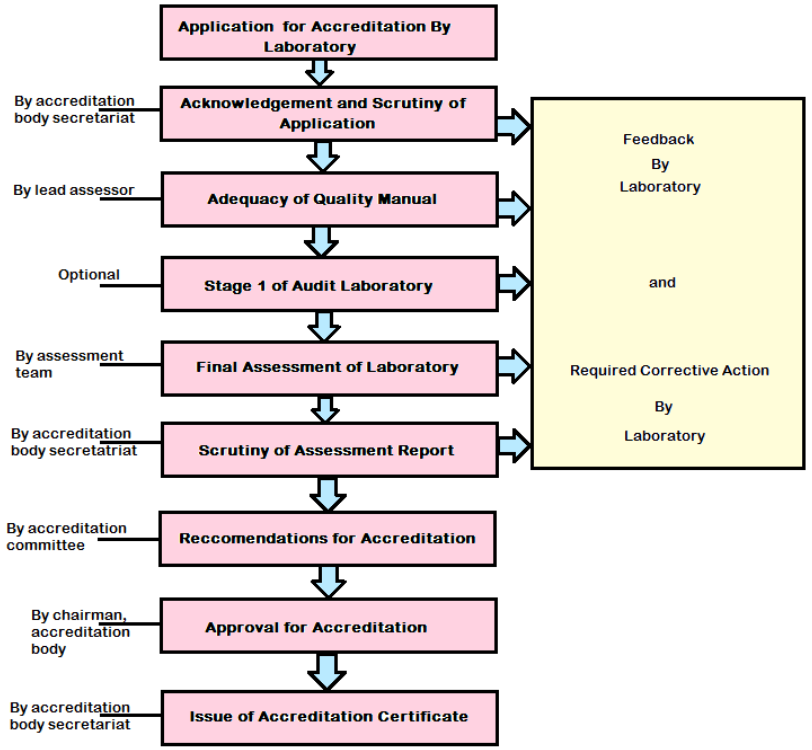
• ISO 17025 supports competency-based lab accreditation.

• Emphasizes continual improvement and documented procedures.

Luxembourg House of Cybersecurity

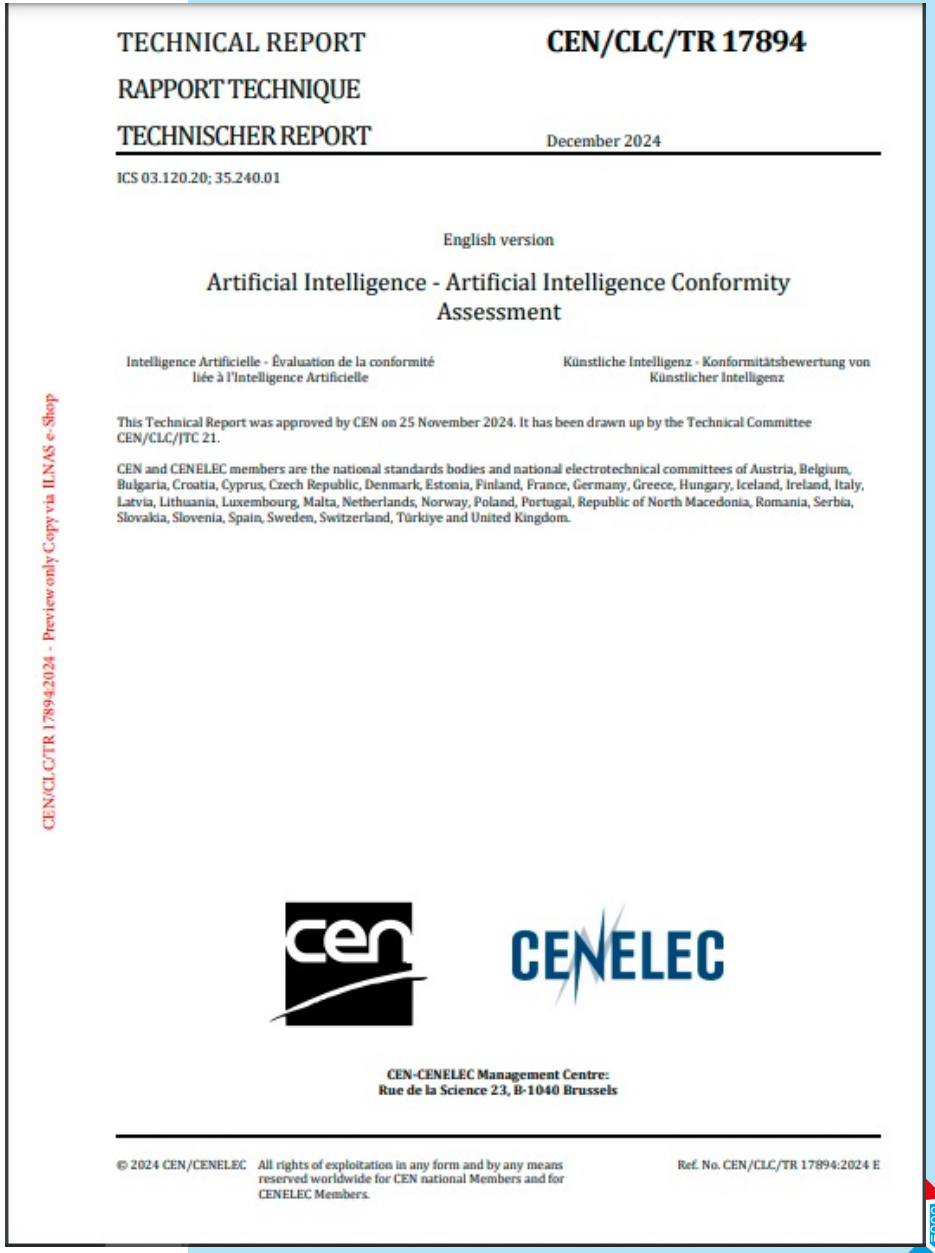
# Workflow in ISO 17025:2017

- A visual diagram typically shows the path from application, audit, report, to accreditation. This is a core structure in ISO 17025 laboratories.




Luxembourg House of Cybersecurity

# Demonstrate compliance to the requirements of the EU AI Act – AI Conformity assessment framework



TECHNICAL REPORT
RAPPORT TECHNIQUE
TECHNISCHER REPORT

**CEN/CLC/TR 17894**

December 2024

ICS 03.120.20; 35.240.01

English version

Artificial Intelligence - Artificial Intelligence Conformity Assessment

Intelligence Artificielle - Évaluation de la conformité liée à l'Intelligence Artificielle

Künstliche Intelligenz - Konformitätsbewertung von Künstlicher Intelligenz

This Technical Report was approved by CEN on 25 November 2024. It has been drawn up by the Technical Committee CEN/CLC/JTC 21.

CEN and CENELEC members are the national standards bodies and national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and United Kingdom.

CEN/CLC/TR 17894:2024 - Preview only Copy via ILNAS e-Shop

CEN-CENELEC Management Centre:
Rue de la Science 23, B-1040 Brussels



Ref. No. CEN/CLC/TR 17894:2024 E

21 https://ilnas.services-publics.lu/ecnor/displayStandard.action?id=260896

# EN AI Conformity assesment -About

This document provides a framework of procedures and processes for conformity assessment related to AI systems. This framework includes both guidance and requirements. Guidance is provided for the determination of the applicable conformity assessment procedures when placing AI systems or products that contain AI-systems on the EU single market or putting them into service.

This document contains how different conformity assessment procedures and processes can be combined and potential gaps filled to ensure essential, and sector specific requirements are met. This includes procedures and processes for documenting and demonstrating compliance with relevant harmonized standards.

This document is intended to support conformity based on Annex VI (Conformity assessment procedure based on internal control) or Annex VII (Conformity based on an assessment of the quality management system and an assessment of the technical documentation) of the EU AI Act.

The work is intended to cover 1st party, 2nd party and 3rd party conformity assessment .

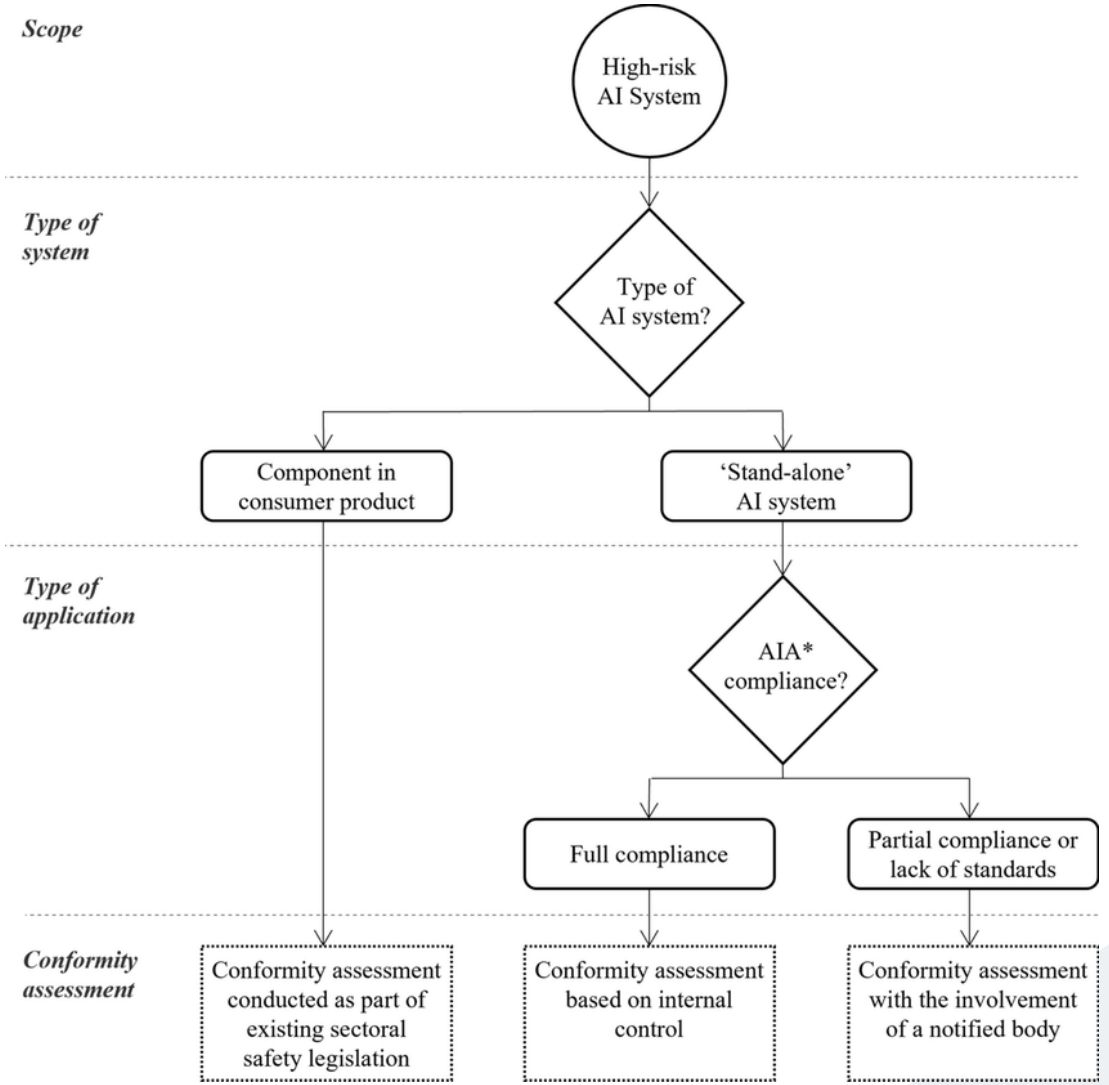
Throughout this document concepts and terminology from the EU Blue Guide [2] and CASCO Toolbox [3] are used and further elaborated as appropriate for the context of AI.

The intended audience for this document is primarily providers of high-risk AI systems that are preparing for undergoing conformity assessment. It is also useful for organizations and people such as AI system stakeholders including AI system developers, providers, customers, partners and regulatory authorities.

The document can be used to evaluate, test and assess AI systems for the purposes of conformity assessment.

Luxembourg House of Cybersecurity

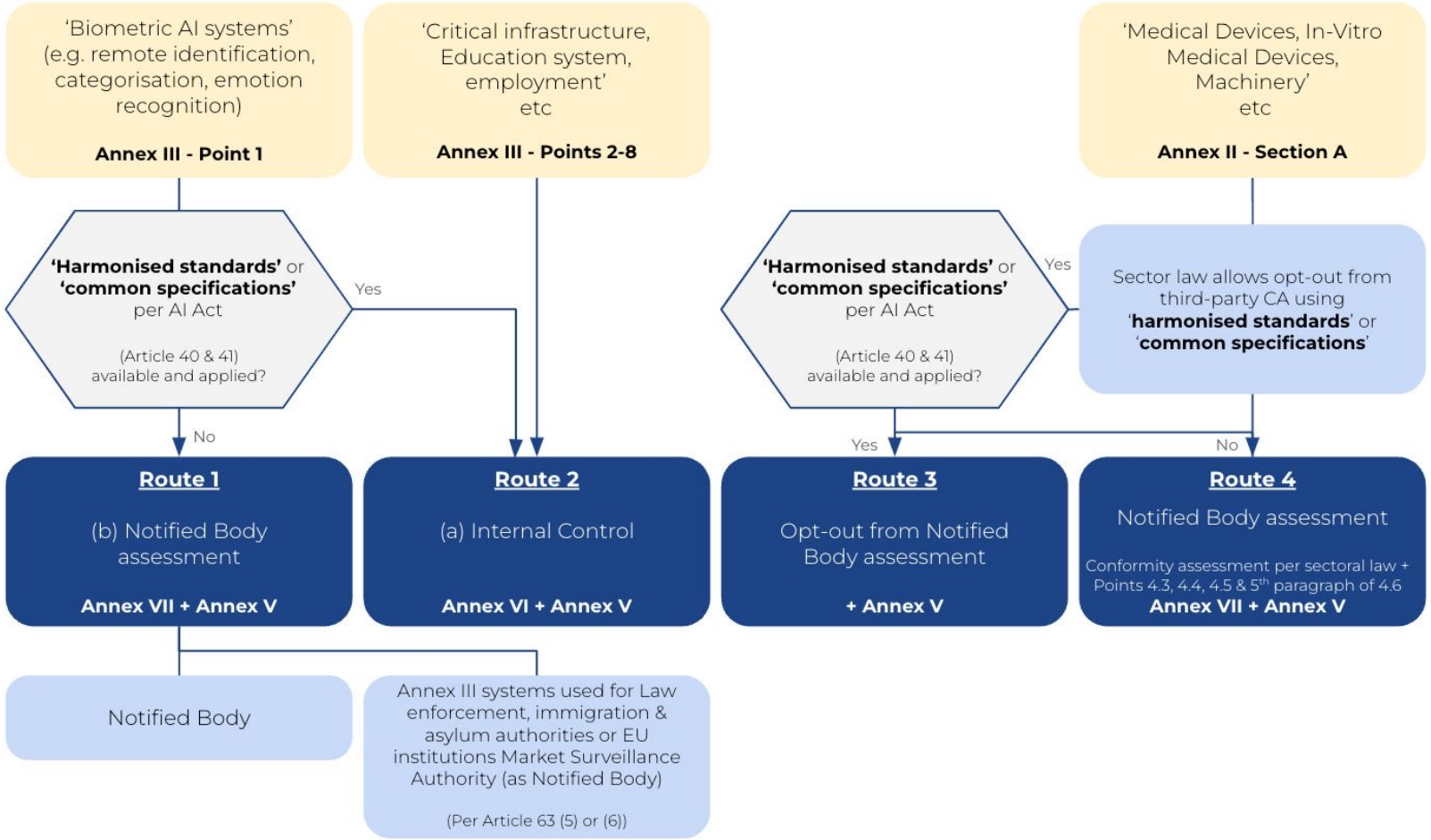
# Main steps in identifying how to build your conformity assesment approach




Mokander, Jakob & Axente, Maria & Casolari, Federico & Floridi, Luciano. (2022). Conformity Assessments and Post-market Monitoring: A Guide to the Role of Auditing in the Proposed European AI Regulation. Minds and Machines. 32. 10.1007/s11023-021-09577-4.

Luxembourg House of Cybersecurity

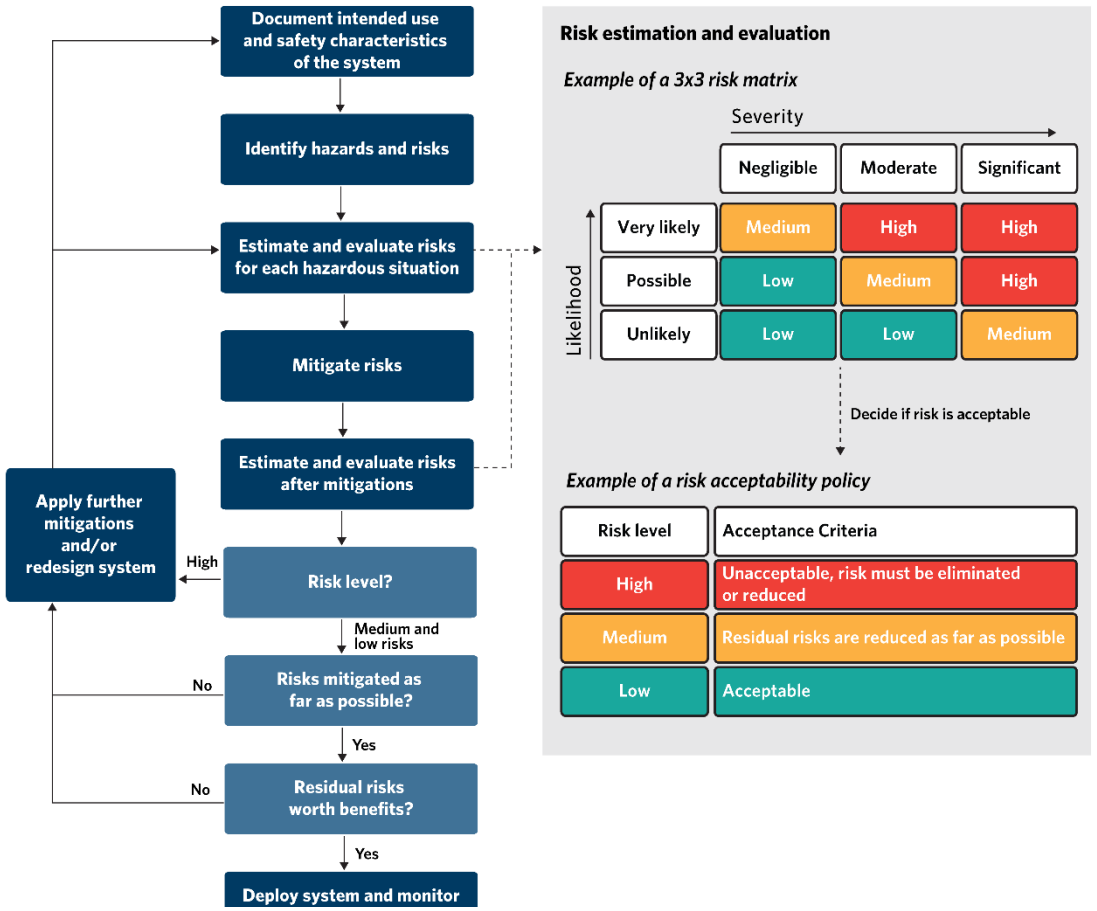
# Conformity assessment routes




Credits: Leon Doorn and Matrix One

Luxembourg House of Cybersecurity

# Preparing the risk management system as support for compliance







- A risk management system requires providers to establish and document:
  - Roles and responsibilities,
  - Risk management steps
  - Methods used in assessing and evaluating risks.

- Included elements for risk assessment (for exemplification only):
  - Severity of identified risks
  - Likelihood of risk levels

# The medical devices use case

**Access to market, cost to achieve access for AI enabled products**

Luxembourg House of Cybersecurity

# Use case: Medical devices

## (EU) Regulations compliance in 2026: *Medical Device Regulation* and *AI act*

AI: **EN AI QMS for EU AI regulatory purposes**
(developed in CEN/CLC JTC 21)

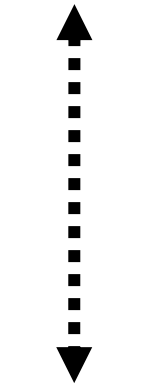
**AI: ISO/IEC DIS 42001** **MD: ISO 13485**

Information technology — Artificial intelligence — **Management system**

**AI: ISO/IEC DIS 25059:2023**

Software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — **Quality model for AI systems**

QMS



RMS

Not sufficient

**Missing product view and considerations of health, safety, fundamental human rights**

**AI: ISO/IEC DIS 23894** **MD: ISO 14971**

Information technology — Artificial intelligence — **Guidance on risk management**

**AI: EN Risk management,** ***including a risk catalogue***

***(developed by CEN/CLC JTC 21)***

**AI enabled medical devices**

**Compliance with sectorial (EU) regulation: MDR**

**Compliance with (EU) AI regulation: AI Act**

CE

**(Global/EU) Standard**

**(EU) Regulations**

Luxembourg House of Cybersecurity

# Use case: Medical devices

## (EU) Regulations compliance **now**: *Medical Device Regulation*

**Technical specifications from EU (international) sectorial standards**

**ISO 13485:2016** Medical devices — **Quality management systems** — Requirements for regulatory purposes

→ **Conformity assessment important elements (EU NLF, CASCO)**

**Quality assurance and Quality Management Systems (QMS)**

**Medical device regulation (MDR)**

⇢ CE

**ISO 14971: 2019** Medical devices — **Application of risk management to medical devices**

→ **Risk assurance and Risk Management Systems (RMS)**

**(Global/EU) Standard**

**(EU) Regulations**

Luxembourg House of Cybersecurity

# Use case: Medical devices

## (EU) Regulations compliance in 2025: *Medical Device Regulation* and *AI act*

| MDR | AI ACT |
|---|---|
| **Risk-based approach** | |
| **No specific requirements for manufacturers** | **Mandatory requirements for AI providers, especially for systems considered as high-risk** |
| **Different levels of risk according to their intended purpose** | **Devices regulated under MDR are considered "high risk".** |

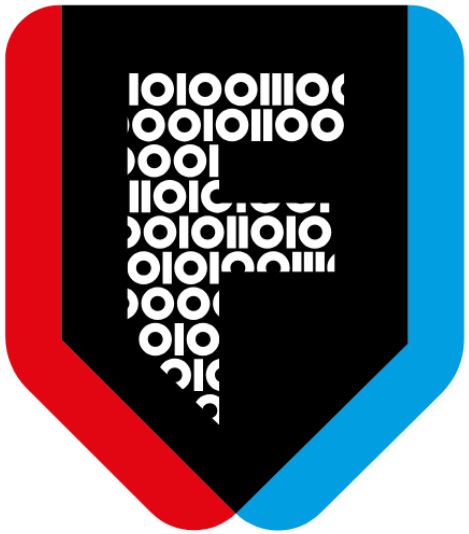
**How to identify devices that are under the scope of the AI act and subject to AI conformity assessment?**

*For medical devices, **only** the medical devices that fall under the medical device regulation (**MDR**) are regulated also by the AI act.*

Luxembourg House of Cybersecurity

# Initiatives in Luxembourg

A new kind of **Capacity**, *built on* ***openness, trust, and dynamic collaborations,*** is needed!



LUXEMBOURG CYBERSECURITY FACTORY



Luxembourg House of Cybersecurity

# RE.M.I. Working Group 5

| | |
|---|---|
| **Objectives** | Identify challenges and gaps for the data-cybersecurity-AI continuum, relating with the legal, information security and AI layers. Collaborate on tackling the identified challenges via the working group, by sharing information, and foster collaborations. |
| **Scope of work** | Assess and map the LU ecosystem challenges in implementing the data-cyber-AI continuum.<br><br>Identify and share complementary expertise, tooling, advise as to build partnerships.<br><br>Identify and share successful use cases, technologies and elements needed in preparing compliance of the AI systems while considering the cybersecurity aspects.<br><br>Organise seminars and workshops for information sharing and community building on topics of complex requirements and active threat risks |

Luxembourg House of Cybersecurity

LUXEMBOURG CYBERSECURITY FACTORY

LUXEMBOURG CYBERSECURITY DATA SPACE

LUXEMBOURG CYBERSECURITY AI HUB

LUXEMBOURG CYBERSECURITY QUANTUM LAB

# Data- Cybersecurity- Artificial Intelligence a continuum for the assessment of AI systems

AI Factories

**Industry use cases (verticals)** = LUXEMBOURG AI FACTORY

Bottom- up process of preparation for compliance

**Artificial Intelligence Regulation: EU AI Act**

**Specific requirements**

Trustworthiness layer

Accuracy | Human oversight | Transparency | Robustness

Logging capabilities

Quality management

Risk management (including AI and cybersecurity)

Data Quality and Governance

**(CEN/CLC JTC 21 EN AI Cybersecurity)**
**Cybersecurity related requirements from the EU AI Act**

**Cybersecurity Regulation: Cyber Solidarity Act, CRA, CSA**

EU cybersecurity Certification - recognition of the level of cybersecurity of ICT solutions across the European Union

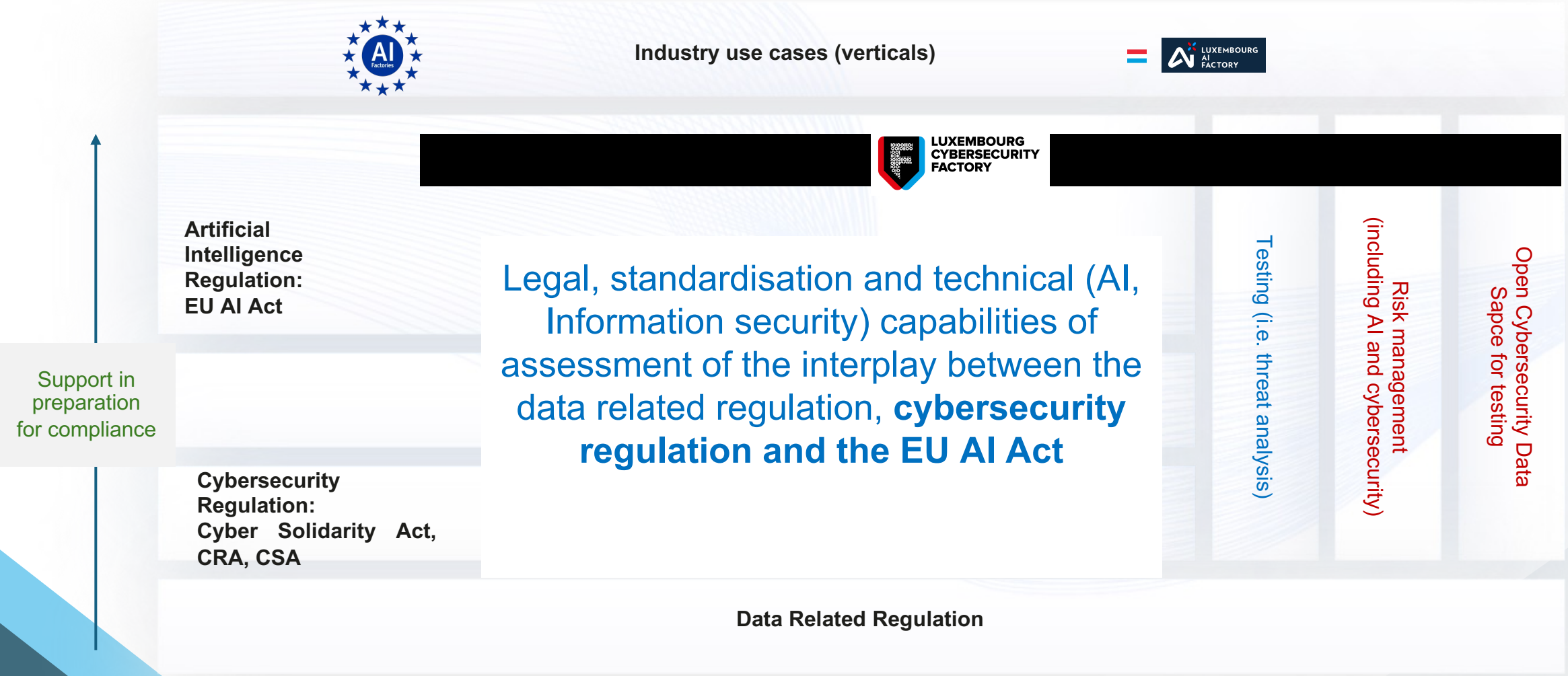
**Data Related Regulation: GDPR, Data Act, Digital Services Act**

**Three horizontal layers of assessment**



Luxembourg House of Cybersecurity

# @LHC Data- Cybersecurity- Artificial Intelligence continuum






Luxembourg House of Cybersecurity

Dr. Emilia Tantar

# Thank you!

Luxembourg House of Cybersecurity

Luxembourg House of Cybersecurity

122, rue Adolphe Fischer
L-1521 Luxembourg

+352 274 00 98 601

factory@lhc.lu

https://lhc.lu