The AI Act & European Standardization

Constantinos Tsiourtos
Public Policy & Legal Advisor
AI, Cybersecurity & Privacy Standardization Expert

CYPRUS ORGANISATION FOR STANDARDISATION
cen
CENELEC

Constantinos Tsiourtos

- Managing Director C.T. KINEAS LLC

Public Policy & Legal Advisor – AI, Cybersecurity, Privacy Standardization Expert

- Standardization: European/International, CYS HoD

CEN CLC JTC21: Artificial Intelligence | CEN/CLC JTC13: Cybersecurity & Data Protection | CEN/CLC JTC21 Artificial Intelligence | ISO/IEC JTC 1/SC 27: Information Security, cybersecurity & privacy protection | ISO/IEC JTC1/SC42: Artificial Intelligence | ETSI Cyber TC (observer) | CEN CLC Standardization Request Ad-Hoc Group (SRAHG) 'AI Act' | CEN CLC WS Digital sovereignty.

- European Union Agency for Cybersecurity (ENISA)

Ad-Hoc WG for the Cloud Security Certification Scheme | Experts Group on Strategy | Experts Group on Vulnerability Handling | ENISA Label Experts Group defining the specifications for the EU Certification Label

- CAI committee of the Council of Europe, building an International legal treaty for Artificial Intelligence
- EU-US Trade and Technology Council
    - WG1: Technology Standards

The AI Act; the proposal in a nutshell

- Published in 2021 COM(2021) 206 final (April 2021)

Subject matter: harmonised rules for the placing on the market, the putting into service and the use of artificial intelligence systems ('AI systems') in the Union;

- **Prohibitions:** the Regulation identifies a series of AI practices that are prohibited because they go against the EU values or because they violate EU individuals' fundamental rights (e.g. social scoring)
- specific **requirements for high-risk AI systems** and obligations for operators of such systems: the proposal primarily focuses on high-risk AI applications and impose stringent requirements on 'providers' and 'users' of AI applications, as well as across the supply chain. In-scope uses are listed in 2 annexes to the legislation
- harmonised **transparency rules: for AI systems** intended to interact with natural persons, **emotion recognition systems** and **biometric categorisation systems, and AI systems used to generate or manipulate image, audio or video content;**
- Set of rules on market monitoring and surveillance.

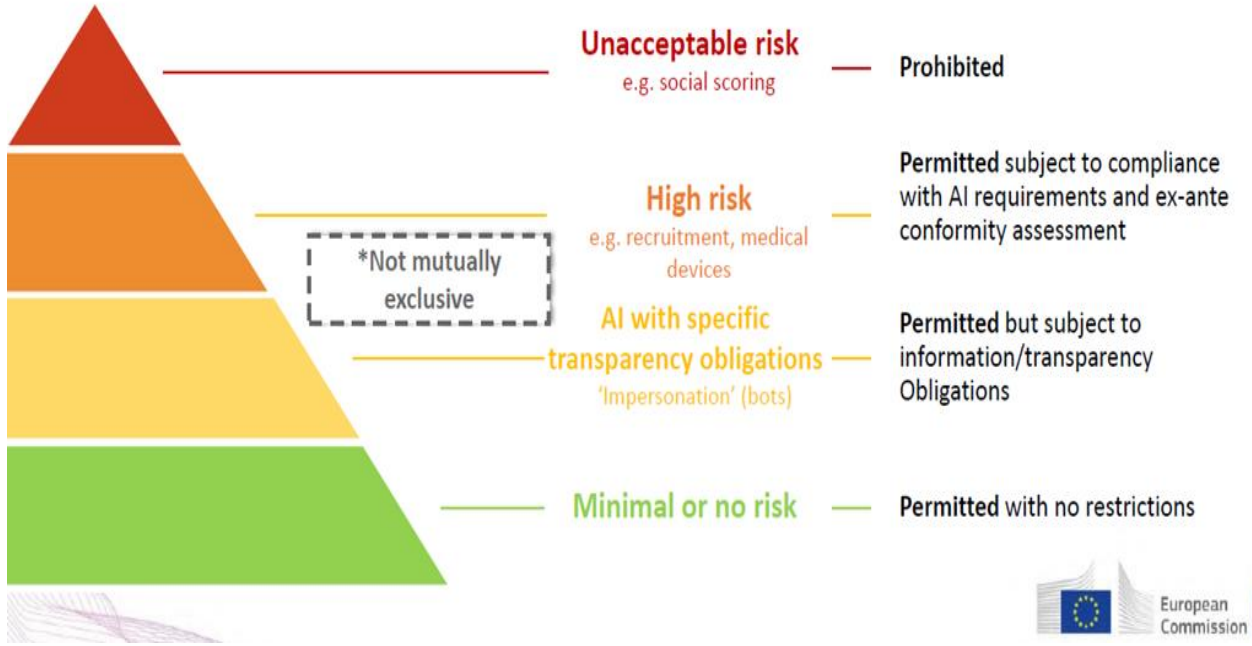
Definition of AI should be as neutral as possible in order to cover techniques which are not yet known/developed

"a software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with"

European Commission

Risk based regulation --> different requirements depending on the level of risk / intended purpose

- **Unacceptable risk:** prohibited use
- **High-risk AI systems:** mandatory obligations, including conformity assessment
- **Limited risk:** subject to limited set of obligations
- **Minimal risk**: green light to be developed and used in the EU



Pre market Conformity Assessment

- AI systems which are regarded as **"high risk"** by the Regulation will need to **undergo conformity assessment before they can be placed on the market** in the EU.
- This will allow **providers to demonstrate their system complies with the mandatory requirements for trustworthy AI** (e.g. data quality, documentation and traceability, transparency, human oversight, security, accuracy and robustness).
- The **precise nature of the conformity assessment procedure required by the Regulation depends on the type of high-risk AI system in question.**

> Pre-Market Conformity Assessment will be followed by Market Surveillance

High Risk AI Systems

The proposal primarily focuses on high-risk AI applications and impose stringent requirements on 'providers' and 'users' of AI applications, as well as across the supply chain. In-scope uses are listed in 2 annexes within the regulation

Annex II

AI systems used as products or safety component of products covered by sectorial Union law including, inter alia:

Provider shall follow the relevant conformity assessment as required under sectorial legal acts.

- Transport
- Medical Devices
- Radio Euipment
- Safety Equipment
- Machinery

Annex III

Other high risk AI applications including, inter alia:

Conformity Assessment via notified body

- Biometric identification and categorization of natural persons

Internal Control No notified body

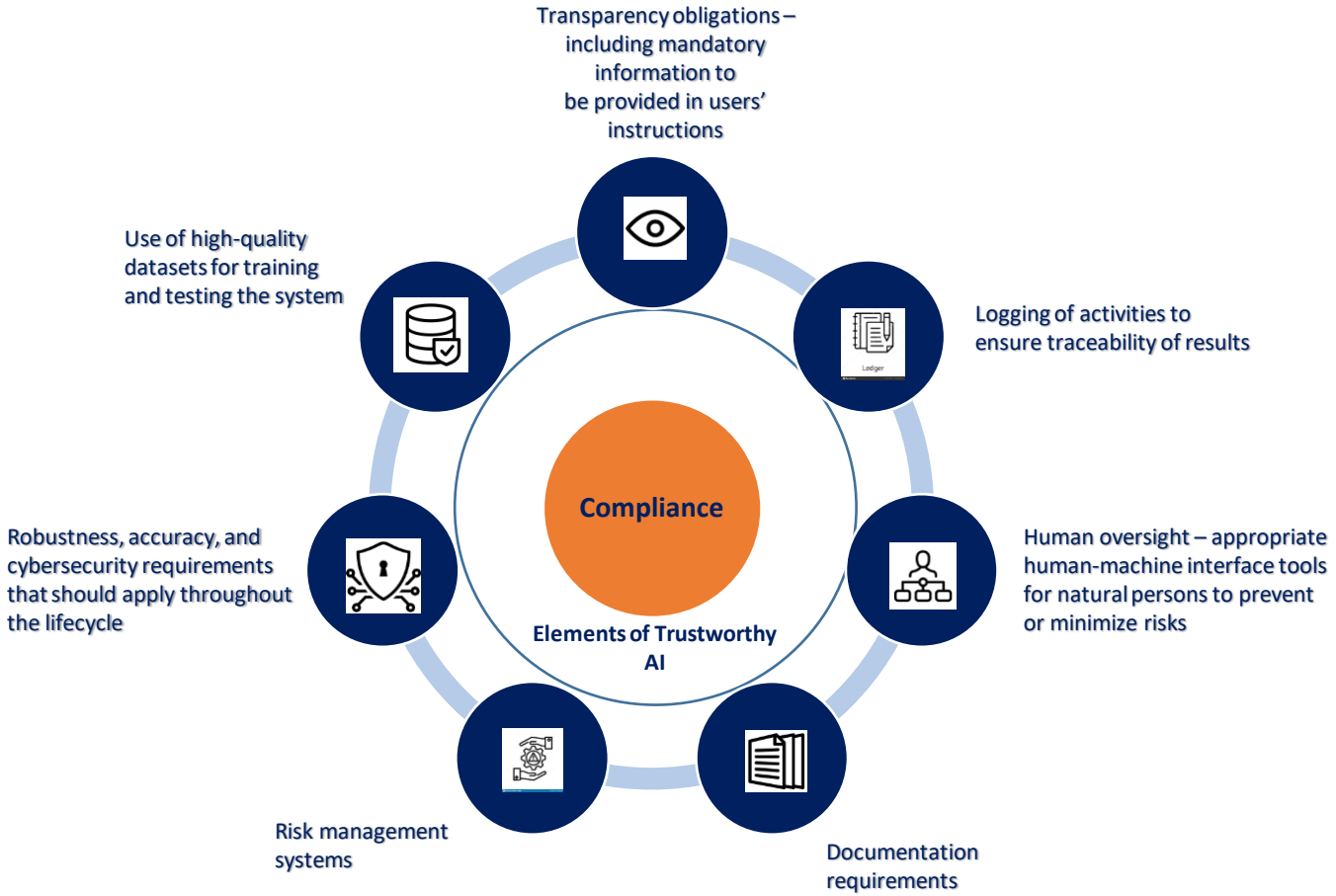
- Management of critical infrastructure
- Education and vocational training
- Employment
- Access to essential private and public services
- Administration of Justice

REMINDER

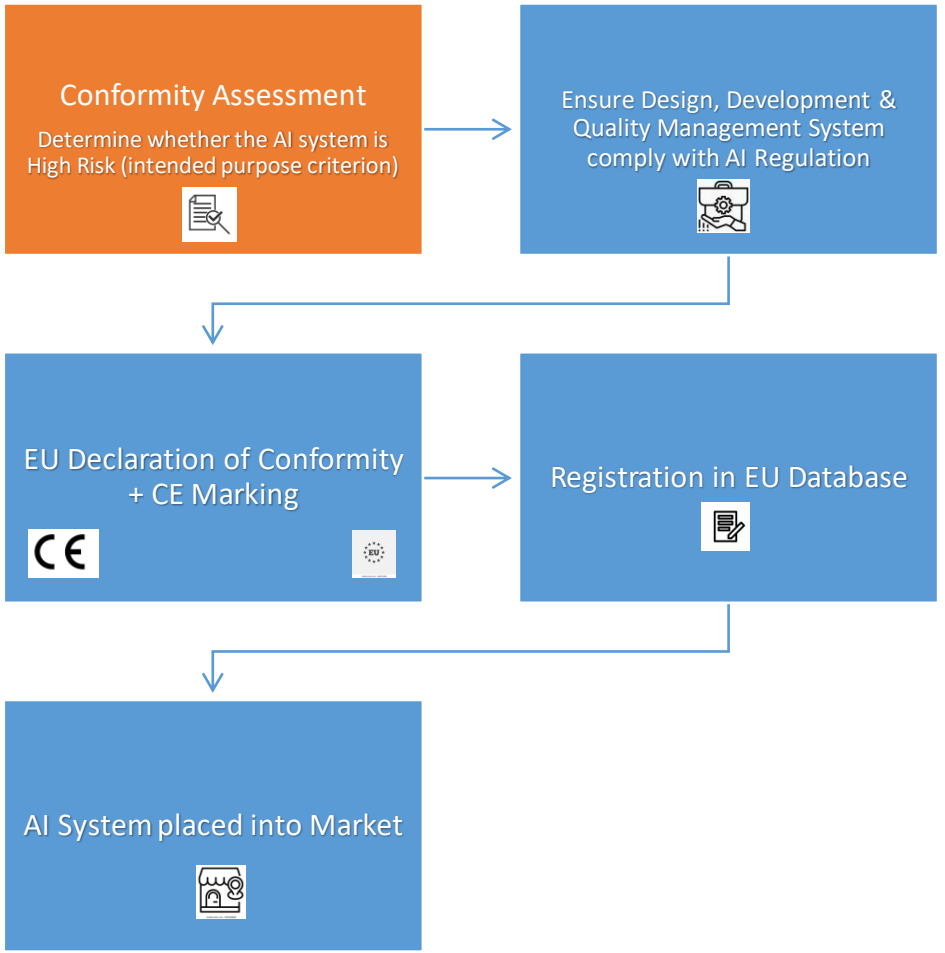
It will apply not only within the EU, but also applies to providers or users that are established or located outside the EU territory and:
(i) which place or put into service AI systems in the EU, or
(ii) the AI output produced by the system is used in the EU.

Ex-Ante requirements checked by a Conformity Assessment

Before the placement of AI systems on the market or their putting into service, high-risk AI systems should undergo a conformity assessment to ensure they are in line with the requirements of the Regulation.

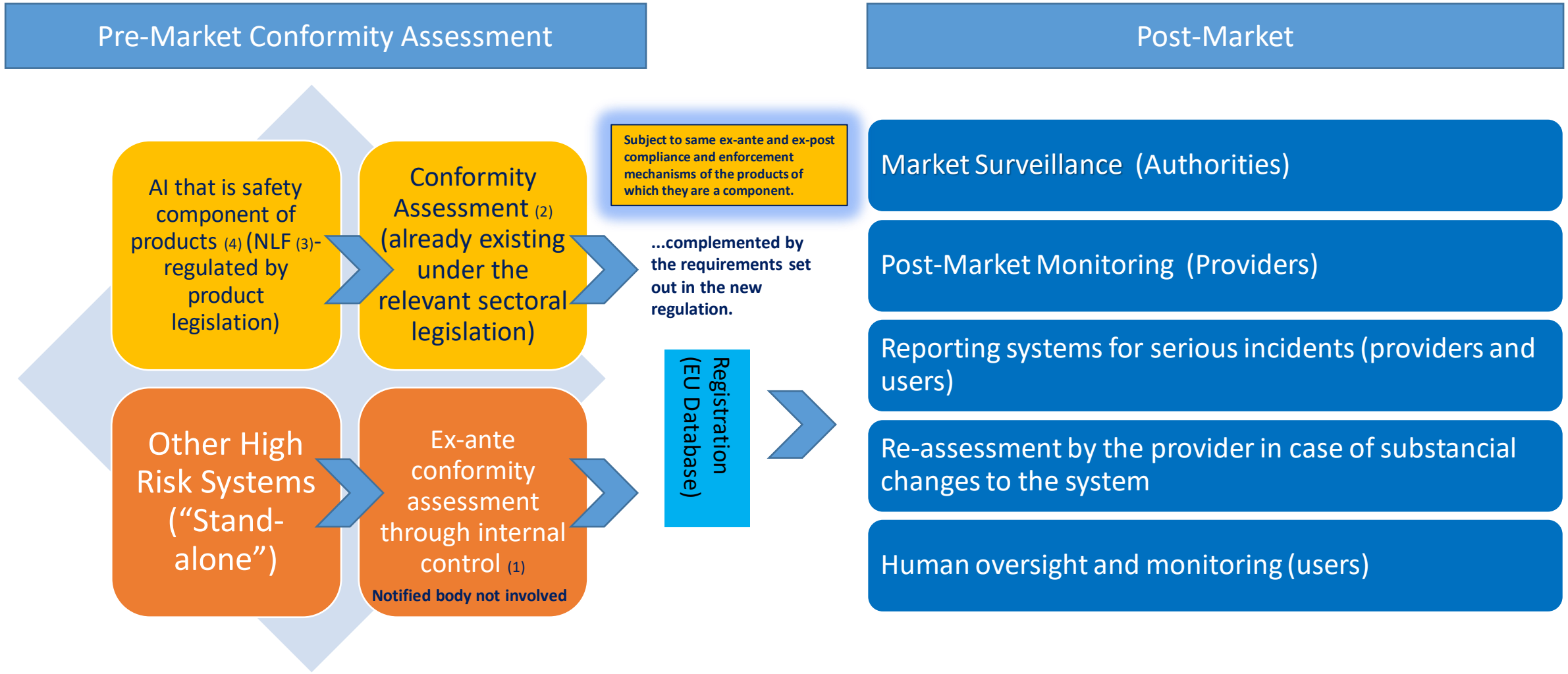


The process



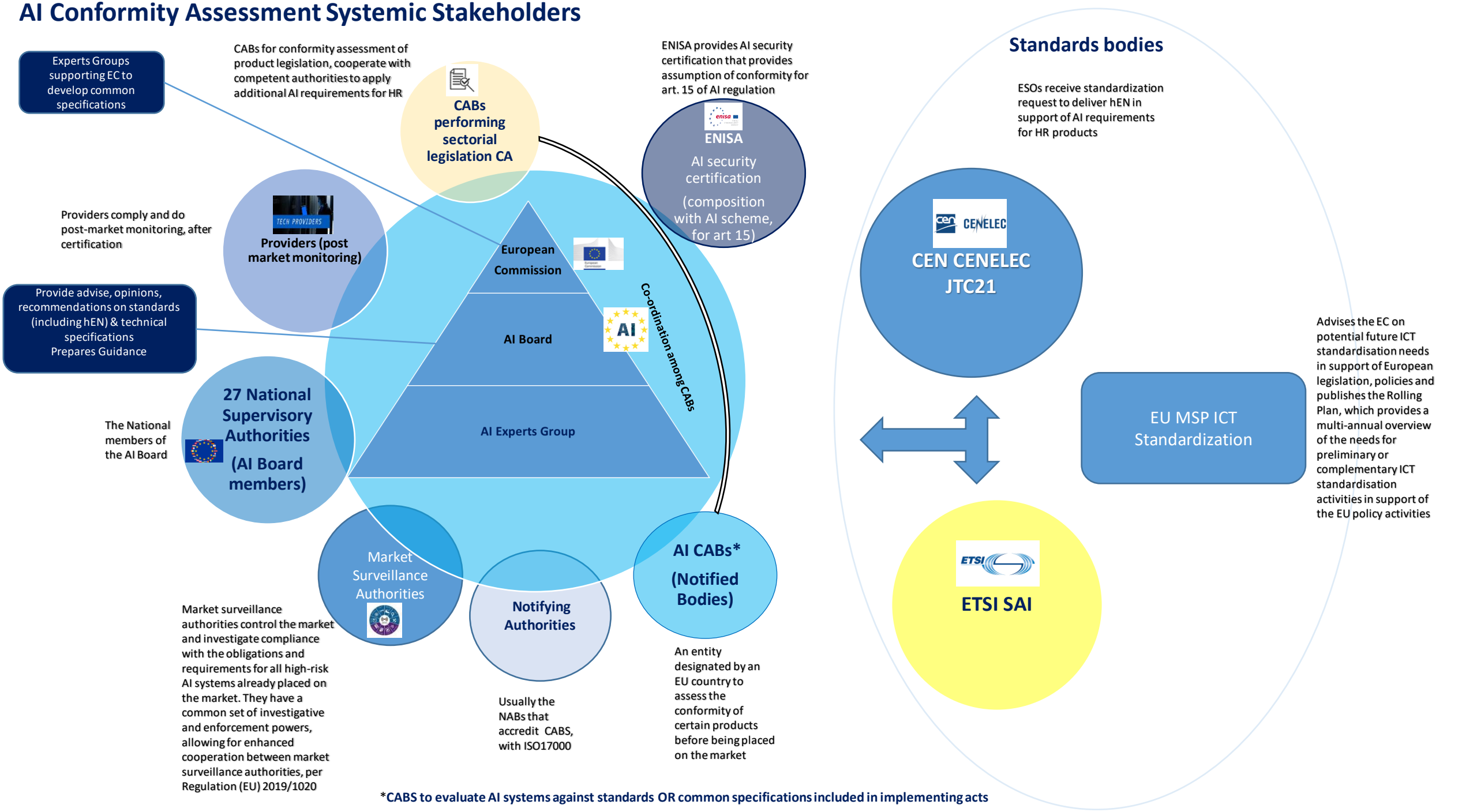
* Importers of AI systems will have to ensure that the foreign provider has already carried out the appropriate conformity assessment procedure and has the technical documentation required by the Regulation. Additionally, importers should ensure that their system bears a European Conformity (CE) marking and is accompanied by the required documentation and instructions of use.

Compliance system explained



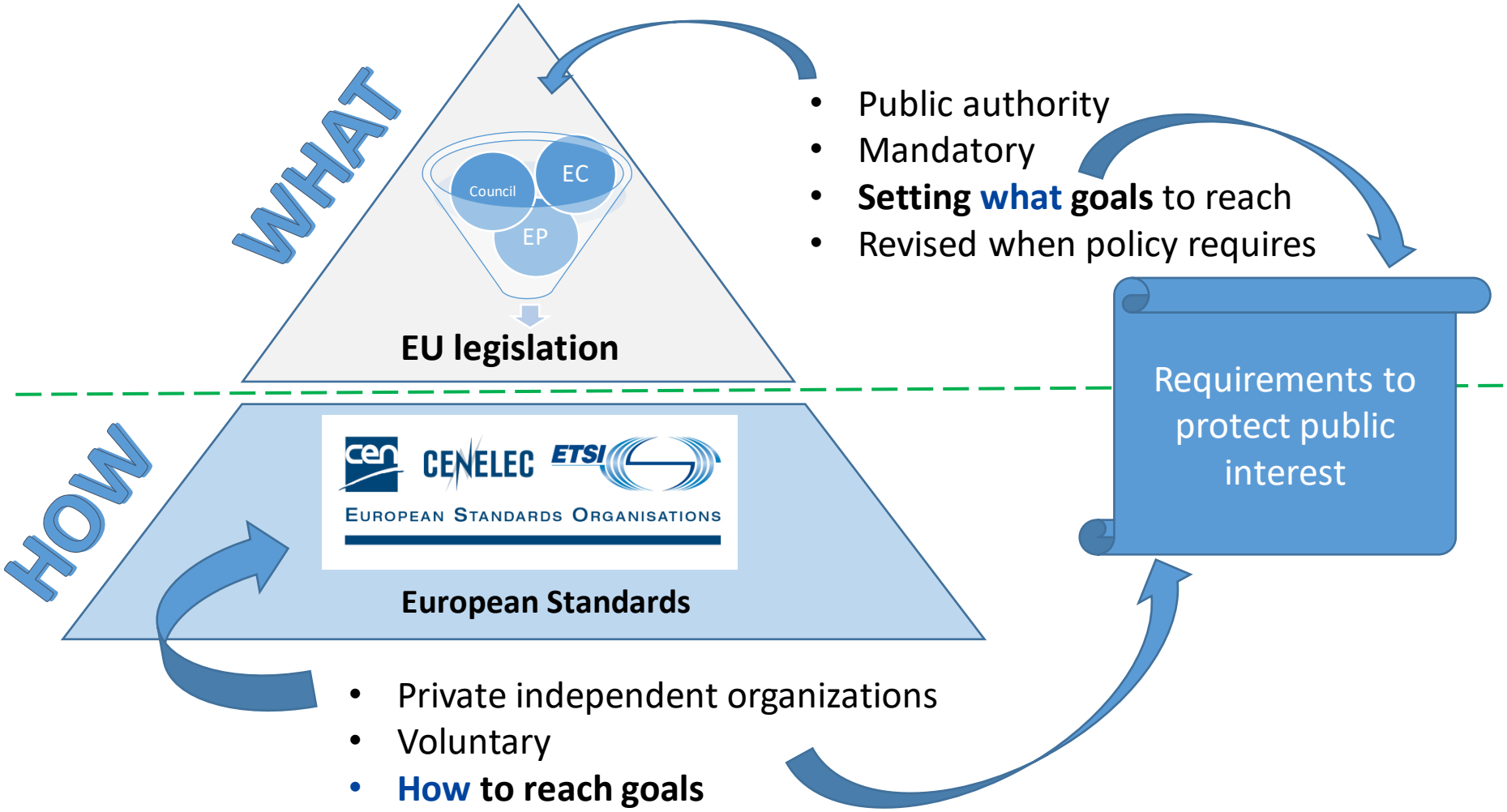
1. Exception: remote biometric authentication (3rd party via notified bodies)
2. If sectorial legislation allows opt-out from 3rd party conformity, the vendor complies with relevant harmonized standards or TS
3. For High-risk AI systems related to products covered by relevant Old Approach legislation (e.g. aviation, cars), the regulation would not directly apply. However, the ex-ante essential requirements for high-risk AI systems will have to be taken into account when adopting relevant implementing or delegated legislation under those acts. In essence, conformity assessment may apply in the future via delegated or implementing acts.
4. Safety components of products covered by sectorial Union legislation will always be high-risk when subject to third-party conformity assessment under that sectorial legislation

AI Conformity Assessment Systemic Stakeholders



*CABS to evaluate AI systems against standards OR common specifications included in implementing acts

How Standardization supports legislation under New Legal Framework



- Public authority
- Mandatory
- **Setting what goals** to reach
- Revised when policy requires

- Private independent organizations
- Voluntary
- **How to reach goals**
- State of the art

Harmonized standards to support the AI Act

A draft standardization request

- ❑ A Draft request was communicated a few months ago, to the CEN CENELEC JTC21. CEN CENELEC & ETSI are both being addressed by the Commission. Both CEN CLC JTC21 and ETSI SAI have initiated preparations for the work.
- ❑ Each of the **requirements for high-risk AI systems must be supported by hENs, hence the long list. (next slide)**

Commission Phased approach:

- 1. This Standardization Request relates to the development of ENs in support of safe and trustworthy artificial intelligence. It is not a request for hENs intended for citation to the OJEU in support of the AIA, as the AIA is not adopted yet. End of 2022
- 2. This request is thus expected to be amended by the European Commission (phase 2) when the AIA is adopted in order to request the ESOs the development of hENs for citation in the Official Journal of the European Union. The future hENs will have to build on the work done based on the present request. When the law will be adopted.

Standards so far:

- **CEN CLC JTC21 "Artificial Intelligence",** already works in cooperation with the European Commission, preparing the work for the HENs. **ETSI SAI** also involved. A roadmap is being planned as well as a work programme to respond to the needs of standards. Many of the needs may be covered by international standards (ISO SC42) if appropriate to the law requirements.
- Some trustworthiness aspects cannot be handled by JTC21. For example, the security specifications call for a collaboration with JTC13 (Cybersecurity).

Harmonized standards to support the AI Act

Table 1: List of European standards and/or European standardisation deliverables to be drafted and deadlines for their adoption

Reference information		Deadline for the adoption by the ESOs
1.	European standard(s) and/or European standardisation deliverable(s) on risk management system for AI systems	31/10/2024
2.	European standard(s) and/or European standardisation deliverable(s) on governance and quality of datasets used to build AI systems	31/10/2024
3.	European standard(s) and/or European standardisation deliverable(s) on Record keeping through built-in logging capabilities in AI systems	31/10/2024
4.	European standard(s) and/or European standardisation deliverable(s) on Transparency and information to the users of AI systems	31/10/2024
5.	European standard(s) and/or European standardisation deliverable(s) on human oversight of AI systems	31/10/2024
6.	European standard(s) and/or European standardisation deliverable(s) on accuracy specifications for AI systems	31/10/2024
7.	European standard(s) and/or European standardisation deliverable(s) on robustness specifications for AI systems	31/10/2024
8.	European standard(s) and/or European standardisation deliverable(s) on cybersecurity specifications for AI systems	31/10/2024
9.	European standard(s) and/or European standardisation deliverable(s) on quality management system for providers of AI system, including post-market monitoring process.	31/10/2024
10.	European standard(s) and/or European standardisation deliverable(s) on conformity assessment for AI systems	31/10/2024

Challenges

1. The future AIA will put forward definitions for several critical terms, in an AI context, that are however already included in the draft standardization request, which, hence, are not defined yet. Therefore, the use of terms such as “accuracy”, “robustness”, “transparency”, “risk”, “governance”, “record keeping”, “information to the users”, “Union values” and “human oversight” (among others) can only be unclear at this stage. These definitions may be drawn from international standards, no need to reinvent the wheel.

1. Standards should harmonize the characteristics, processes, operations, or elements that are common to as many AI systems as possible. Taking ‘intended purpose’ into consideration would require developing standards for each intended purpose - fragmenting the potential harmonisation. The notion of “reasonably foreseeable uses and misuses” appears more appropriate rather than “intended purpose”. Vertical standards will be able to build on this approach too. Under discussion.

Annex I: Tentative Legislative Timeline for AI Act

Legislative Train Timeline Forecast

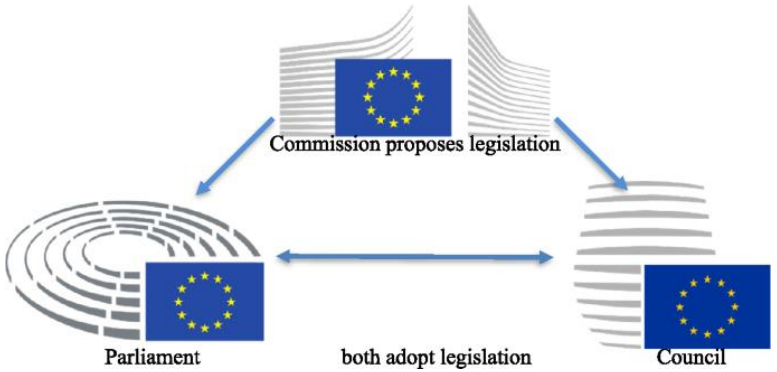
Q2 2021	Q4 2022	2023	2023	LAW APPLICABLE: 2025
Legal Proposal to Council and EP	1st Reading at the EP Council Position	Trialogue	No prediction possible for this stage Doesn't usually take more than 2 years	

More than 3000 amendments submitted. Committee report pending for November.

If the 2 institutions cannot agree on amendments, a trialogue takes place.

Once an agreement has been reached, the text is the Put before the parliament and Council for approval so it can finally be adopted as law

Law would enter into force but only become applicable 24 months after, when HENs will be available.



1st Standardization Request

2nd Standardization Request

Standards to support product certification complementarity

Target of Evaluation: A smartphone

Certified under RED DA { art. 3(3) d,e,f} / then Certified under CRA when application commences

Certified under AI Regulation for trustworthiness/security of AI system embedded

Certified under Chips Act for the security/trustworthiness of the chips components

Certified under the eIDAS2, for the security of mobile-based eID solutions / digital identity wallets

Certified under GPSR with support from CRA for security aspects

Certified under GDPR for personal data processing

All the above legislations are implemented via certification processes supported by standards

- RED Harmonized Standards >> under development
- CRA >> will replace RED, then new hENs will be developed by CEN CLC
- AI regulation Harmonized Standards >> process initiated
- Chips Act >> pending Chips Act approval by the European Parliament
- eIDAS2 >> FITCEM (EN 17640) to support it, gap analysis for standards required

CRA: Cyber Resilience Act
RED: Radio Equipment Directive
eIDAS: electronic Identification, Authentication and Trust Services Regulation
GPSR: General Product Safety Regulation
GDPR: General Data Protection Regulation