EU AI Act: Standards and Tools – Key for Compliance

AI Trust in Electronics Summit
Oslo, 4 September 2025

Dr Jochen Friedrich
Technical Relations Executive

jochen@de.ibm.com

Overview

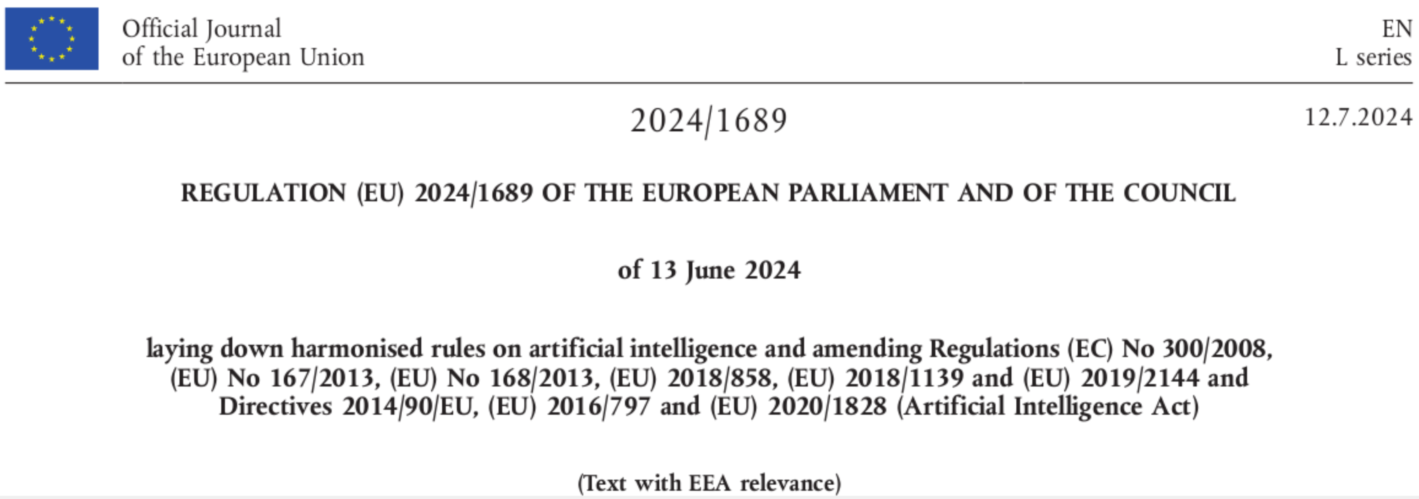
The EU AI Act – EU Technical Regulation: Where are we?

Areas of Regulation: General Purpose AI Models, High-Risk AI Systems

Standards – State of Play and Outlook

Tools

Typical EU Market Access and Safety Regulation



Official Journal
of the European Union

EN
L series

2024/1689

12.7.2024

REGULATION (EU) 2024/1689 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 13 June 2024

laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)

(Text with EEA relevance)

Scope

Promote the uptake of human centric and trustworthy artificial intelligence, while ensuring a high level of protection of health, safety, fundamental rights

Harmonised rules for the placing on the market, the putting into service and the use of artificial intelligence systems (‘AI systems’)

Prohibitions of certain artificial intelligence practices;

Specific requirements for high-risk AI systems and obligations for operators of such systems;

Harmonised transparency rules for certain AI systems;

Harmonised rules for the placing on the market of general-purpose AI models.

What characterises a "typical EU Technical Regulation" ?

Who is that ?

Jacques Delors

* 20. Juli 1925
† 27. Dezember 2023

Former president of the European Commission (1985-1995)

Major role in overcoming the “europsclerosis” of the 1980s and accelerating the process of strengthening European unity (EEA, Maastricht treaty, re-organising the European Commission

And why is he of relevance for our topic…?

15	€1 MILLION
14	€500.000
13	€125.000
12	€64.000
11	€32.000
10	€16.000
9	€8.000
8	€4.000
7	€2.000
6	€1.000
5	€500
4	€300
3	€200
2	€100
1	€50

During Jacques Delor's term of office as President of the European Commission he

A: Ordered that regulations should be written like standards

B: Introduced a law entitling the European Parliament to set technical standards

C: Introduced the legal framework of the New Approach

D: Required EU Member States to set up national Standardisation Bodies

And why is he of relevance for our topic…?

During Jacques Delor's term of office as President of the European Commission he

A: Ordered that regulations should be written like standards

B:

C: Introduced the legal framework of the New Approach

D:

AI Act – EU technical regulation

IBM has decades-long experience in working with such regulations in the field of hardware compliance, e.g. product safety, electromagnetic compatibility, etc.

Basic Principle (**“EU New Legislative Framework”** formerly New Approach):

Legislators

Legal acts lay down the essential requirements and define safety objectives.

Private Sector

Harmonised European Standards define the technical way how to fulfil the legal requirements and be compliant with the safety objectives.

Compliance is mandatory for market access.

Harmonised standards are developed in one or more of the European standardisation organisations and are based on formal EU standardisation requests.

The New Approach / New Legislative Framework: Before and After

BEFORE

All technical requirements were part of the legal acts.

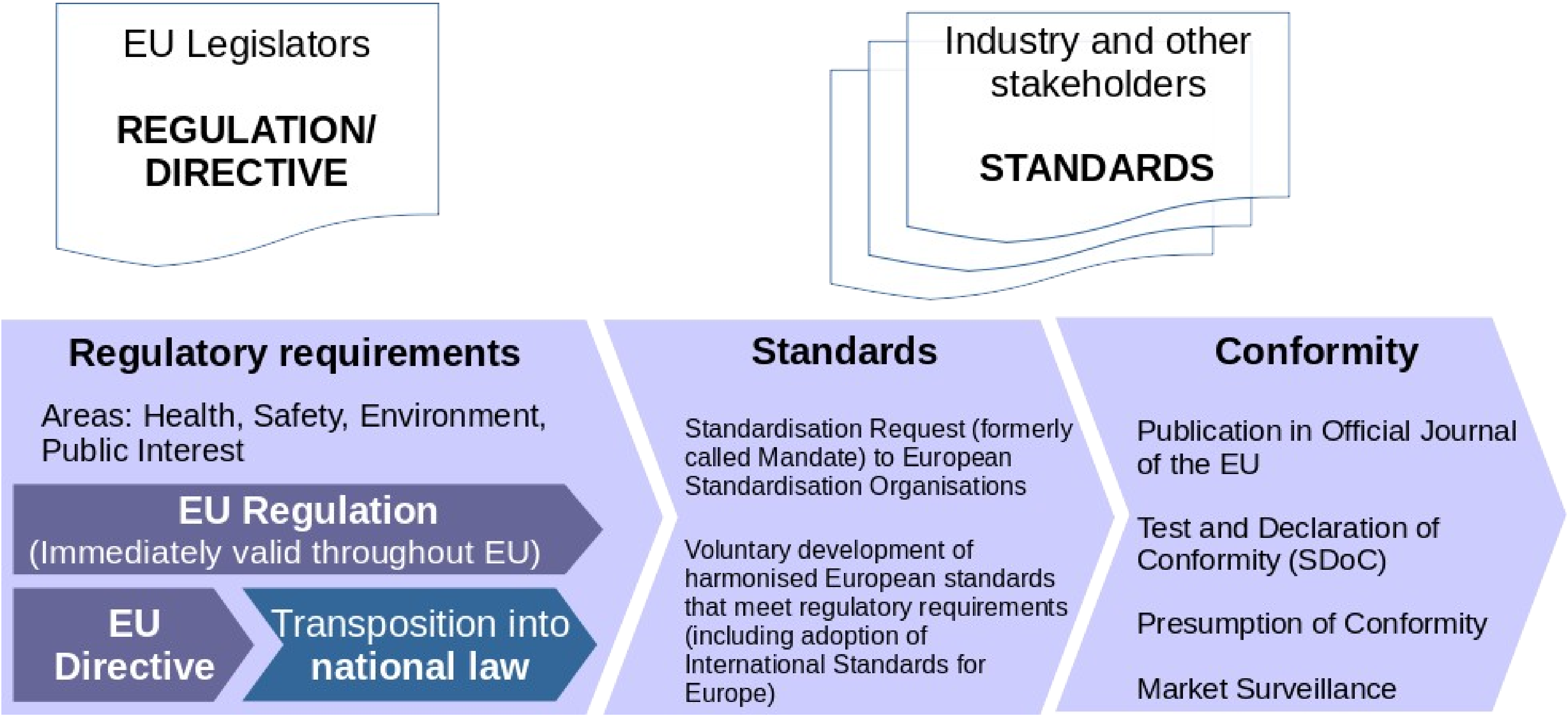
AFTER

Legal acts lay down the legal requirements and define safety objectives.

Harmonised European Standards define the technical way how to fulfil the legal requirements and be compliant with the safety objectives.

New Legislative Framework (NLF): Key Role for Standards

- Key element of the EU regulatory framework and the EU single market
- Definition of safety objectives in legal acts, technical details laid down in standards
- Standards development on the basis of an EU Standardisation Request
- Compliant products may be brought to the market in the EU under the presumption of conformity
- Innovation friendly – innovation via standards



EU Legislators

REGULATION/ DIRECTIVE

Industry and other stakeholders

STANDARDS

Regulatory requirements

Areas: Health, Safety, Environment, Public Interest

EU Regulation (Immediately valid throughout EU)

EU Directive

Transposition into national law

Standards

Standardisation Request (formerly called Mandate) to European Standardisation Organisations

Voluntary development of harmonised European standards that meet regulatory requirements (including adoption of International Standards for Europe)

Conformity

Publication in Official Journal of the EU

Test and Declaration of Conformity (SDoC)

Presumption of Conformity

Market Surveillance

Setting the law

Request to private sector

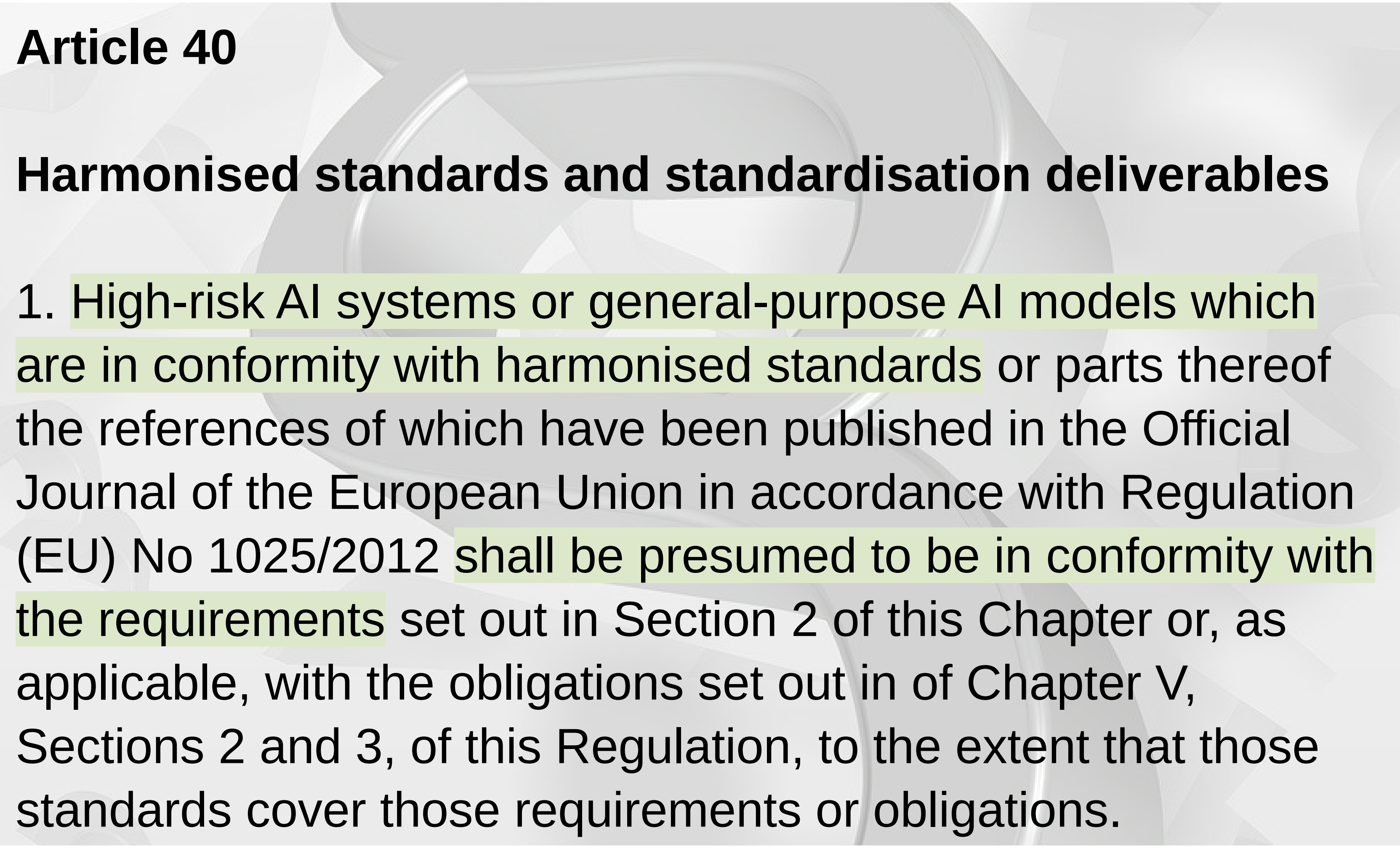
Conformity assessment and demonstration

AI Act:
Key Role of Standards

Article 40 establishes the processes of the EU New Legislative Framework to be used.

A Supplier’s Declaration of Conformity testifies compliance and allows to bring and operate technologies on the market.

No 3rd party certification required.



Article 40

Harmonised standards and standardisation deliverables

1. High-risk AI systems or general-purpose AI models which are in conformity with harmonised standards or parts thereof the references of which have been published in the Official Journal of the European Union in accordance with Regulation (EU) No 1025/2012 shall be presumed to be in conformity with the requirements set out in Section 2 of this Chapter or, as applicable, with the obligations set out in of Chapter V, Sections 2 and 3, of this Regulation, to the extent that those standards cover those requirements or obligations.

EU AI Act: Requirements

Prohibited practices

Applies 6 months after AI Act coming into force, i.e. February 2, 2025.

General purpose AI

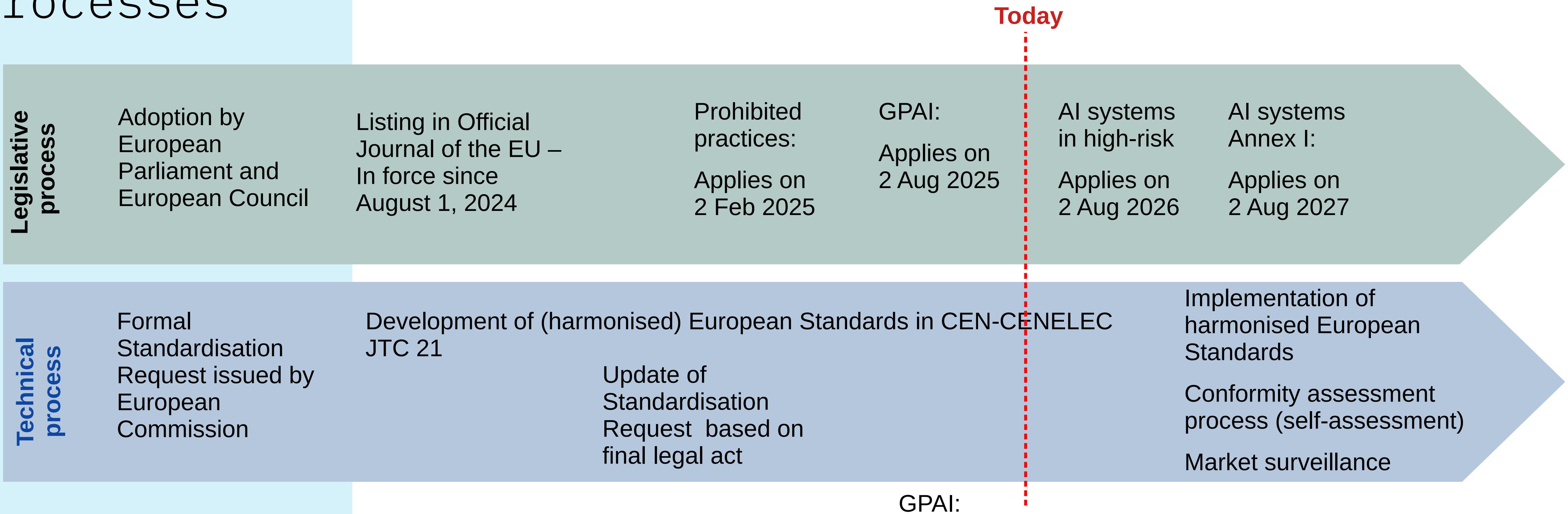
Applies 12 months after AI Act coming into force, i.e. August 2, 2025.

AI systems in high-risk areas

For areas listed in Annex III: applies 24 months after AI Act coming into force, i.e. August 2, 2026.

For areas related to Annex I: applies 36 months after AI Act coming into force, i.e. August 2, 2027.

AI Act: Legislative and technical processes



Today

Legislative process

Adoption by European Parliament and European Council

Listing in Official Journal of the EU – In force since August 1, 2024

Prohibited practices:

Applies on 2 Feb 2025

GPAI:

Applies on 2 Aug 2025

AI systems in high-risk

Applies on 2 Aug 2026

AI systems Annex I:

Applies on 2 Aug 2027

Technical process

Formal Standardisation Request issued by European Commission

Development of (harmonised) European Standards in CEN-CENELEC JTC 21

Update of Standardisation Request based on final legal act

Implementation of harmonised European Standards

Conformity assessment process (self-assessment)

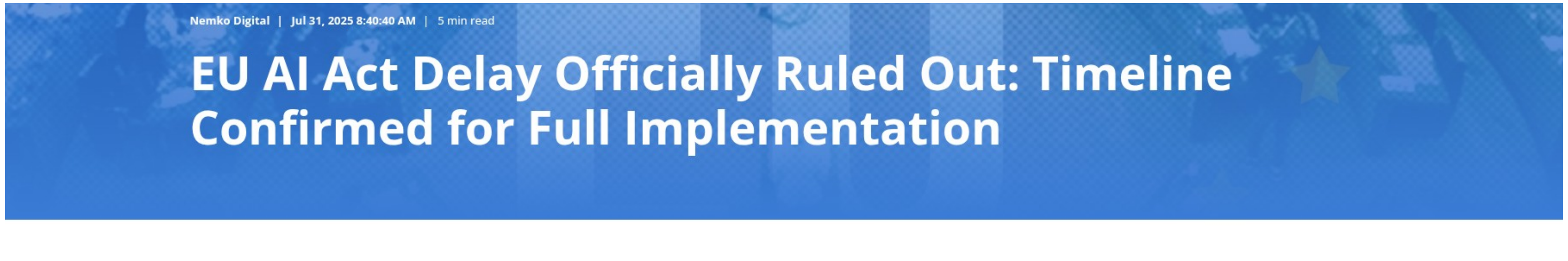
Market surveillance

GPAI:

Code(s) of practice to bridge time until harmonised standards are available

A further standardisation request will be issued on GPAI and sustainable AI

Will the EU AI Act be withdrawn, delayed, … ?



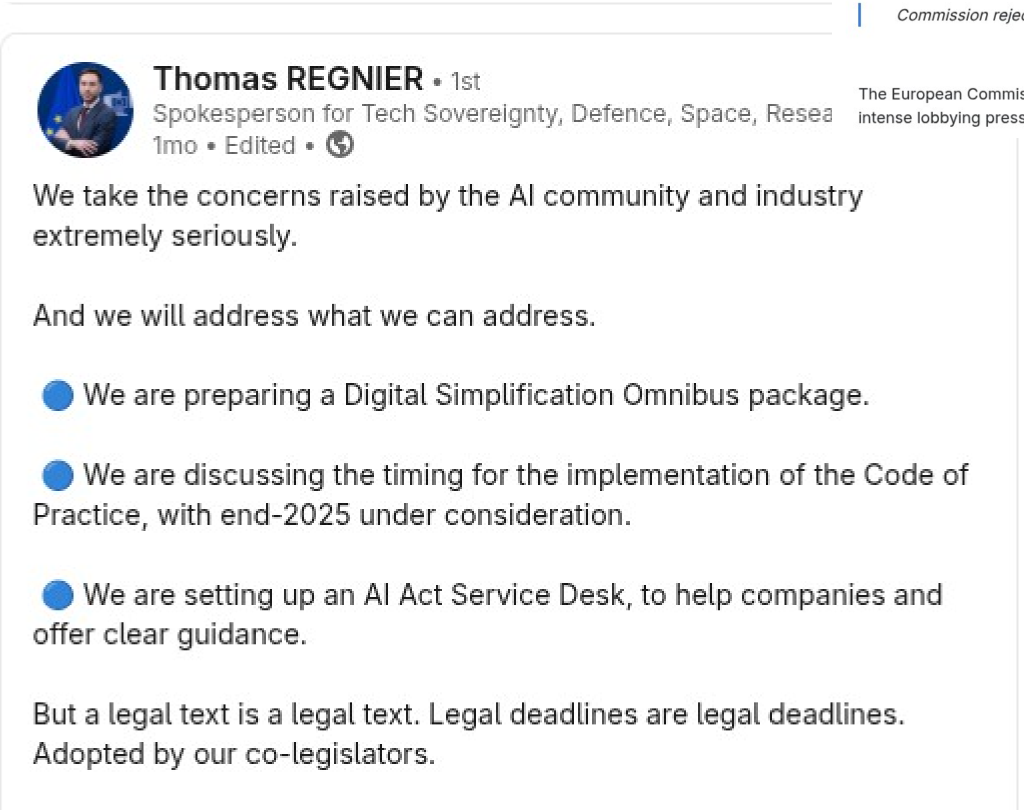
Nemko Digital | Jul 31, 2025 8:40:40 AM | 5 min read

EU AI Act Delay Officially Ruled Out: Timeline Confirmed for Full Implementation

Commission rejects EU AI Act delay requests. August 2025 GPAI deadline approaches. Expert guidance on navigating fixed compliance timeline.

The European Commission has definitively ruled out any **EU AI Act delay**, confirming that the world's first comprehensive artificial intelligence legislation will proceed according to its original timeline despite intense lobbying pressure from the industry for postponement.

https://digital.nemko.com/news/eu-ai-act-delay-officially-ruled-out



Thomas REGNIER • 1st
Spokesperson for Tech Sovereignty, Defence, Space, Resea
1mo • Edited •

We take the concerns raised by the AI community and industry extremely seriously.

And we will address what we can address.

- We are preparing a Digital Simplification Omnibus package.
- We are discussing the timing for the implementation of the Code of Practice, with end-2025 under consideration.
- We are setting up an AI Act Service Desk, to help companies and offer clear guidance.

But a legal text is a legal text. Legal deadlines are legal deadlines. Adopted by our co-legislators.

https://www.linkedin.com/posts/thomas-regnier-24a05810b_we-take-the-concerns-raised-by-the-ai-community-activity-7346868389400768512-gTd_?utm_source=share&utm_medium=member_desktop&rcm=ACoAAACuCT8B_mFRc3OCvFMc4roxoB982lEjlIs

The time lines are laid down in the legal act. Changing them would require a new legal proposal and agreement from the EP and the Council.

The rules and processes for prohibited AI technologies and for GPAI are settled and working. So all that is still open are the rules for high-risk AI systems.

The Commission closely follows the development of the harmonised standards and will be able to react.

Also market surveillance will play a key role in guiding the process.

Two Areas subject to Market Access Regulation

GPAI

Requirements apply since 2 Aug 2025

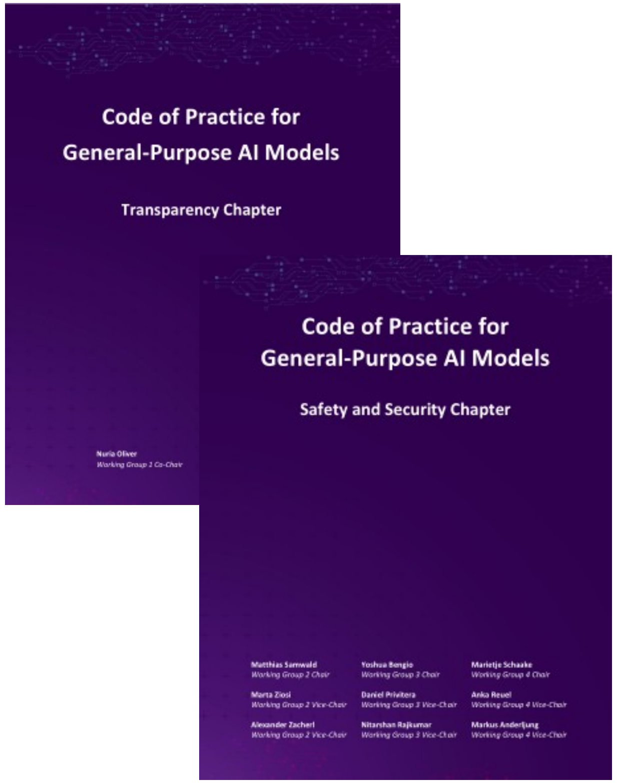
Code of Practice (CoP – done by European Commission, AI Office; stakeholders were able to comment on drafts) available.

Also available: Template for publishing openness information

IBM is an early signatory to this CoP.

On the long run: Harmonised European standards will be developed and replace the Code of Practice.

EU Code of Practice: Examples of the Requirements



Code of Practice for General-Purpose AI Models

Transparency Chapter

Nuria Oliver
Working Group 1 Co-Chair

Code of Practice for General-Purpose AI Models

Safety and Security Chapter

Matthias Samwald
Working Group 2 Chair

Marta Ziosi
Working Group 2 Vice-Chair

Alexander Zacherl
Working Group 2 Vice-Chair

Yoshua Bengio
Working Group 3 Chair

Daniel Privitera
Working Group 3 Vice-Chair

Nitarshan Rajkumar
Working Group 3 Vice-Chair

Marietje Schaake
Working Group 4 Chair

Anka Reuel
Working Group 4 Vice-Chair

Markus Anderljung
Working Group 4 Vice-Chair

Transparency

Measure 1.1 Drawing up and keeping up-to-date model documentation

Measure 1.2 Providing relevant information

Measure 1.3 Ensuring quality, integrity, and security of information

Security and Safety

Commitment 1 Safety and Security Framework

- Measure 1.1 Creating the Framework
- Measure 1.2 Implementing the Framework
- Measure 1.3 Updating the Framework
- Measure 1.4 Framework notifications

In total: 9 commitments with specific measures.

IBM Granite – performant and trusted AI models. Open Source

Open

Choose the right model, from sub-billion to 34B parameters, open-sourced under Apache 2.0.

Performant

Don’t sacrifice performance for cost. Granite performance is proven across a variety of enterprise tasks.

Trusted

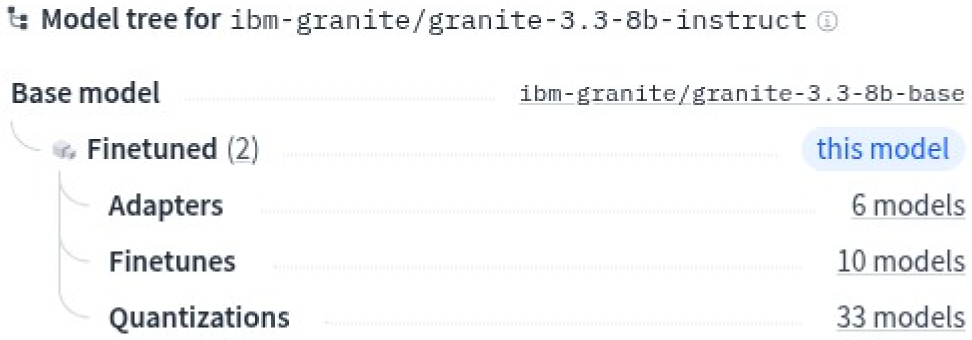
Build responsible AI with a comprehensive set of risk and harm detection capabilities, transparency, and IP protection.

The future of AI is Open.

https://www.ibm.com/granite/docs/models/granite/

IBM adopted the Linux Foundation’s Model Openness Framework for assessing the models
https://developer.ibm.com/articles/cl-open-architecture-update/

Detailed openness information published
https://huggingface.co/ibm-granite/granite-3.3-8b-instruct



Model tree for `ibm-granite/granite-3.3-8b-instruct`

Base model	`ibm-granite/granite-3.3-8b-base`
Finetuned (2)	this model
Adapters	6 models
Finetunes	10 models
Quantizations	33 models

Two Areas subject to Market Access Regulation

GPAI

Requirements apply since 2 Aug 2025

Code of Practice (CoP – done by European Commission, AI Office; stakeholders were able to comment on drafts) available.

Also available: Template for publishing openness information

IBM is an early signatory to this CoP.

On the long run: Harmonised European standards will be developed and replace the Code of Practice.

High-risk AI Systems

Essential requirements apply by 2 Aug 2026

Currently in progress: Development of harmonised European standards according to the process of the New Legislative Framework and a Standardisation Request issued by the European Commission

Once the standards are available their correct implementation will provide presumption of conformity.

Reminder: No 3rd Party Certification required accept in exceptional cases

In the hands of the private sector

With the listing of the AI Act in the Official Journal of the EU – the legal process was done.

Development of the harmonised European Standards required for compliance is in the hands of the private sector.

European Commission: Right of initiative for legal acts

European Council and European Parliament: Two chambers negotiating and agreeing on final legal act

LEGISLATIVE PROCESS COMPLETED WITH LISTING IN OFFICIAL JOURNAL OF EU

PRIVATE SECTOR ENTITLED TO DEVELOP HARMONISED EUROPEAN STANDARDS

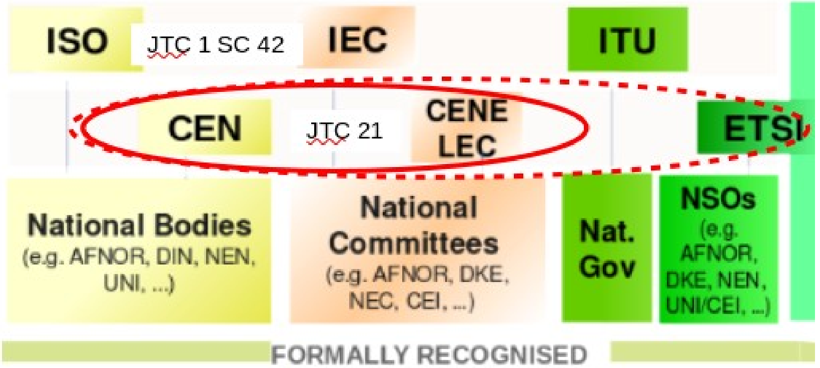
Industry

Civil Society

Research

Academia

…



CONFORMITY ASSESSMENT

Conformity assessment may be done either in the form of well documented self-assessment or in collaboration with a notified body.

EU MEMBER STATES

Accreditation of notified bodies

Building up of market surveillance

Work on harmonised European standards

Essential requirements (in the law)

Risk management system

Data and data governance

Technical documentation

Record-keeping

Transparency and provision of information to users

Human oversight

Accuracy, robustness and cybersecurity

EU Standardisation Request in place

Risk management system for AI systems

Governance and quality of datasets used to build AI systems

Record keeping through built-in logging capabilities in AI systems

Transparency and information to the users of AI systems

Human oversight of AI systems

Accuracy specifications for AI systems

Robustness specifications for AI systems

Cybersecurity specifications for AI systems

Quality management system for providers of AI system, including post-market monitoring process.

Conformity assessment for AI systems

Expected in future Standardisation Request based on final AI Act

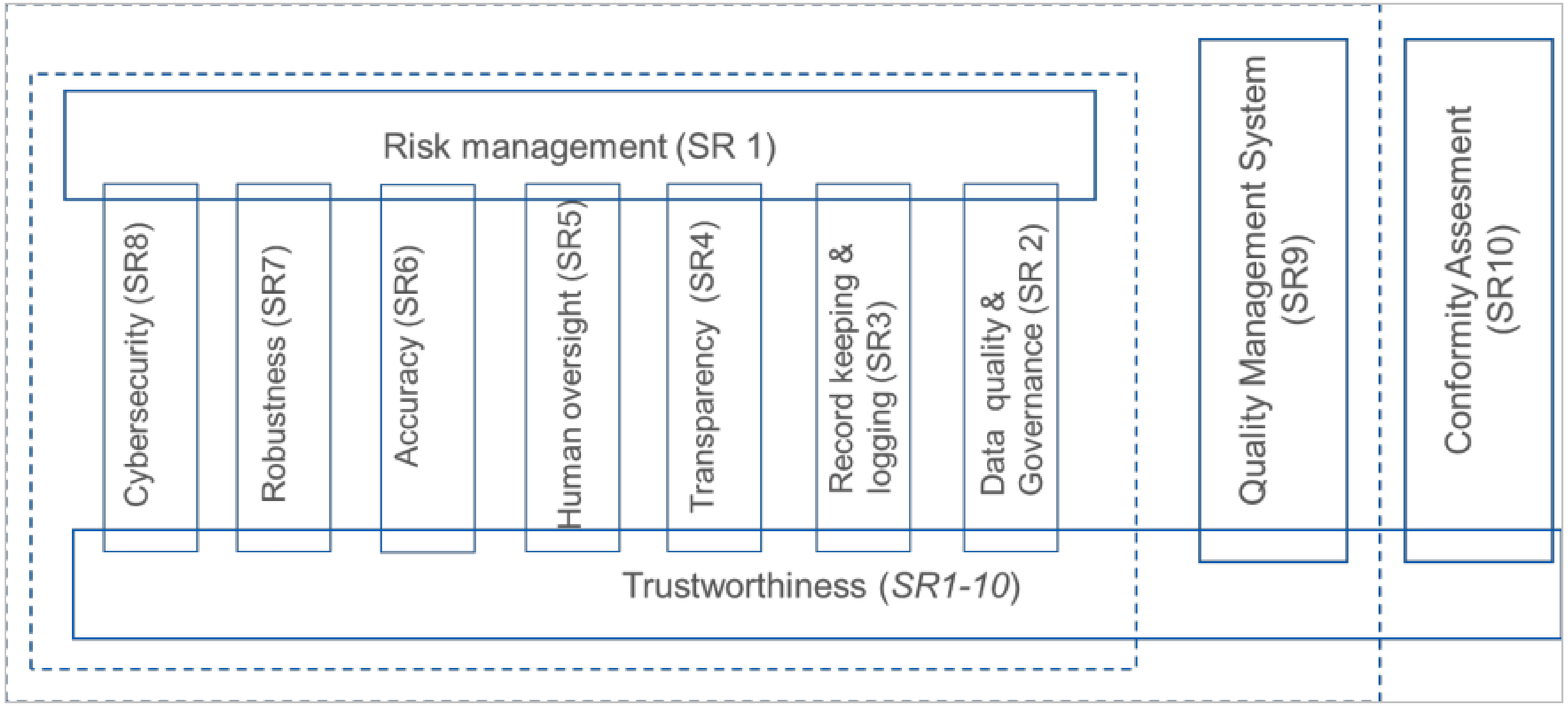
Sustainable AI:

”reporting and documentation processes to improve AI systems resource performance, such as reduction of energy and other resources consumption of the high-risk AI system during its lifecycle, and on energy efficient development of general-purpose AI models”

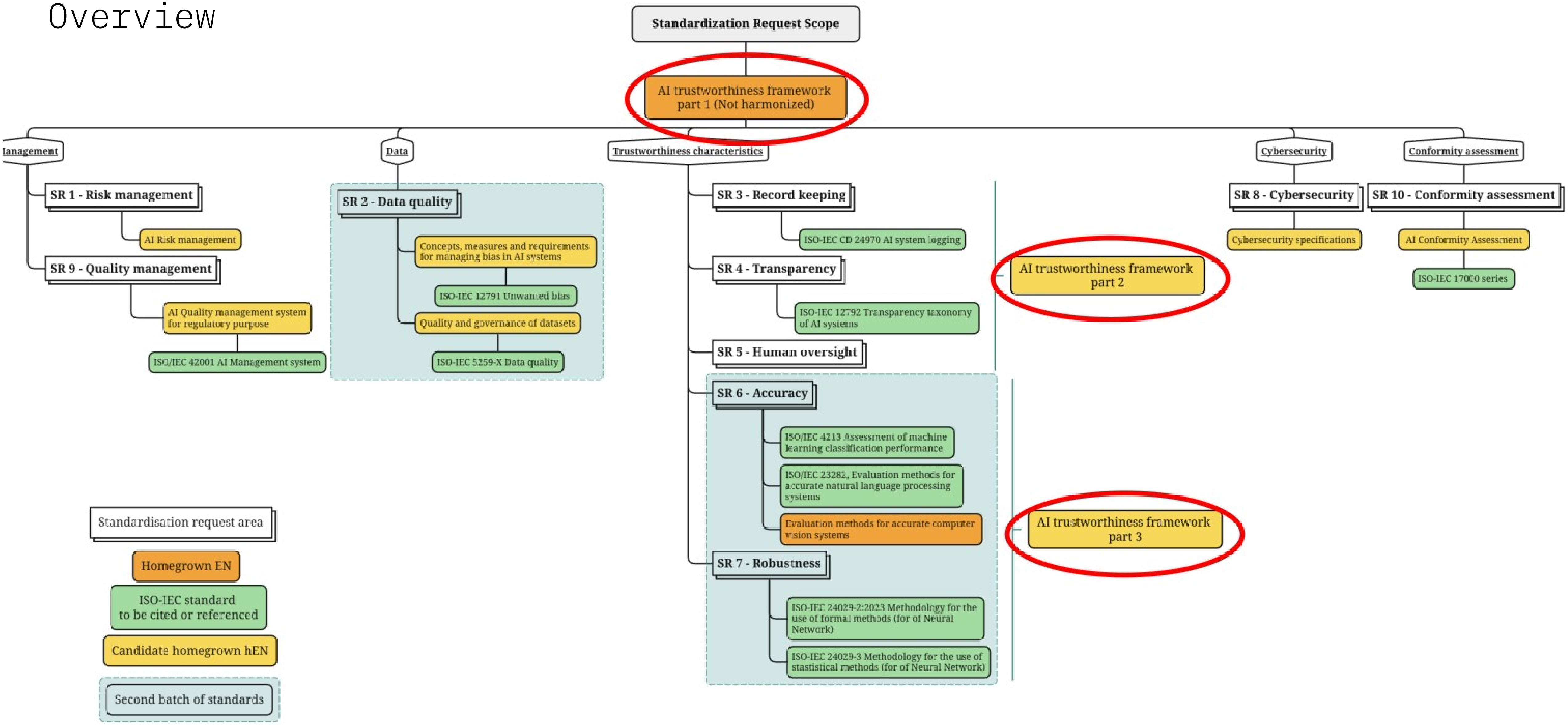
European standards supporting the transparency obligations for GPAI

Harmonised European Standards for AI

Standards intended to support the AI Act will be mapped on the following architecture of standards.



Standardisation Work – Overview



Standardization Request Scope

AI trustworthiness framework part 1 (Not harmonized)

lanagement
- SR 1 - Risk management
  - AI Risk management
- SR 9 - Quality management
  - AI Quality management system for regulatory purpose
  - ISO/IEC 42001 AI Management system

Data
- SR 2 - Data quality
  - Concepts, measures and requirements for managing bias in AI systems
  - ISO-IEC 12791 Unwanted bias
  - Quality and governance of datasets
  - ISO-IEC 5259-X Data quality

Trustworthiness characteristics
- SR 3 - Record keeping
  - ISO-IEC CD 24970 AI system logging
- SR 4 - Transparency
  - ISO-IEC 12792 Transparency taxonomy of AI systems
- SR 5 - Human oversight
- SR 6 - Accuracy
  - ISO/IEC 4213 Assessment of machine learning classification performance
  - ISO/IEC 23282, Evaluation methods for accurate natural language processing systems
  - Evaluation methods for accurate computer vision systems
- SR 7 - Robustness
  - ISO-IEC 24029-2:2023 Methodology for the use of formal methods (for of Neural Network)
  - ISO-IEC 24029-3 Methodology for the use of stastistical methods (for of Neural Network)

AI trustworthiness framework part 2

AI trustworthiness framework part 3

Cybersecurity
- SR 8 - Cybersecurity
  - Cybersecurity specifications

Conformity assessment
- SR 10 - Conformity assessment
  - AI Conformity Assessment
  - ISO-IEC 17000 series

Standardisation request area

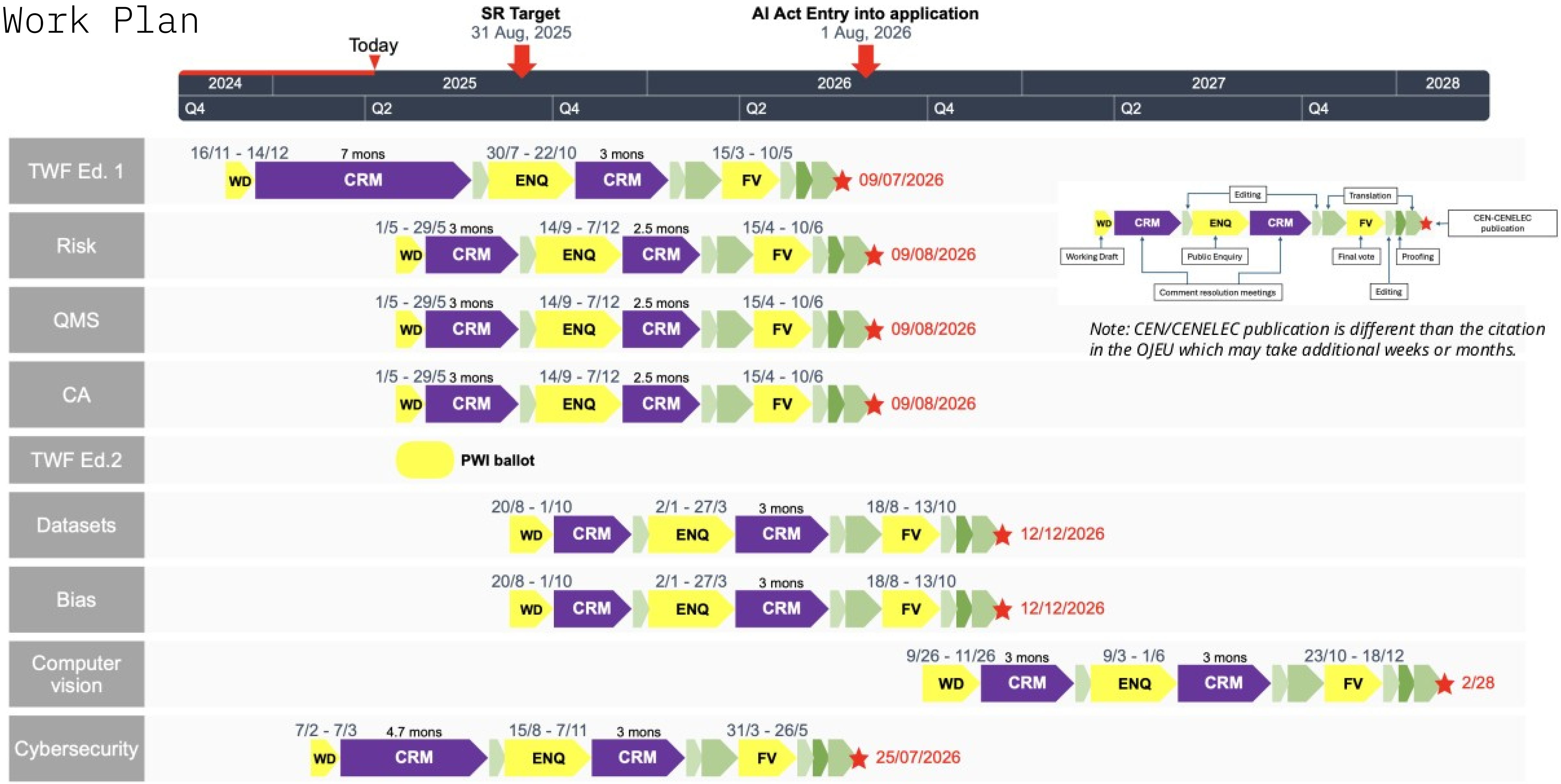
Homegrown EN

ISO-IEC standard to be cited or referenced

Candidate homegrown hEN

Second batch of standards

CEN-CENELEC Work Plan



Today

SR Target
31 Aug, 2025

AI Act Entry into application
1 Aug, 2026

2024 | 2025 | 2026 | 2027 | 2028

Q4 | Q2 | Q4 | Q2 | Q4 | Q2 | Q4

TWF Ed. 1: 16/11 - 14/12 WD; 7 mons CRM; 30/7 - 22/10 ENQ; 3 mons CRM; 15/3 - 10/5 FV; 09/07/2026

Risk: 1/5 - 29/5 WD; 3 mons CRM; 14/9 - 7/12 ENQ; 2.5 mons CRM; 15/4 - 10/6 FV; 09/08/2026

QMS: 1/5 - 29/5 WD; 3 mons CRM; 14/9 - 7/12 ENQ; 2.5 mons CRM; 15/4 - 10/6 FV; 09/08/2026

CA: 1/5 - 29/5 WD; 3 mons CRM; 14/9 - 7/12 ENQ; 2.5 mons CRM; 15/4 - 10/6 FV; 09/08/2026

TWF Ed.2: PWI ballot

Datasets: 20/8 - 1/10 WD; CRM; 2/1 - 27/3 ENQ; 3 mons CRM; 18/8 - 13/10 FV; 12/12/2026

Bias: 20/8 - 1/10 WD; CRM; 2/1 - 27/3 ENQ; 3 mons CRM; 18/8 - 13/10 FV; 12/12/2026

Computer vision: 9/26 - 11/26 WD; 3 mons CRM; 9/3 - 1/6 ENQ; 3 mons CRM; 23/10 - 18/12 FV; 2/28

Cybersecurity: 7/2 - 7/3 WD; 4.7 mons CRM; 15/8 - 7/11 ENQ; 3 mons CRM; 31/3 - 26/5 FV; 25/07/2026

WD – Working Draft; CRM; ENQ – Public Enquiry; CRM; FV – Final vote; CEN-CENELEC publication

Editing

Translation

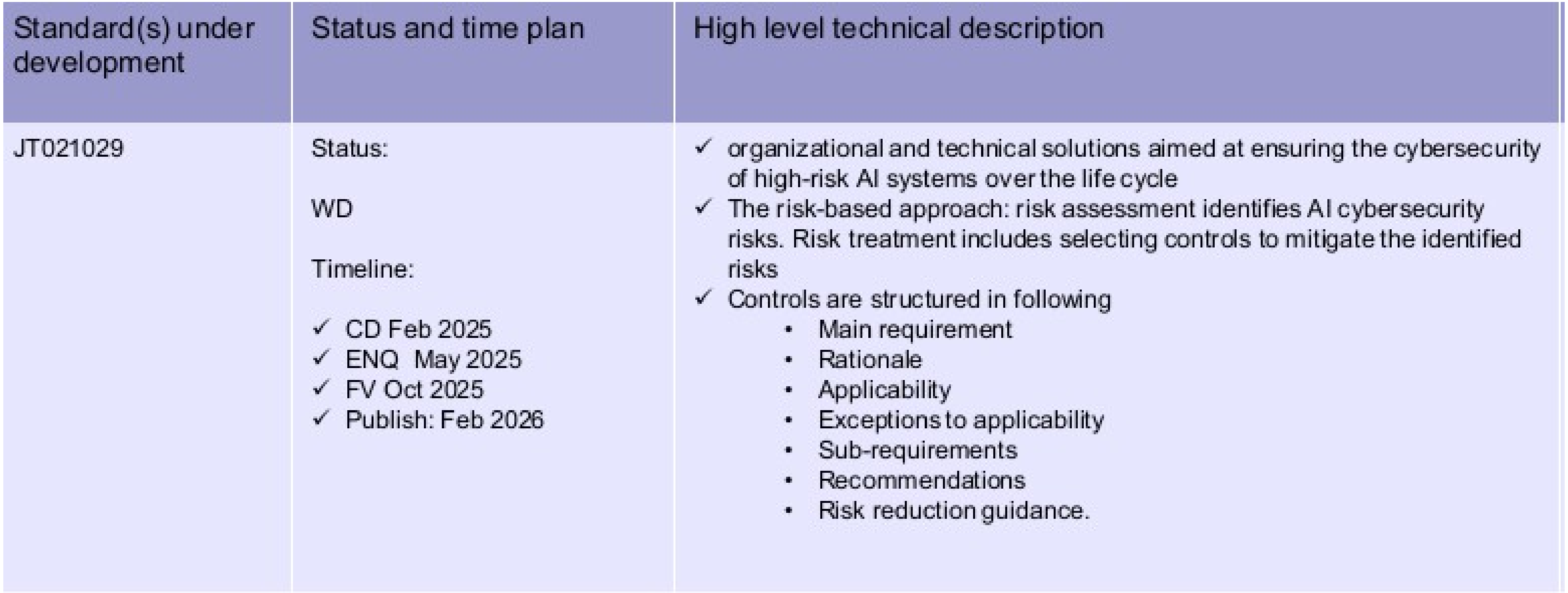
Comment resolution meetings

Editing

Proofing

Note: CEN/CENELEC publication is different than the citation in the OJEU which may take additional weeks or months.

Postcard: Cybersecurity for AI Systems



Standard(s) under development	Status and time plan	High level technical description
JT021029	Status: WD Timeline: ✓ CD Feb 2025 ✓ ENQ May 2025 ✓ FV Oct 2025 ✓ Publish: Feb 2026	✓ organizational and technical solutions aimed at ensuring the cybersecurity of high-risk AI systems over the life cycle ✓ The risk-based approach: risk assessment identifies AI cybersecurity risks. Risk treatment includes selecting controls to mitigate the identified risks ✓ Controls are structured in following • Main requirement • Rationale • Applicability • Exceptions to applicability • Sub-requirements • Recommendations • Risk reduction guidance.

Will the matter with the standards work out?

starting point

AI Act and harmonised standards for compliance – new territory. Initial slow progress, (too) many discussions, etc.

situation

Standardisation process needs time and means lot of effort.

Some standards may be late.

Many drafts are too complex and, in their current way, not implementable by industry.

Some rigour needs to be applied in the coming weeks to get things right.

risk

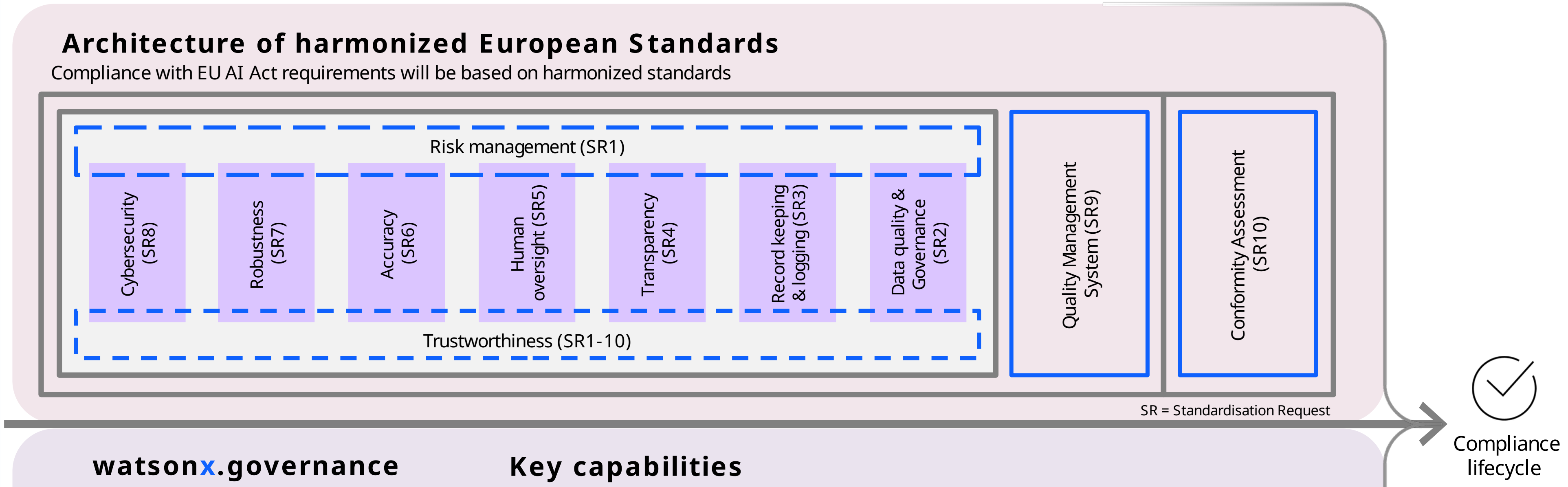
Standards may not be available in time or not listed in the Official Journal of the EU.

Market surveillance need to give some directions for this likely situation.

IBM governance tools aligned with European standards

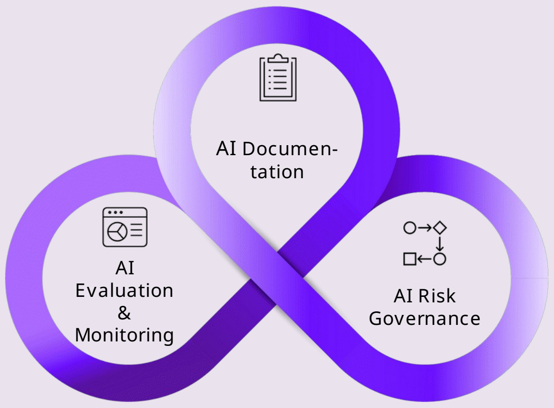
IBM's watsonx.governance toolset is informed by the technical requirements laid down in the harmonised European standards under development.

watsonx.governance enables performing the respective system management tasks, tests and lifecycle monitoring, inter alia by providing comprehensive dashboards.



Architecture of harmonized European Standards
Compliance with EU AI Act requirements will be based on harmonized standards
Risk management (SR1)
Cybersecurity (SR8)
Robustness (SR7)
Accuracy (SR6)
Human oversight (SR5)
Transparency (SR4)
Record keeping & logging (SR3)
Data quality & Governance (SR2)
Trustworthiness (SR1-10)
Quality Management System (SR9)
Conformity Assessment (SR10)
SR = Standardisation Request
Compliance lifecycle

watsonx.governance



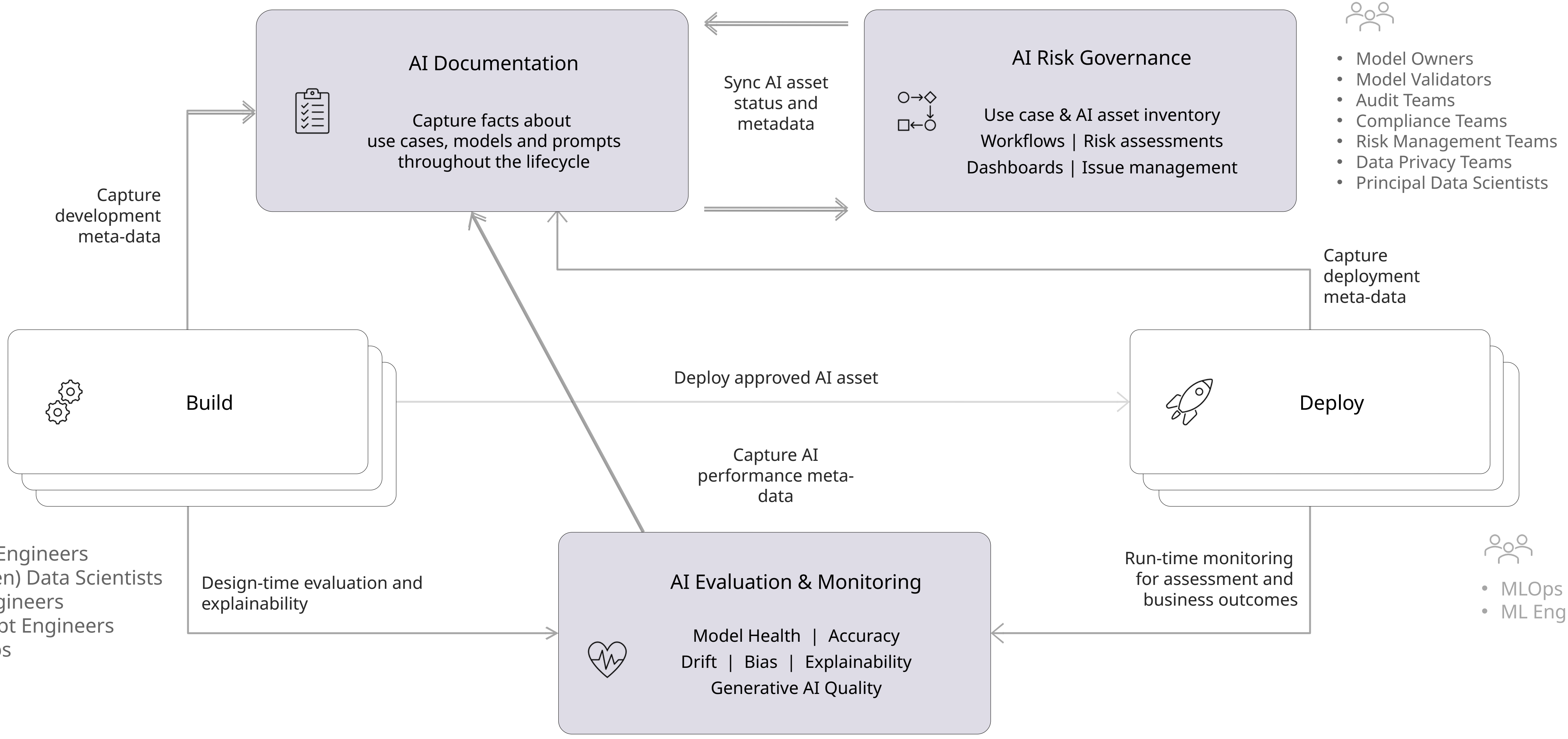
Key capabilities

Compliance – help manage AI transparency and address compliance with policies and standards. Connect data to key risk controls and use factsheets to help with capture and reporting of model metadata in support of inquiries and audits.

Risk management – preset thresholds, helping to proactively detect and mitigate AI model risks. Monitor for fairness, drift, bias, performance against evaluation metrics, instances of toxic language, and for personally identifiable information (PII). Gain insights into organizational risk with user-based dashboards and reports.

Lifecycle governance – help govern both generative AI and predictive machine learning models across the lifecycle using integrated workflows and approvals, monitor the status of use cases, in-process change requests, challenges, issues and assigned tasks.

watsonx.governance - conceptual mapping of potentially relevant provisions of the EU AI Act



AI Documentation

Capture facts about use cases, models and prompts throughout the lifecycle

Sync AI asset status and metadata

AI Risk Governance

Use case & AI asset inventory

Workflows | Risk assessments

Dashboards | Issue management

- Model Owners
- Model Validators
- Audit Teams
- Compliance Teams
- Risk Management Teams
- Data Privacy Teams
- Principal Data Scientists

Capture development meta-data

Capture deployment meta-data

Build

Deploy approved AI asset

Deploy

Capture AI performance meta-data

- Data Engineers
- (Citizen) Data Scientists
- AI Engineers
- Prompt Engineers
- MLOps

Design-time evaluation and explainability

AI Evaluation & Monitoring

Model Health | Accuracy

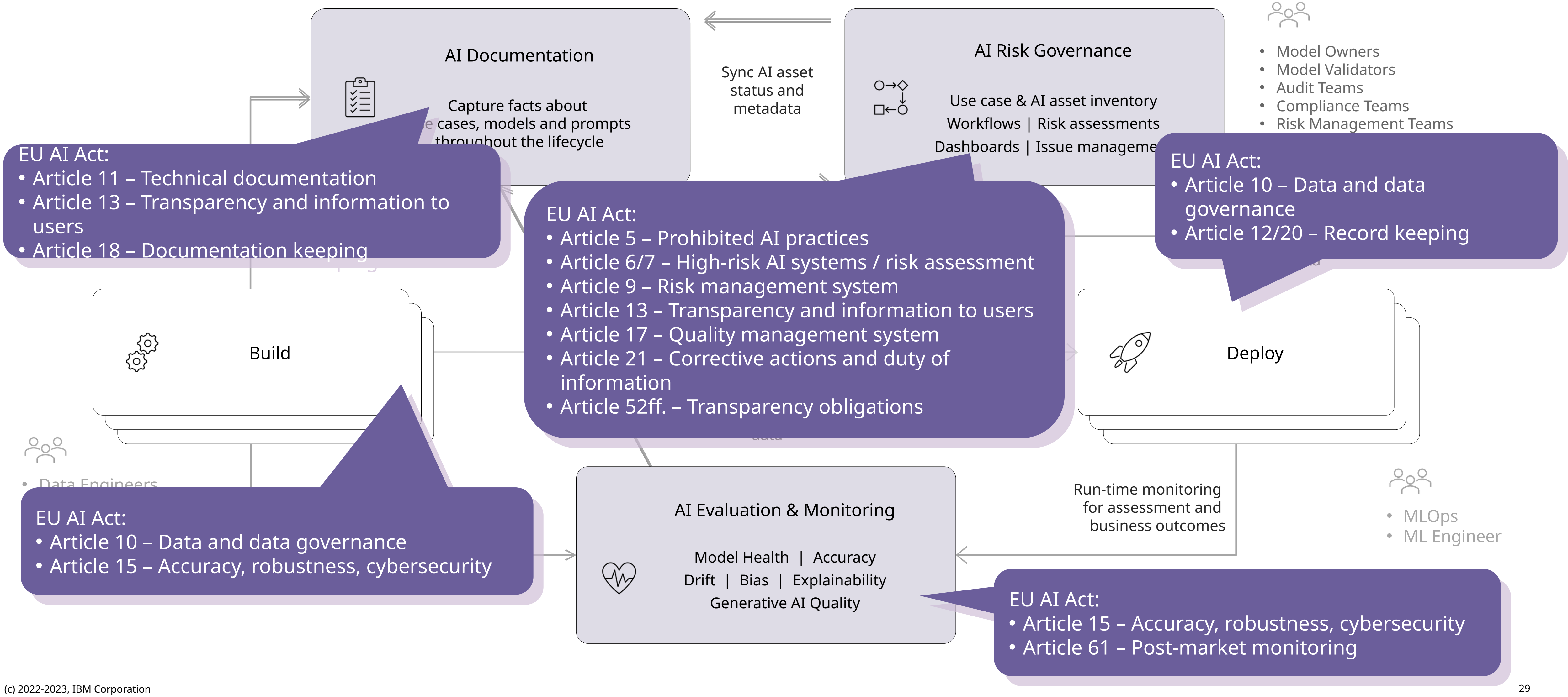
Drift | Bias | Explainability

Generative AI Quality

Run-time monitoring for assessment and business outcomes

- MLOps
- ML Engineer

watsonx.governance - conceptual mapping of potentially relevant provisions of the EU AI Act



AI Documentation

Capture facts about use cases, models and prompts throughout the lifecycle

Sync AI asset status and metadata

AI Risk Governance

Use case & AI asset inventory

Workflows | Risk assessments

Dashboards | Issue manageme

- Model Owners
- Model Validators
- Audit Teams
- Compliance Teams
- Risk Management Teams

EU AI Act:
- Article 11 – Technical documentation
- Article 13 – Transparency and information to users
- Article 18 – Documentation keeping

EU AI Act:
- Article 5 – Prohibited AI practices
- Article 6/7 – High-risk AI systems / risk assessment
- Article 9 – Risk management system
- Article 13 – Transparency and information to users
- Article 17 – Quality management system
- Article 21 – Corrective actions and duty of information
- Article 52ff. – Transparency obligations

EU AI Act:
- Article 10 – Data and data governance
- Article 12/20 – Record keeping

Build

Deploy

- Data Engineers

EU AI Act:
- Article 10 – Data and data governance
- Article 15 – Accuracy, robustness, cybersecurity

AI Evaluation & Monitoring

Model Health | Accuracy

Drift | Bias | Explainability

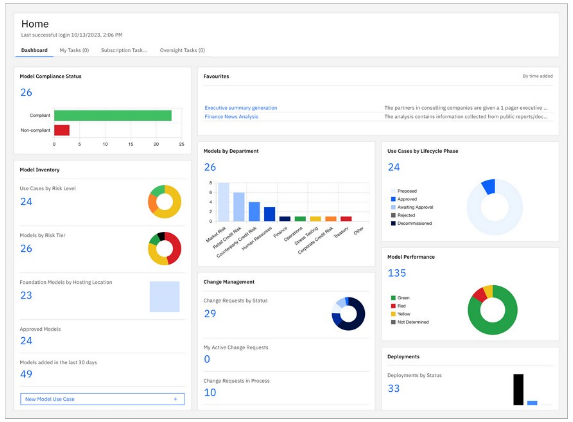
Generative AI Quality

Run-time monitoring for assessment and business outcomes

- MLOps
- ML Engineer

EU AI Act:
- Article 15 – Accuracy, robustness, cybersecurity
- Article 61 – Post-market monitoring

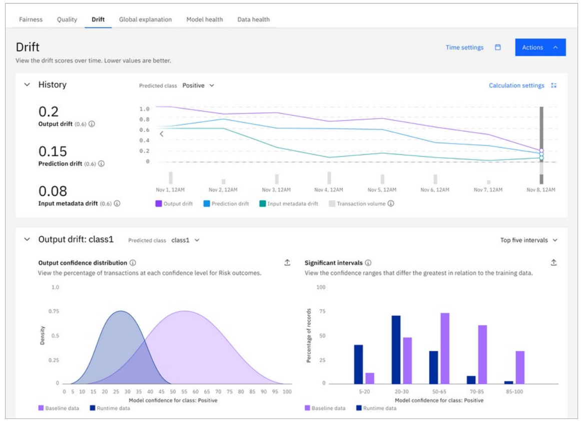
watsonx.governance support for compliance with the EU AI Act



Last successful login 10/13/2023, 2:06 PM

The partners in consulting companies are given a 1 pager executive ...

The analysis contains information collected from public reports/doc...



View the drift scores over time. Lower values are better.

View the percentage of transactions at each confidence level for Risk outcomes.

View the confidence ranges that differ the greatest in relation to the training data.

Applicability and Risk Categorisations

[Articles 5,6,7]

Watsonx.governance provides EU AI Applicability and Risk Categorisation Assessment Questionaire. Updates on the act will be considered via regularly provided updates on these questionaires.

 Governance Console

Compliance Requirements for High-Risk AI Systems

[Article 8]

watsonx.governance is a compliance tracking system that monitors and ensures adherence to the EU AI Act and other relevant regulations including a unified documentation and reporting system

 Governance Console, AI Documentation

Risk management system for high-risk AI systems

[Article 9]

watsonx.governance is a comprehensive risk management system for AI systems, identifying, analyzing, estimating, and evaluating risks, as well as adopting appropriate risk management measures.

 Governance Console

Need for high-quality data sets and robust data governance practices

[Article 10]

Part of the development process identify bias in training data etc.

 Evaluation & Monitoring

Technical documentation

[Article 11]

Workflows in the Governance console ensure the documentation is in place before a model is put into production. All metadata of a model and its development and monitoring activities are automatically captured in the AI factsheet.

 Governance Console, AI Documentation

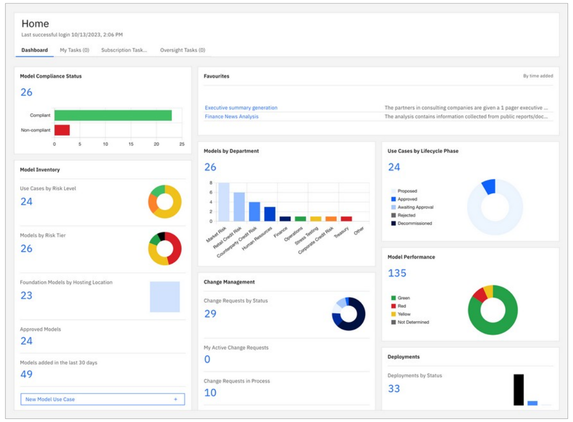
Record-keeping

[Article 12, 20]

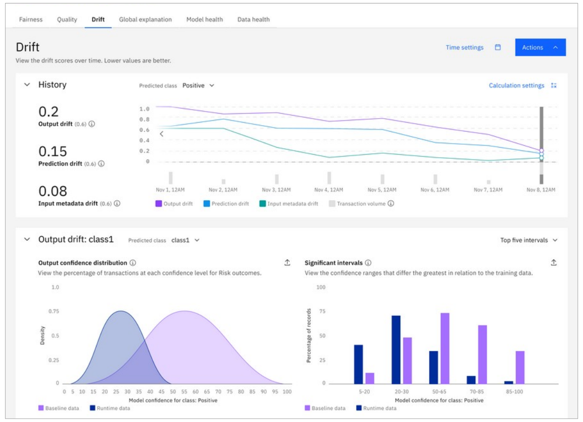
Model inferences are logged through the Monitoring service, regardless of the deployment environment, in order to record risk-related events and increase transparency

 Evaluation & Monitoring

watsonx.governance support for compliance with the EU AI Act



Executive summary generation	The partners in consulting companies are given a 1 pager executive ...
Finance News Analysis	The analysis contains information collected from public reports/doc...



View the drift scores over time. Lower values are better.

View the percentage of transactions at each confidence level for Risk outcomes.

View the confidence ranges that differ the greatest in relation to the training data.

Transparency and Provision of Information to Deployers of High-Risk AI Systems

[Article 13]

Model cards (watsonx.ai)

Human Oversight of High-Risk AI Systems

[Article 14]

watsonx.governance allows effective oversight by humans during their use of high-risk systems

 Governance Console

Accuracy, robustness and cybersecurity

[Article 15]

Monitor for various accuracy metrics through the model lifecycle, preventing drift and bias

 Evaluation & Monitoring

Documentation keeping

[Article 18]

AI factsheets remain in the system through the lifecycle of a use case and can be exported as PDF documents to be stored in dedicated folders / archives

 AI Documentation

Intermediate Summarising Remarks

Deep involvement and high investment of IBM into European and international standardisation bringing in our experience on trustworthy AI.

IBM has decade-long experience with the EU regulatory system, the New Legislative Framework and the use of harmonised European standards for compliance.

Standards required for compliance with the AI Act are under way with a clear work and time plan.

It must be expected that some standards or their citation on the OJEU will be late – market surveillance authorities should provide guidance and solutions for this case.

IBM has knowledge of evolving AI standards and is able to provide optimal support to clients on this basis.

IBM’s tools are informed by the requirements laid down in the AI Act and the standards for supporting good governance of AI systems.

ISO 42001 – Not for compliance with the EU AI Act

ISO 42001 is a “Management System Standard” intended for certification (similar to ISO 9001 or ISO 27001).

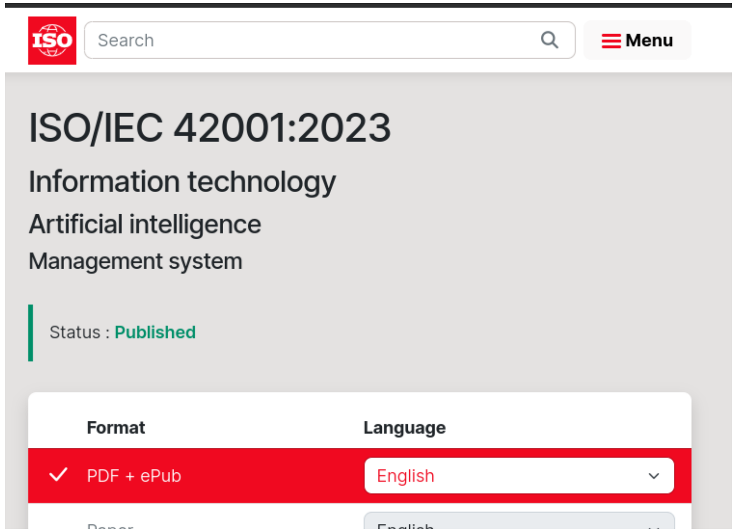
It sets certain controls around trustworthiness, governance and responsible AI that an organisation should fulfil – but not specific for high-risk AI systems.

The European Commission made very clear that ISO 42001 is not suitable for meeting the requirements of the EU AI Act:

“[42001’s] primary objective is to help organisations manage uncertainty in line with their own organisational and business goals, rather than to ensure a high level of protection for health, safety, and fundamental rights as required by AI Act.

“While recognising the differences between medical devices and the AI systems, EN ISO 13485 offers a regulatory logic, conceptual framework and structure that is more closely aligned to new legislative framework and the AI Act (e.g. on the definition of risk, and safety objectives) than ISO/IEC 42001.”

[From a recent submission of the European Commission to CEN-CENELEC JTC 21.]



ISO/IEC 42001:2023

Information technology

Artificial intelligence

Management system

Status : Published

Format	Language
✓ PDF + ePub	English

Many thanks for your attention…

… handing over to Monica

Dr. Jochen Friedrich

jochen@de.ibm.com
https://www.linkedin.com/in/jochenfriedrich/