

AI Risk Assessment: First Steps

Digital Health Week
Live Online Event
7 November 2024, 1-2 PM
Claudia Otto, COT Legal



Agenda

- I. The EU AI Act
- II. Relationship AI Act / ISO standards
- III. Risk Management under the AI Act
- IV. AI Risk Assessment
- V. First steps
- VI. Q&A

I. The EU AI Act...

1. ... is a Regulation

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)

PE/24/2024/REV/1

OJ L, 2024/1689, 12.7.2024, ELI: <http://data.europa.eu/eli/reg/2024/1689/oj> (BG, ES, CS, DA, DE, ET, EL, EN, FR, GA, HR, IT, LV, LT, HU, MT, NL, PL, PT, RO, SK, SL, FI, SV)

● In force

ELI: <http://data.europa.eu/eli/reg/2024/1689/oj>

That means: It is binding and directly applicable.

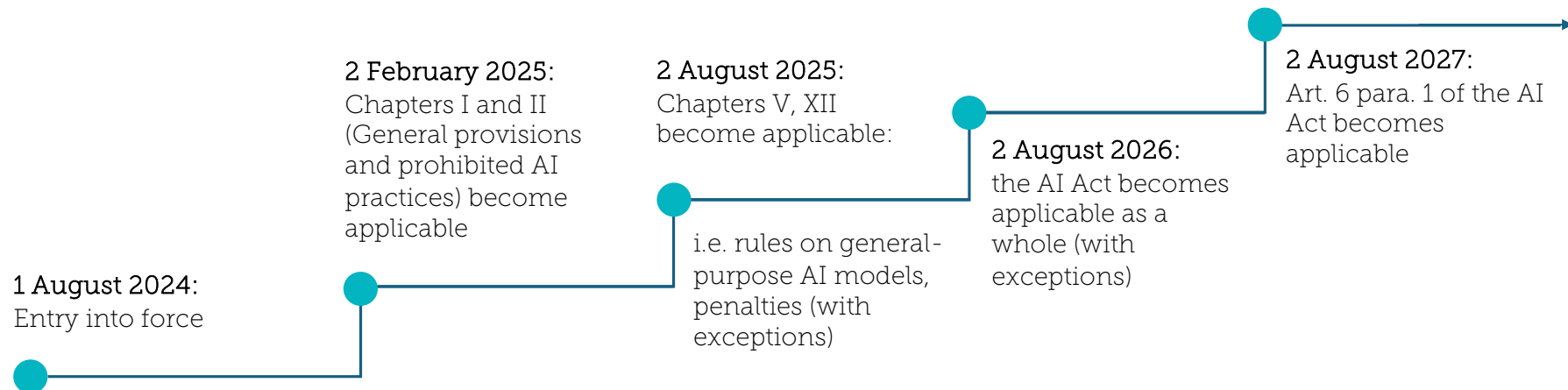
I. The EU AI Act...

1. ... is a Regulation, i.e., binding and directly applicable
2. ... came into force on 1 August 2024



I. The EU AI Act...

1. ... is a Regulation, i.e., binding and directly applicable
2. ... came into force on 1 August 2024
3. ... applies gradually according to Art. 113 of the AI Act:



I. The EU AI Act...

1. ... is a Regulation, i.e., binding and directly applicable
2. ... came into force on 1 August 2024
3. ... applies gradually according to Art. 113 of the AI Act
4. ... does not regulate AI

I. The EU AI Act...

1. ... is a Regulation, i.e., binding and directly applicable
2. ... came into force on 1 August 2024
3. ... applies gradually according to Art. 113 of the AI Act
4. ... does not regulate AI



Wait. WHAT?!

4. The EU AI Act does not regulate AI...

...only rights and obligations with regard to certain AI systems and general-purpose AI models.

Recital 4, 138

„AI is a fast evolving family of technologies“

Art. 3 (1): AI system

“a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments”

Art. 3 (63): general-purpose AI model

“an AI model, including where such an AI model is trained with a large amount of data using self-supervision at scale, that displays significant generality and is capable of competently performing a wide range of distinct tasks regardless of the way the model is placed on the market and that can be integrated into a variety of downstream systems or applications, except AI models that are used for research, development or prototyping activities before they are placed on the market”

4. The EU AI Act does not regulate AI...

...only rights and obligations with regard to certain AI systems and general-purpose AI models.

The definitions are descriptive and based on human perception, not on technical details.

Why? The AI Act is technologically neutral, i.e., it makes circumvention less easy.

Art. 3 (1): AI system

"a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments"

Art. 3 (63): general-purpose AI model

"an AI model, including where such an AI model is trained with a large amount of data using self-supervision at scale, that displays significant generality and is capable of competently performing a wide range of distinct tasks regardless of the way the model is placed on the market and that can be integrated into a variety of downstream systems or applications, except AI models that are used for research, development or prototyping activities before they are placed on the market"

I. The EU AI Act...

1. ... is a Regulation, i.e., binding and directly applicable
2. ... came into force on 1 August 2024
3. ... applies gradually according to Art. 113 of the AI Act
4. ... does not regulate AI
5. ... does not require AI trainings and AI expertise

I. The EU AI Act...

1. ... is a Regulation, i.e., binding and directly applicable
2. ... came into force on 1 August 2024
3. ... applies gradually according to Art. 113 of the AI Act
4. ... does not regulate AI
5. ... does not require AI trainings and AI expertise



But-but on
LinkedIn they
say...

5. AI Literacy (Chapter I, Art. 4 AI Act)...

...does not mean that you must be an expert or must train your employees to be "AI experts" by or after 2 February 2025:

Article 4

AI literacy

Providers and deployers of AI systems shall take measures to ensure, to their best extent, a sufficient level of AI literacy of their staff and other persons dealing with the operation and use of AI systems on their behalf, taking into account their technical knowledge, experience, education and training and the context the AI systems are to be used in, and considering the persons or groups of persons on whom the AI systems are to be used.

5. AI Literacy (Chapter I, Art. 4 AI Act)...

...does not mean that you must be an expert or must train your employees to be "AI experts" by or after 2 February 2025:

Article 4

AI literacy

Providers and deployers of AI systems shall take measures to ensure, to their best extent, a sufficient level of AI literacy of their staff and other persons dealing with the operation and use of AI systems on their behalf, taking into account their technical knowledge, experience, education and training and the context the AI systems are to be used in, and considering the persons or groups of persons on whom the AI systems are to be used.

Article 3 (definitions)

(56) 'AI literacy' means skills, knowledge and understanding that allow providers, deployers and affected persons, taking into account their respective rights and obligations in the context of this Regulation, to make an informed deployment of AI systems, as well as to gain awareness about the opportunities and risks of AI and possible harm it can cause;

5. AI Literacy (Chapter I, Art. 4 AI Act)...

...does not mean that you must be an expert or must train your employees to be "AI experts" by or after 2 February 2025:

Article 4

AI literacy

Providers and deployers of AI systems shall take measures to ensure, to their best extent, a sufficient level of AI literacy of their staff and other persons dealing with the operation and use of AI systems on their behalf, taking into account their technical knowledge, experience, education and training and the context the AI systems are to be used in, and considering the persons or groups of persons on whom the AI systems are to be used.

Article 3 (definitions)

(56) 'AI literacy' means skills, knowledge and understanding that allow providers, deployers and affected persons, taking into account their respective rights and obligations in the context of this Regulation, to make an informed deployment of AI systems, as well as to gain awareness about the opportunities and risks of AI and possible harm it can cause;

5. AI Literacy (Chapter I, Art. 4 AI Act)...

...does not mean that you must be an expert or must train your employees to be "AI experts" by or after 2 February 2025:

Article 4

AI literacy

Providers and deployers of AI systems shall take measures to ensure, to their best extent, a sufficient level of AI literacy of their staff and other persons dealing with the operation and use of AI systems on their behalf, taking into account their technical knowledge, experience, education and training and the context the AI systems are to be used in, and considering the persons or groups of persons on whom the AI systems are to be used.

Article 3 (definitions)

(56) 'AI literacy' means skills, knowledge and understanding that allow providers, deployers and affected persons, taking into account their respective rights and obligations in the context of this Regulation, to make an informed deployment of AI systems, as well as to gain awareness about the opportunities and risks of AI and possible harm it can cause;

It neither applies to AI in general (i.e. the "fast evolving family of technologies") nor general-purpose AI models!

5. AI Literacy (Chapter I, Art. 4 AI Act)...

...does not mean that you must be an expert or must train your employees to be "AI experts" by or after 2 February 2025:

Article 4

AI literacy

Providers and deployers of AI systems shall take measures to ensure, to their best extent, a sufficient level of AI literacy of their staff and other persons dealing with the operation and use of AI systems on their behalf, taking into account their technical knowledge, experience, education and training and the context the AI systems are to be used in, and considering the persons or groups of persons on whom the AI systems are to be used.

Article 3 (definitions)

(56) 'AI literacy' means skills, knowledge and understanding that allow providers, deployers and affected persons, taking into account their respective rights and obligations in the context of this Regulation, to make an informed deployment of AI systems, as well as to gain awareness about the opportunities and risks of AI and possible harm it can cause;

5. AI Literacy (Chapter I, Art. 4 AI Act)...

...does not mean that you must be an expert or must train your employees to be "AI experts" by or after 2 February 2025:

Article 4

AI literacy

Providers and deployers of AI systems shall take measures to ensure, to their best extent, a sufficient level of AI literacy of their staff and other persons dealing with the operation and use of AI systems on their behalf, taking into account their technical knowledge, experience, education and training and the context the AI systems are to be used in, and considering the persons or groups of persons on whom the AI systems are to be used.

Measures can be anything that ensures ...

Article 3 (definitions)

(56) 'AI literacy' means skills, knowledge and understanding that allow providers, deployers and affected persons, taking into account their respective rights and obligations in the context of this Regulation, to make an informed deployment of AI systems, as well as to gain awareness about the opportunities and risks of AI and possible harm it can cause;

5. AI Literacy (Chapter I, Art. 4 AI Act)...

...does not mean that you must be an expert or must train your employees to be "AI experts" by or after 2 February 2025:

Article 4

AI literacy

Providers and deployers of AI systems shall take measures to ensure, to their best extent, a sufficient level of AI literacy of their staff and other persons dealing with the operation and use of AI systems on their behalf, taking into account their technical knowledge, experience, education and training and the context the AI systems are to be used in, and considering the persons or groups of persons on whom the AI systems are to be used.

Measures can be anything that ensures a sufficient level of AI literacy.

Article 3 (definitions)

(56) 'AI literacy' means skills, knowledge and understanding that allow providers, deployers and affected persons, taking into account their respective rights and obligations in the context of this Regulation, to make an informed deployment of AI systems, as well as to gain awareness about the opportunities and risks of AI and possible harm it can cause;

5. AI Literacy (Chapter I, Art. 4 AI Act)...

...does not mean that you must be an expert or must train your employees to be "AI experts" by or after 2 February 2025:

Article 4

AI literacy

Providers and deployers of AI systems shall take measures to ensure, to their best extent, a sufficient level of AI literacy of their staff and other persons dealing with the operation and use of AI systems on their behalf, taking into account their technical knowledge, experience, education and training and the context the AI systems are to be used in, and considering the persons or groups of persons on whom the AI systems are to be used.

How to "ensure a sufficient level to best extent"?

Article 3 (definitions)

(56) 'AI literacy' means skills, knowledge and understanding that allow providers, deployers and affected persons, taking into account their respective rights and obligations in the context of this Regulation, to make an informed deployment of AI systems, as well as to gain awareness about the opportunities and risks of AI and possible harm it can cause;

5. AI Literacy (Chapter I, Art. 4 AI Act)...

...does not mean that you must be an expert or must train your employees to be "AI experts" by or after 2 February 2025:

Article 4

AI literacy

Providers and deployers of AI systems shall take measures to ensure, to their best extent, a sufficient level of AI literacy of their staff and other persons dealing with the operation and use of AI systems on their behalf, taking into account their technical knowledge, experience, education and training and the context the AI systems are to be used in, and considering the persons or groups of persons on whom the AI systems are to be used.

There are no clear instructions!

Article 3 (definitions)

(56) 'AI literacy' means skills, knowledge and understanding that allow providers, deployers and affected persons, taking into account their respective rights and obligations in the context of this Regulation, to make an informed deployment of AI systems, as well as to gain awareness about the opportunities and risks of AI and possible harm it can cause;

5. AI Literacy (Chapter I, Art. 4 AI Act)...

...does not mean that you must be an expert or must train your employees to be "AI experts" by or after 2 February 2025:

Article 4

AI literacy

Providers and deployers of AI systems shall take measures to ensure, to their best extent, a sufficient level of AI literacy of their staff and other persons dealing with the operation and use of AI systems on their behalf, taking into account their technical knowledge, experience, education and training and the context the AI systems are to be used in, and considering the persons or groups of persons on whom the AI systems are to be used.

Article 3 (definitions)

(56) 'AI literacy' means skills, knowledge and understanding that allow providers, deployers and affected persons, taking into account their respective rights and obligations in the context of this Regulation, to make an informed deployment of AI systems, as well as to gain awareness about the opportunities and risks of AI and possible harm it can cause;

However, we know
the goal!

5. AI Literacy (Chapter I, Art. 4 AI Act)...

...does not mean that you must be an expert or must train your employees to be "AI experts" by or after 2 February 2025:

Article 4

AI literacy

Providers and deployers of AI systems shall take measures to ensure, to their best extent, a sufficient level of AI literacy of their staff and other persons dealing with the operation and use of AI systems on their behalf, taking into account their technical knowledge, experience, education and training and the context the AI systems are to be used in, and considering the persons or groups of persons on whom the AI systems are to be used.

Article 3 (definitions)

(56) 'AI literacy' means skills, knowledge and understanding that allow providers, deployers and affected persons, taking into account their respective rights and obligations in the context of this Regulation, to make an informed deployment of AI systems, as well as to gain awareness about the opportunities and risks of AI and possible harm it can cause;

...to ensure, that obligations are fulfilled and rights, risks are being taken care of

5. AI Literacy (Chapter I, Art. 4 AI Act)...

...does not mean that you must be an expert or must train your employees to be "AI experts" by or after 2 February 2025:

Article 4

AI literacy

Providers and deployers of AI systems shall take measures to ensure, to their best extent, a sufficient level of AI literacy of their staff and other persons dealing with the operation and use of AI systems on their behalf, taking into account their technical knowledge, experience, education and training and the context the AI systems are to be used in, and considering the persons or groups of persons on whom the AI systems are to be used.

Article 3 (definitions)

(56) 'AI literacy' means skills, knowledge and understanding that allow providers, deployers and affected persons, taking into account their respective rights and obligations in the context of this Regulation, to make an informed deployment of AI systems, as well as to gain awareness about the opportunities and risks of AI and possible harm it can cause;

...in particular

RISKS

5. AI Literacy (Chapter I, Art. 4 AI Act)...

...does not mean that you must be an expert or must train your employees to be "AI experts" by or after 2 February 2025:

Article 4

AI literacy

Providers and deployers of AI systems shall take measures to ensure, to their best extent, a sufficient level of AI literacy of their staff and other persons dealing with the operation and use of AI systems on their behalf, taking into account their technical knowledge, experience, education and training and the context the AI systems are to be used in, and considering the persons or groups of persons on whom the AI systems are to be used.

Achieving AI Literacy means different measures for each provider or deployer. They must be determined individually.

5. AI Literacy (Chapter I, Art. 4 AI Act)...

...does not mean that you must be an expert or must train your employees to be "AI experts" by or after 2 February 2025:

Article 4

AI literacy

Providers and deployers of AI systems shall take measures to ensure, to their best extent, a sufficient level of AI literacy of their staff and other persons dealing with the operation and use of AI systems on their behalf, taking into account their technical knowledge, experience, education and training and the context the AI systems are to be used in, and considering the persons or groups of persons on whom the AI systems are to be used.

Due to this "need for customization", there is no corresponding penalty provision. You cannot violate Art. 4 of the AI Act. However, if the obligations referenced in Art. 99 of the AI Act are violated due to lack of AI Literacy, a penalty is possible – and "we didn't know" is not a defense.

5. AI Literacy (Chapter I, Art. 4 AI Act)...

...is necessary to understand the harms and risks related to AI systems

Article 4

AI literacy

Providers and deployers of AI systems shall take measures to ensure, to their best extent, a sufficient level of AI literacy of their staff and other persons dealing with the operation and use of AI systems on their behalf, taking into account their technical knowledge, experience, education and training and the context the AI systems are to be used in, and considering the persons or groups of persons on whom the AI systems are to be used.

What's a good way to start complying?

Having a concept of measures within the meaning of Art. 4 of the AI Act ready by 2 February 2025 is a good start!

5. AI Literacy (Chapter I, Art. 4 AI Act)...

What is a concept of measures within the meaning of Art. 4?

5. AI Literacy (Chapter I, Art. 4 AI Act)...

What is a concept of measures within the meaning of Art. 4?

It's a plan.

5. AI Literacy (Chapter I, Art. 4 AI Act)...

What is a concept of measures within the meaning of Art. 4?



5. AI Literacy (Chapter I, Art. 4 AI Act)...

What is a concept of measures within the meaning of Art. 4?

The concept of measures depends on the properties of the AI system(s) dealt with.



5. AI Literacy (Chapter I, Art. 4 AI Act)...

What is a concept of measures within the meaning of Art. 4?

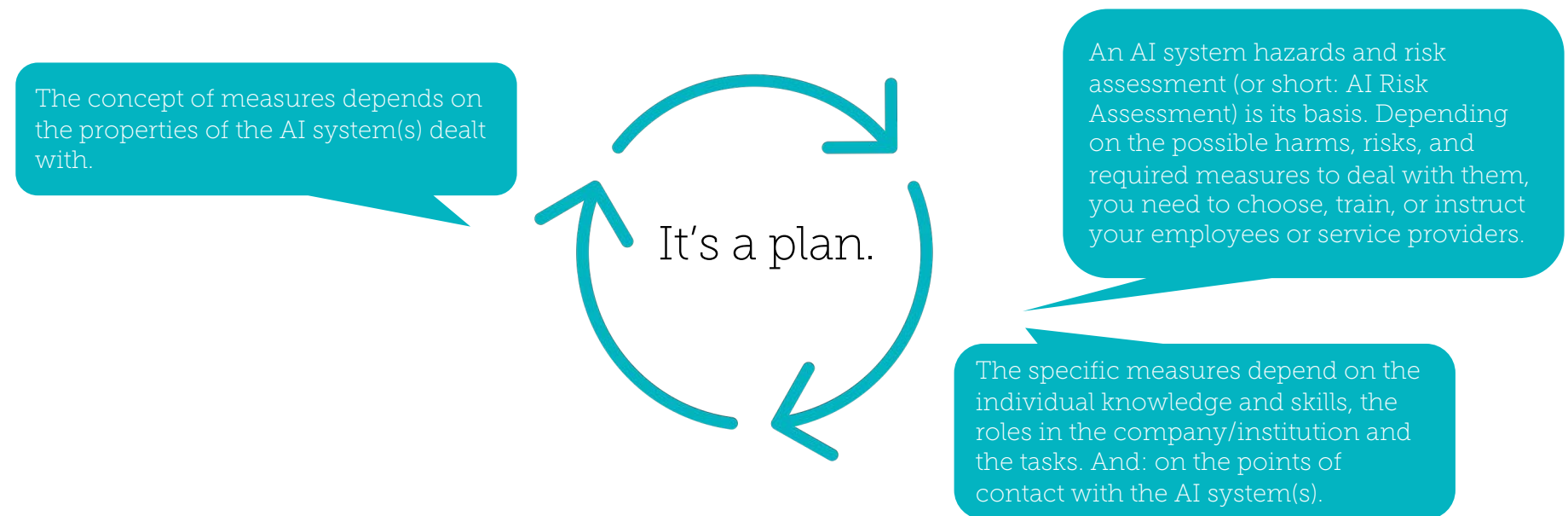
The concept of measures depends on the properties of the AI system(s) dealt with.

It's a plan.

An AI system hazards and risk assessment (or short: AI Risk Assessment) is its basis. Depending on the possible harms, risks, and required measures to deal with them, you need to choose, train, or instruct your employees or service providers.

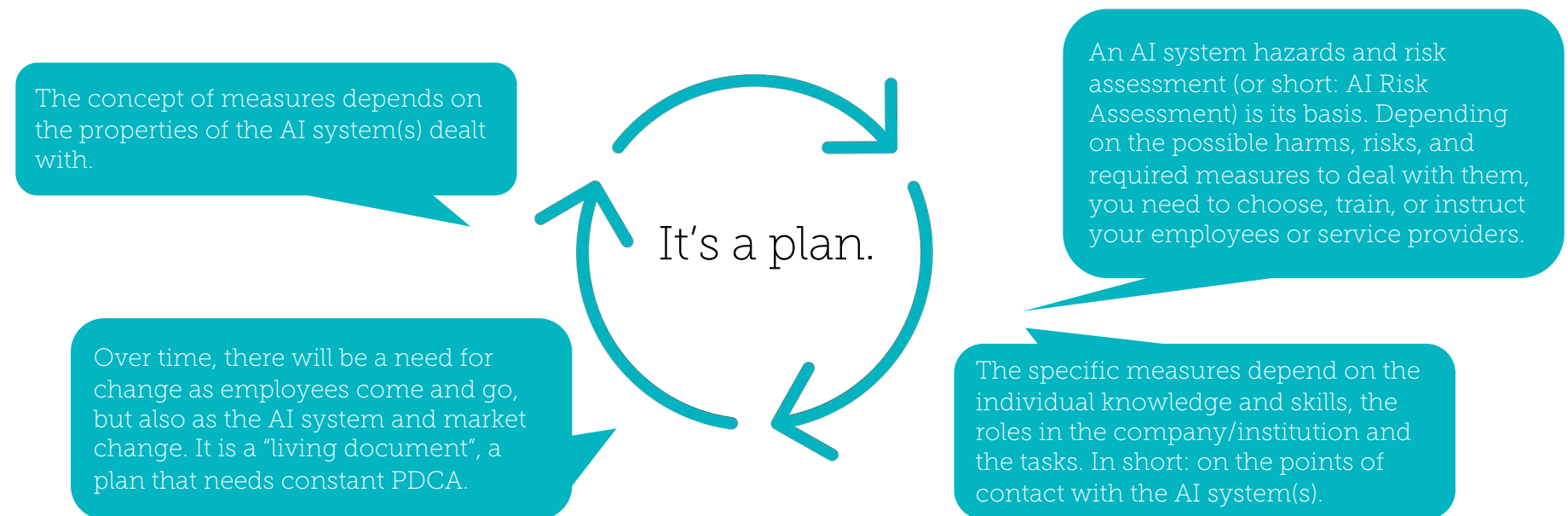
5. AI Literacy (Chapter I, Art. 4 AI Act)...

What is a concept of measures within the meaning of Art. 4?



5. AI Literacy (Chapter I, Art. 4 AI Act)...

What is a concept of measures within the meaning of Art. 4?



II. Relationship AI Act / ISO standards

How do the AI Act and ISO standards relate to each other?



II. Relationship AI Act / ISO standards

1. Differences

- The AI Act is binding.
- ISO(/IEC etc.) standards are voluntary.
- However, ISO standards can become binding, e.g., through reference in contracts or legislation.



II. Relationship AI Act / ISO standards

2. Relationship AI Act – ISO standards

Why did the EU reject the idea to implement the standard ISO/IEC 42001:2023 Management System for AI?

II. Relationship AI Act / ISO standards

2. Relationship AI Act – ISO standards (here: ISO/IEC 42001:2023)

Because of their differences:

Different understanding of "risk":

ISO/IEC 42001:2023: 'risk' means effect of uncertainty

Art. 3 (2) AI Act: 'risk' means the combination of the probability of an occurrence of harm and the severity of that harm

Different focus points:

ISO/IEC 42001:2023 focuses on companies:

"This document intends to help organizations responsibly perform their role with respect to AI systems (e.g. to use, develop, monitor or provide products or services that utilize AI)."

AI Act is AI system/model-oriented

Different goals:

ISO/IEC 42001:2023 aims at "good practice"

The AI Act aims at enforceable requirements

II. Relationship AI Act / ISO standards

2. Relationship AI Act – ISO standards (here: ISO/IEC 23894:2023)

AI – Guidance on risk management

Different understanding of "risk":

ISO/IEC 31000:2018: 'risk' means effect of uncertainty

Art. 3 (2) AI Act: 'risk' means the combination of the probability of an occurrence of harm and the severity of that harm

Different focus points:

ISO/IEC 23894:2023 focuses on companies:

"The purpose of risk management is the creation and protection of value. It improves performance, encourages innovation and supports the achievement of objectives."

AI Act is AI system/model-oriented

Different goals:

ISO/IEC 23894:2023 aims at "good practice"

The AI Act aims at enforceable requirements

II. Relationship AI Act / ISO standards

2. Relationship AI Act – ISO standards (here: ISO/IEC 23894:2023)

AI – Guidance on risk management

Different understanding of "risk":

ISO/IEC 31000:2018: 'risk' means effect of uncertainty

Art. 3 (2) AI Act: 'risk' means the combination of the probability of an occurrence of harm and the severity of that harm

Deviating terms:

ISO/IEC 23894:2023

- ▼ 6.4 Risk assessment
 - 6.4.1 General
 - ▶ 6.4.2 Risk identification
 - ▶ 6.4.3 Risk analysis
 - 6.4.4 Risk evaluation
 - ▶ 6.5 Risk treatment
 - 6.6 Monitoring and review
 - 6.7 Recording and reporting

Article 9

Risk management system

1. A risk management system shall be established, implemented, documented and maintained in relation to high-risk AI systems.
2. The risk management system shall be understood as a continuous iterative process planned and run throughout the entire lifecycle of a high-risk AI system, requiring regular systematic review and updating. It shall comprise the following steps:
 - (a) the 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 when the high-risk AI system is used in accordance with its intended purpose;
 - (b) the estimation and evaluation of the risks that may emerge when the high-risk AI system is used in accordance with its intended purpose, and under conditions of reasonably foreseeable misuse;
 - (c) the evaluation of other risks possibly arising, based on the analysis of data gathered from the post-market monitoring system referred to in Article 72;
 - (d) the adoption of appropriate and targeted risk management measures designed to address the risks identified pursuant to point (a).

II. Relationship AI Act / ISO standards

2. Relationship AI Act – ISO standards

AI – Guidance on risk management

While the ISO standard generalizes a (voluntary) risk management process including risk assessment, Art. 9 describes various (mandatory) risk assessment processes as part of the risk management.

Different understanding of "risk":

ISO/IEC 31000:2018: 'risk' means effect of uncertainty

Art. 3 (2) AI Act: 'risk' means the combination of the probability of an occurrence of harm and the severity of that harm

Deviating terms:

ISO/IEC 23894:2023

- ▼ 6.4 Risk assessment
 - 6.4.1 General
 - ▶ 6.4.2 Risk identification
 - ▶ 6.4.3 Risk analysis
 - 6.4.4 Risk evaluation
 - ▶ 6.5 Risk treatment
 - 6.6 Monitoring and review
 - 6.7 Recording and reporting

Article 9

Risk management system

1. A risk management system shall be established, implemented, documented and maintained in relation to high-risk AI systems.
2. The risk management system shall be understood as a continuous iterative process planned and run throughout the entire lifecycle of a high-risk AI system, requiring regular systematic review and updating. It shall comprise the following steps:
 - (a) the 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 when the high-risk AI system is used in accordance with its intended purpose;
 - (b) the estimation and evaluation of the risks that may emerge when the high-risk AI system is used in accordance with its intended purpose, and under conditions of reasonably foreseeable misuse;
 - (c) the evaluation of other risks possibly arising, based on the analysis of data gathered from the post-market monitoring system referred to in Article 72;
 - (d) the adoption of appropriate and targeted risk management measures designed to address the risks identified pursuant to point (a).

II. Relationship AI Act / ISO standards

2. Relationship AI Act – ISO standards

So, the differences are the reason, why CEN/CENELEC (JTC 21) is working on an AI Act-specific standard for AI Risk Management Systems.

II. Relationship AI Act / ISO standards

3. Interoperability

Since you can't separate an organization from its "products", both must get along

→ that is why ISO standards will be referenced in the new EU standards



So, it's not a cat-and-dog relationship.

II. Relationship AI Act / ISO standards

4. Availability

The work schedule is publicly available

→ EU standard for AI Risk Management will be available after forecasted voting date, which is currently 31 December 2025

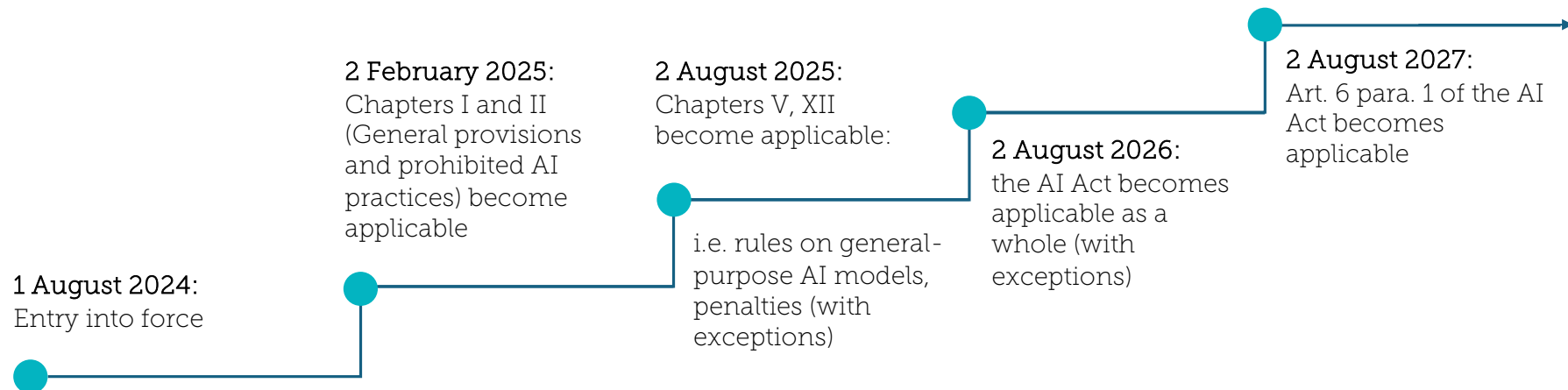
The screenshot shows the CEN website. The top navigation bar includes 'About CEN', 'About CENELEC', and 'Contact Us'. The main header features the CEN logo and the text 'EUROPEAN STANDARDIZATION'. Below this, the 'About CEN' section is displayed, followed by a navigation bar with 'CEN Communities', 'Technical Work', and 'Structure and Governance'. The 'Technical Work' section is active, showing 'CEN Technical Bodies' and 'CEN Standards Evolution and Forecast'. The 'CEN/CLC/JTC 21 - Artificial Intelligence' section is highlighted, with tabs for 'General', 'Structure', 'Work programme', and 'Published Standards'. The 'Work programme' tab is selected, displaying a table of projects.

Project reference	Status	Initial Date	Current Stage	Next Stage	Forecasted voting date
EN ISO/IEC 22989:2023/prA2 (WI=JTO21031) Information technology — Artificial intelligence — Artificial intelligence concepts and terminology — Amendment 1	Under Drafting	2024-05-04	2024-05-04	2024-11-04	2026-06-15

prEN XXX (WI=JTO21024) AI Risk Management	Under Drafting	2024-03-20	2024-03-20	2024-07-17	2025-12-31
--	----------------	------------	------------	------------	------------

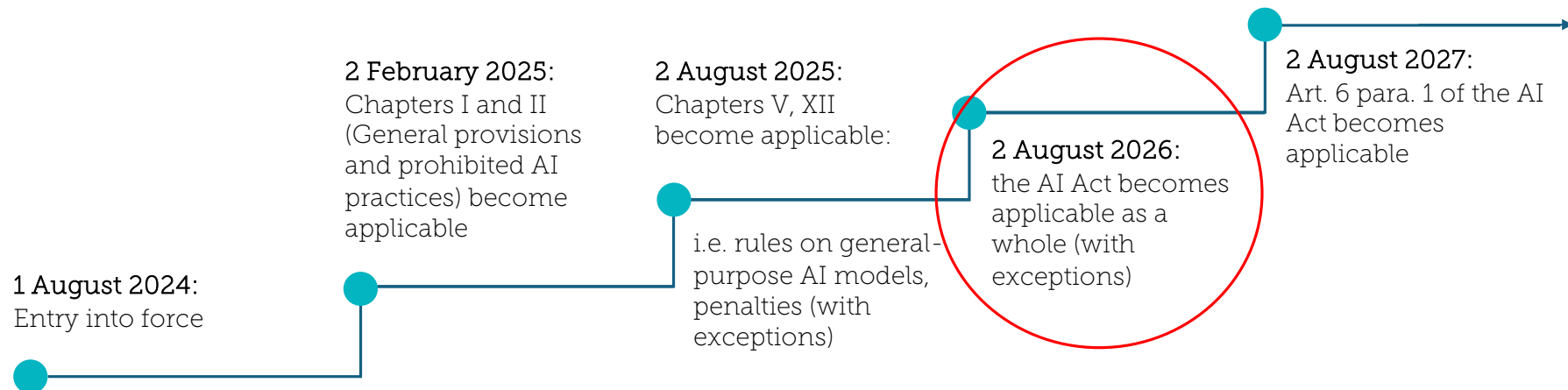
I. The EU AI Act...

1. ... is a Regulation, i.e., binding and directly applicable
2. ... came into force on 1 August 2024
3. ... applies gradually according to Art. 113 of the AI Act:



I. The EU AI Act...

1. ... is a Regulation, i.e., binding and directly applicable
2. ... came into force on 1 August 2024
3. ... applies gradually according to Art. 113 of the AI Act:



II. Relationship AI Act / ISO standards

5. Beware of "experts"

Due to the differences, compliance with the AI Act cannot be achieved through ISO-based consulting, audits, and/or certifications.

- Check offers thoroughly
- Thoroughly review the roles and expertise of your consultants (no less than the expertise of your employees, cf. AI Literacy), and if in doubt, ask for proof of expertise. You don't need additional legal risk.



III. Risk Management under the AI Act

1. Risk Management System required only for so-called high-risk AI systems

Art. 9 para. 1 of the AI Act:

"A risk management system shall be established, implemented, documented and maintained in relation to high-risk AI systems."

III. Risk Management under the AI Act

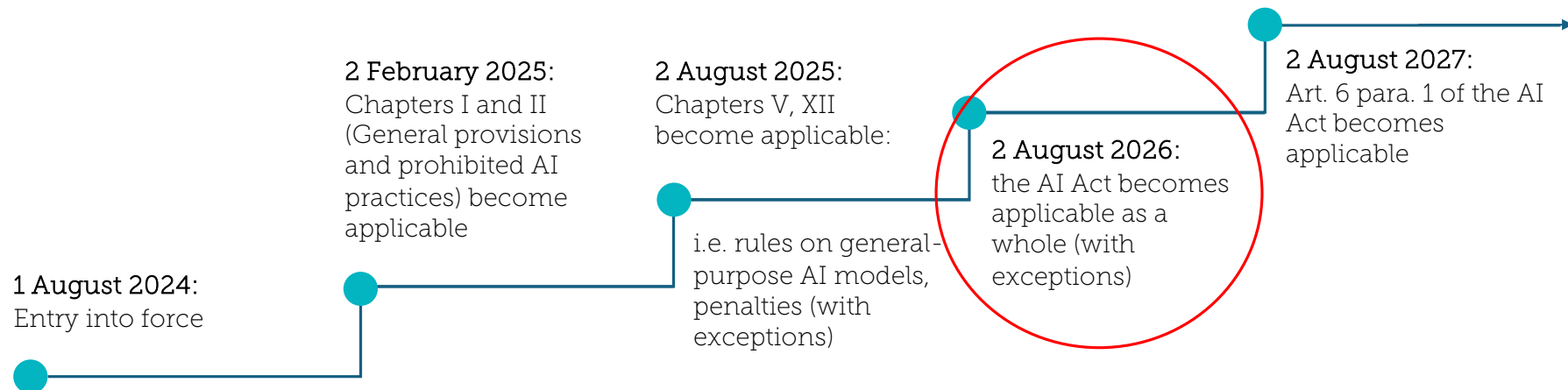
1. Risk Management System required only for so-called high-risk AI systems

Art. 9 para. 2 s. 1 of the AI Act:

"The risk management system shall be understood as a continuous iterative process planned and run throughout the entire lifecycle of a high-risk AI system, requiring regular systematic review and updating."

I. The EU AI Act...

1. ... is a Regulation, i.e., binding and directly applicable
2. ... came into force on 1 August 2024
3. ... applies gradually according to Art. 113 of the AI Act:



IV. Risk Assessment under the AI Act



Yay! So, we can go back to work and concentrate on other things!

IV. Risk Assessment under the AI Act



Sorry, but rather not.

IV. Risk Assessment under the AI Act

1. “Officially”, it is part of the Risk Management System

Article 9

Risk management system

1. A risk management system shall be established, implemented, documented and maintained in relation to high-risk AI systems.
2. The risk management system shall be understood as a continuous iterative process planned and run throughout the entire lifecycle of a high-risk AI system, requiring regular systematic review and updating. It shall comprise the following steps:
 - (a) the 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 when the high-risk AI system is used in accordance with its intended purpose;
 - (b) the estimation and evaluation of the risks that may emerge when the high-risk AI system is used in accordance with its intended purpose, and under conditions of reasonably foreseeable misuse;
 - (c) the evaluation of other risks possibly arising, based on the analysis of data gathered from the post-market monitoring system referred to in Article 72;
 - (d) the adoption of appropriate and targeted risk management measures designed to address the risks identified pursuant to point (a).



IV. Risk Assessment under the AI Act

1. "Officially", it is part of the Risk Management System

Article 9

Risk management system

1. A risk management system shall be established, implemented, documented and maintained in relation to high-risk AI systems.
2. The risk management system shall be understood as a continuous iterative process planned and run throughout the entire lifecycle of a high-risk AI system, requiring regular systematic review and updating. It shall comprise the following steps:
 - (a) the 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 when the high-risk AI system is used in accordance with its intended purpose;
 - (b) the estimation and evaluation of the risks that may emerge when the high-risk AI system is used in accordance with its intended purpose, and under conditions of reasonably foreseeable misuse;
 - (c) the evaluation of other risks possibly arising, based on the analysis of data gathered from the post-market monitoring system referred to in Article 72;
 - (d) the adoption of appropriate and targeted risk management measures designed to address the risks identified pursuant to point (a).



IV. Risk Assessment under the AI Act

1. "Officially", it is part of the Risk Management System

Article 9

Risk management system

1. A risk management system shall be established, implemented, documented and maintained in relation to high-risk AI systems.
2. The risk management system shall be understood as a continuous iterative process planned and run throughout the entire lifecycle of a high-risk AI system, requiring regular systematic review and updating. It shall comprise the following steps:
 - (a) the 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 when the high-risk AI system is used in accordance with its intended purpose;
 - (b) the estimation and evaluation of the risks that may emerge when the high-risk AI system is used in accordance with its intended purpose, and under conditions of reasonably foreseeable misuse;
 - (c) the evaluation of other risks possibly arising, based on the analysis of data gathered from the post-market monitoring system referred to in Article 72;
 - (d) the adoption of appropriate and ~~targeted risk management measures~~ designed to address the risks identified pursuant to point (a).

I summarize "identification, analysis, estimation, evaluation", and "assessment" (Art. 6 para. 4 s. 1) as AI Risk Assessment.

IV. Risk Assessment under the AI Act

2. Official, general Risk Assessment obligations regarding “high-risk AI systems”:

Art. 9 para. 1 of the AI Act:

Risk Assessment as part of the risk management system shall be (...) documented (...).



Art. 9 para. 2 s. 1 of the AI Act:

Risk assessment as part of the risk management system shall be understood as a continuous iterative process planned and run throughout the entire lifecycle of a high-risk AI system, requiring regular systematic review and updating.



Art. 9 para. 2 s. 2 points a-c of the AI Act:

- a) identification and analysis of the known and the reasonably foreseeable risks (...)
- b) estimation and evaluation of the risks that may emerge (...)
- c) evaluation of other risks possibly arising (...)



IV. Risk Assessment under the AI Act



And unofficially...?

IV. Risk Assessment under the AI Act



A very good question!

IV. Risk Assessment under the AI Act

3. There are 3 categories of AI systems

So-called high-risk AI systems

→ Art. 6 of the AI Act

Prohibited AI practices

→ Art. 5 of the AI Act

Transparency obligations

→ Art. 50 of the AI Act

IV. Risk Assessment under the AI Act

3. There are 3 categories of AI systems

So-called high-risk AI systems

- Art. 6 of the AI Act
- Art. 6 para. 1: the “products”
- Art. 6 para. 2: critical use cases, e.g. biometrics, education, employment (HR)
- Art. 6 para. 3: NOT high-risk AI systems

Prohibited AI practices

- Art. 5 of the AI Act

Transparency obligations

- Art. 50 of the AI Act

IV. Risk Assessment under the AI Act

3. There are 3 categories of AI systems

So-called high-risk AI systems

- Art. 6 of the AI Act
- Art. 6 para. 1: the “products”
- Art. 6 para. 2: critical use cases, e.g. biometrics, education, employment (HR)
- Art. 6 para. 3: NOT high-risk AI systems

Prohibited AI practices

- Art. 5 of the AI Act
- e.g., exploiting vulnerabilities (e.g. due to age) and distorting behavior with the reasonable likelihood of causing significant harm (Art. 5 para. 1 s. 1 point b)

Transparency obligations

- Art. 50 of the AI Act

IV. Risk Assessment under the AI Act

3. There are 3 categories of AI systems

So-called high-risk AI systems

- Art. 6 of the AI Act
- Art. 6 para. 1: the “products”
- Art. 6 para. 2: critical use cases, e.g. biometrics, education, employment (HR)
- Art. 6 para. 3: NOT high-risk AI systems

Prohibited AI practices

- Art. 5 of the AI Act
- e.g., exploiting vulnerabilities (e.g. due to age) and distorting behavior with the reasonable likelihood of causing significant harm (Art. 5 para. 1 s. 1 point b)

Transparency obligations

- Art. 50 of the AI Act
- e.g., AI systems intended to interact directly with natural persons: provider's obligation to inform that they are interacting with an AI system (Art. 50 para 1)

IV. Risk Assessment under the AI Act

3. (AI) Risk Assessment regarding so-called not high-risk AI systems

Art. 6 paras. 3, 4 s. 1 of the AI Act:

4. A provider who considers that an AI system referred to in Annex III is not high-risk shall document its assessment before that system is placed on the market or put into service. Such provider shall be subject to the registration obligation set out in Article 49(2). Upon request of national competent authorities, the provider shall provide the documentation of the assessment.

IV. Risk Assessment under the AI Act

3. (AI) Risk Assessment regarding so-called not high-risk AI systems

Art. 6 paras. 3, 4 s. 1 of the AI Act:

4. A provider who considers that an AI system referred to in Annex III is not high-risk shall document its assessment before that system is placed on the market or put into service. Such provider shall be subject to the registration obligation set out in Article 49(2). Upon request of national competent authorities, the provider shall provide the documentation of the assessment.

IV. Risk Assessment under the AI Act

4. (AI) Risk Assessment regarding prohibited AI practices (Art. 5)

An AI Risk Assessment is not expressly required, but part of complying with Art. 5 of the AI Act.

→ see the “risk”-components in points a-c (reasonable likelihood, significant harm)

Article 5

Prohibited AI practices

1. The following AI practices shall be prohibited:

- (a) the placing on the market, the putting into service or the use of an AI system that deploys subliminal techniques beyond a person's consciousness or purposefully manipulative or deceptive techniques, with the objective, or the effect of materially distorting the behaviour of a person or a group of persons by appreciably impairing their ability to make an informed decision, thereby causing them to take a decision that they would not have otherwise taken in a manner that causes or is reasonably likely to cause that person, another person or group of persons significant harm;
- (b) the placing on the market, the putting into service or the use of an AI system that exploits any of the vulnerabilities of a natural person or a specific group of persons due to their age, disability or a specific social or economic situation, with the objective, or the effect, of materially distorting the behaviour of that person or a person belonging to that group in a manner that causes or is reasonably likely to cause that person or another person significant harm;
- (c) the placing on the market, the putting into service or the use of AI systems for the evaluation or classification of natural persons or groups of persons over a certain period of time based on their social behaviour or known, inferred or predicted personal or personality characteristics, with the social score leading to either or both of the following:
 - (i) detrimental or unfavourable treatment of certain natural persons or groups of persons in social contexts that are unrelated to the contexts in which the data was originally generated or collected;
 - (ii) detrimental or unfavourable treatment of certain natural persons or groups of persons that is unjustified or disproportionate to their social behaviour or its gravity;

IV. Risk Assessment under the AI Act

5. (AI) Risk Assessment regarding transparency (Art. 50)

An AI Risk Assessment is not expressly required, but part of complying with Art. 50 para. 1 and 2 of the AI Act.

→ see the “risk”-components “reasonably well-informed”, circumstances, context of use, etc.

→ apart from this, the lawmaker’s risk assessment is sufficient

Article 50

Transparency obligations for providers and deployers of certain AI systems

1. Providers shall ensure that AI systems intended to interact directly with natural persons are designed and developed in such a way that the natural persons concerned are informed that they are interacting with an AI system, unless this is obvious from the point of view of a natural person who is reasonably well-informed, observant and circumspect, taking into account the circumstances and the context of use. This obligation shall not apply to AI systems authorised by law to detect, prevent, investigate or prosecute criminal offences, subject to appropriate safeguards for the rights and freedoms of third parties, unless those systems are available for the public to report a criminal offence.

2. Providers of AI systems, including general-purpose AI systems, generating synthetic audio, image, video or text content, shall ensure that the outputs of the AI system are marked in a machine-readable format and detectable as artificially generated or manipulated. Providers shall ensure their technical solutions are effective, interoperable, robust and reliable as far as this is technically feasible, taking into account the specificities and limitations of various types of content, the costs of implementation and the generally acknowledged state of the art, as may be reflected in relevant technical standards. This obligation shall not apply to the extent the AI systems perform an assistive function for standard editing or do not substantially alter the input data provided by the deployer or the semantics thereof, or where authorised by law to detect, prevent, investigate or prosecute criminal offences.

IV. Risk Assessment under the AI Act



The lawmaker's risk assessment?!

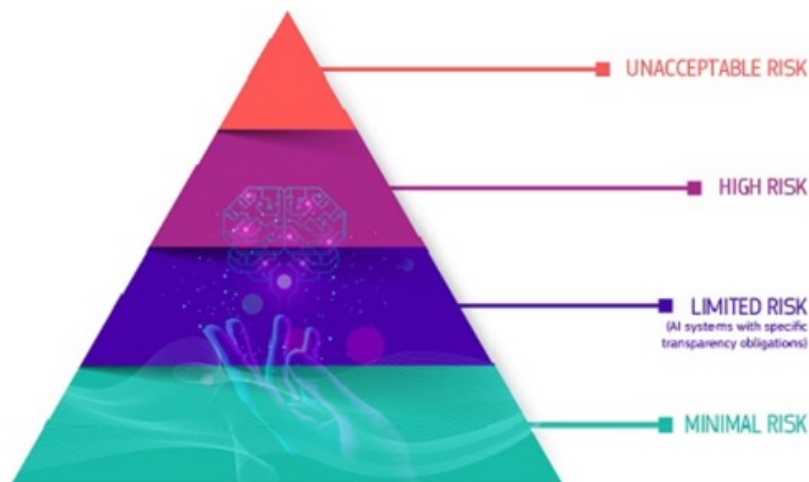
IV. Risk Assessment under the AI Act



Yes. There are two different AI Risk Assessments.

IV. Risk Assessment under the AI Act

6. There are two different AI Risk Assessments

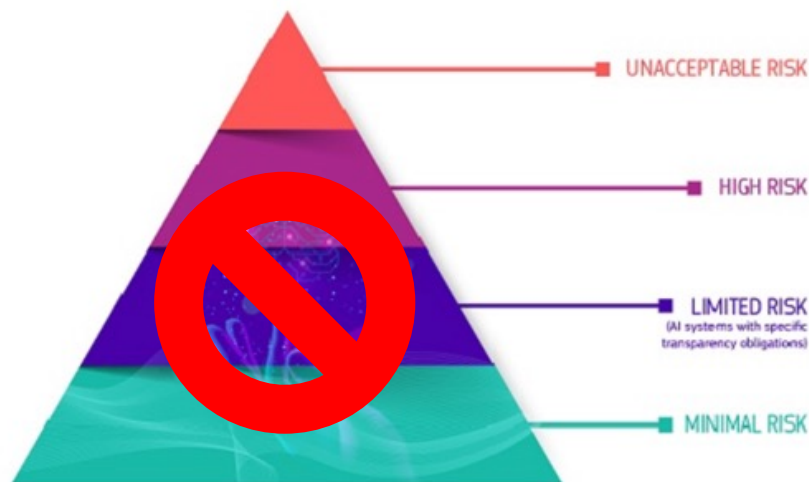


The EU Commission's one (cf. Art. 7 of the AI Act), often illustrated using a pyramid. It is generalized, often based on assumptions.

The provider's or deployer's individual AI Risk Assessment has to include each single relevant risk (cf. Art. 9 para. 5 of the AI Act).

IV. Risk Assessment under the AI Act

→ This pyramid does not correspond to reality. It is a representation of the motivation of the EU Commission to promote innovation.



Keep in mind: Hazards and associated risks are not separated from each other like this.

IV. Risk Assessment under the AI Act



Good lord! So, where and when is the AI Risk Assessment needed?

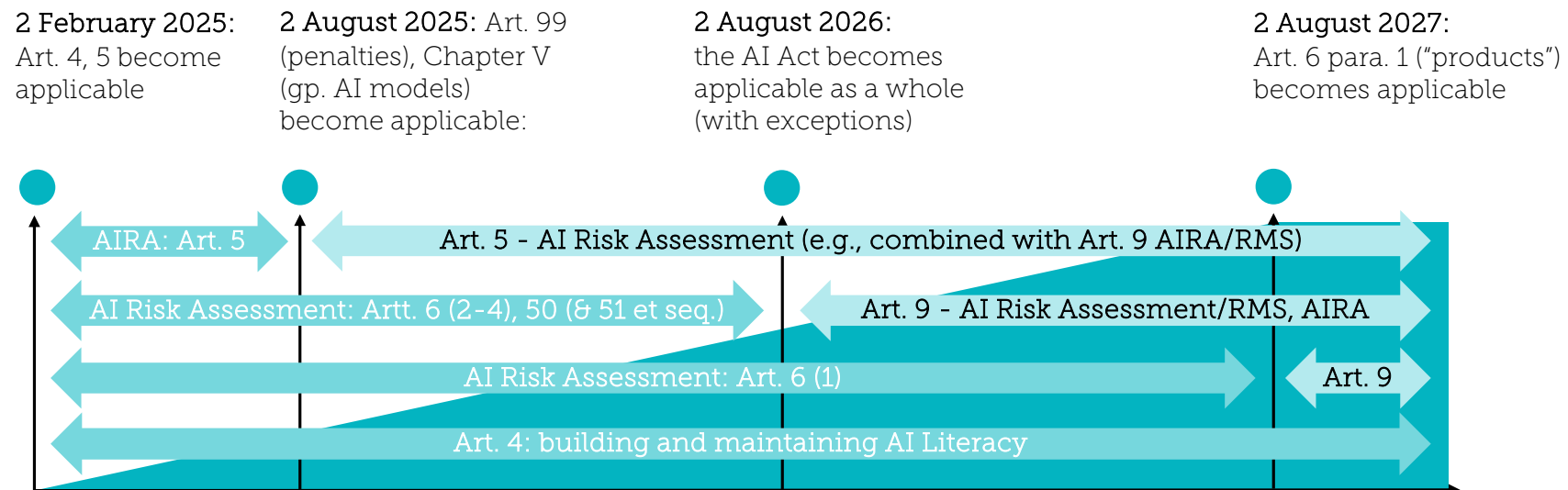
IV. Risk Assessment under the AI Act



Great question!

IV. Risk Assessment under the AI Act

7. So where is the AI Risk Assessment needed?



IV. Risk Assessment under the AI Act

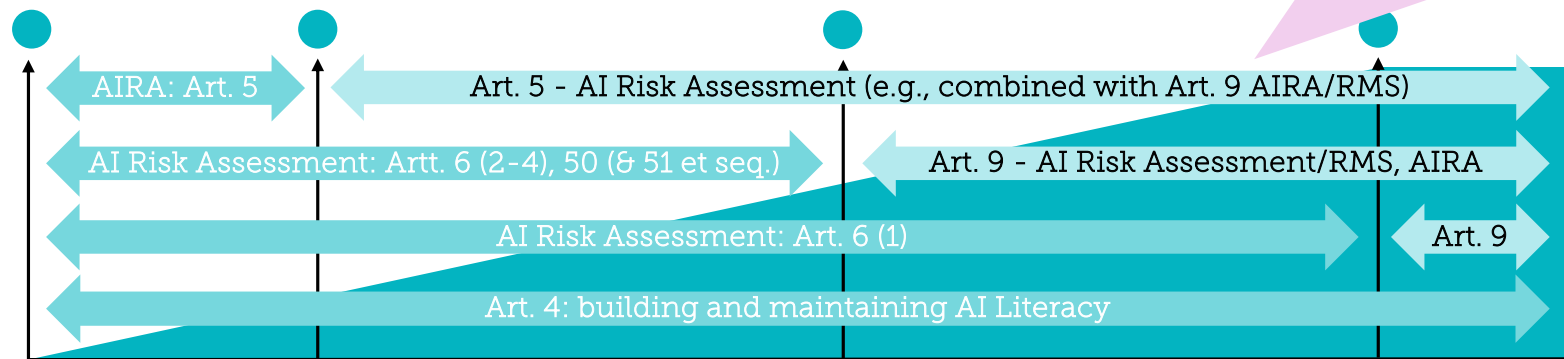
7. So where is the AI Risk Assessment needed?

2 February 2025:
Art. 4, 5 become
applicable

2 August 2025: Art. 99
(penalties), Chapter V
(gp. AI models)
become applicable:

2 August 2026:
the AI Act becomes
applicable as a whole
(with exceptions)

Risk assessment capability
should be built up
gradually, based on needs,
i.e., the applicability of the
AI Act and scope of
obligations.



V. First steps

1. Identify what information you need (AI Act, MDR, etc.)
2. Gather the information you need
3. Document the gathered information in a systematic manner which allows updates
4. Separate AI risk assessment and AI risk management functions
5. Set up an AI Risk Assessment policy
6. Determine an AI Risk Assessment methodology



V. First steps

1. Identify what information you need (AI Act, MDR, etc.)

→ Risk assessment is all about information collection, analysis, and evaluation (to keep it short).

You can start with the questions:

- Is your AI system or AI model one within the meaning of the AI Act? (chances are good due to technological neutrality)
- What categories apply?



V. First steps

2. Gather the information you need

Collect information to answer the questions:

- Is your AI system or AI model one within the meaning of the AI Act? (chances are good due to technological neutrality)
- What categories apply?



V. First steps

3. Document the gathered information in a systematic manner which allows updates

- It is best to build on a familiar basis and adapt the documentation in a way that it reflects the systematics of the AI Act. This also helps to build and maintain AI Literacy.
- The goal is to make AI Risk Assessment as easy as possible for you.



V. First steps

4. Separate AI risk assessment and risk management functions

- This is best practice to avoid conflicts of interest, bias, operational blindness, and therefore non-compliance.
- Not everyone is suited to these roles. When selecting, now and later, keep AI Literacy in mind as the key to fulfilling obligations.



V. First steps

5. Set up an AI Risk Assessment Policy

- This is best practice to ensure that the risk assessments meet your compliance requirements. Especially when new employees are involved, or external expertise is sought.
- In it, you can determine how to document, how to assess risks, how to deal with uncertainties, for example.
- You can also regulate/exclude certain types of “risk assessment” that are known to be misleading or inadequate, e.g., the use of benchmarks or tools from the internet.



V. First steps

6. Determine an AI Risk Assessment Methodology

- Due to the complexity of risk assessment under the AI Act, a quantitative methodology is insufficient.
- A qualitative-quantitative methodology seems to be more suitable due to the measurement possibilities it offers.
- Beware of ISO "experts", do not rely on internet downloads. You do not need extra legal risk.



If you need help with this, let me know. You do not need to start from scratch.

V. Q&A



Thank you!

COT Legal
Rechtsanwältin Claudia Otto
Stadttor Ost
Rudolf-Diesel-Str. 11
69115 Heidelberg (Germany)
E-mail: claudia.otto@cotlegal.de
Web: <https://cotlegal.de>
Phone: +49 6221 648 4036

