

AI Risks: Are we all going to die or should we certify?

This year we saw a shift from the endless possibilities of AI, to AI risks that actually materialized into security incidents and chances are we're just at the start of emerging risks.

At the same time, we find ourselves with a narrative that goes as far as extinction of the human race and it's not the first time in history that we hear a prediction about a new technology taking over... .

We'll first dive into what AI risks are and how they are fundamentally different from any other risks we encountered over the last decades. Furthermore, we'll look into the difference of AI risks per type of AI system, model and use.

The risk between an uncontrolled agentic swarm and an AI system that is dedicated to translate your texts is obvious – even if both have risks that we were unaware of a couple of years ago.

What about the solutions?

We'll first present you an AI Risk taxonomy that clearly shows the new AI risks and typical key risk indicators that most organisations are not even taking into account today.

Furthermore, we'll present a pragmatic approach of dealing with these risks. From classification of AI systems to dealing with cybersecurity, data governance & data quality, bias & drift, ai lifecycle management, technical documentation, etc.

These capabilities are not just a random set of measures to mitigate your risks and make your AI more robust – they are all part of the EU AI Act, a regulation that is already affecting organisations in the Caribbean, the US, Canada and South America.

The EU AI Act currently prohibits the use of certain AI systems, obliges transparency by means of adding AI icons to AI generated content and foresees certification and CE labeling of your high risk AI systems.

We'll explain what this regulation is about, how it affects you and your organisation and show you a practical methodology on how to implement it.

In fact, this regulation could turn out to be the answer to the AI risks we (and even the magnificent 7) are bringing up today.

We can argue about the “Die” option, but the “Certify” route will mitigate AI risks in the most robust manner we know today.

Benefits of this presentation:

You will not only understand the risks of AI but also how to deal with them in a practical matter – reusing existing material and methodologies derived from best practices and proven frameworks.

Disclaimer: this presentation summary & the bio were 100% created by a human.



Christoph Balduck

CTO of Data Trust Associates

As managing partner and CTO of Data Trust Associates, Christoph Balduck supports organizations in the areas of privacy, data protection, data compliance, and information security. Christoph combines these capabilities with expertise in data & AI management – especially focussed on Data and AI governance, Data Quality and Data Architecture.

His vision has always been that the world of data & AI compliance is tightly coupled with the world of operational data management and AI. With growing digital regulations in all parts of the world, we see both of these worlds coming together. Most new digital regulations embed parts of data management, AI, data interoperability, privacy & data protection and information security.

Christoph focuses in his daily work on a practical implementation that enables companies to derive value from their data. This means he will coach companies to find the right use cases, do the data analysis and make sure use cases get fully implemented in a compliant and secure manner.

Besides the combination of the two worlds and the practical hands-on approach with customers, Christoph is using AI to automate data compliance and data & AI management processes in order to keep up with the fast growing digital challenges.

Christoph is a long time professor at the Data Protection Institute where he helped certify over 3000 data protection officers, but also delivers training in data management, data protection and technology, AI etc. .

He was the first one to teach data governance & data quality management to Data Protection Officers and Information Security professionals.

Furthermore he is a visiting professor at the Thomas Moore University in Belgium where he teaches Privacy and Information Security by design and by default.

Christoph also advises and trains several regulatory authorities on how to assess and regulate cases.