

# Auditing in the era of AI

CA Day 2025

Matthias Wiedenhorst | TÜV NORD CERT GmbH | 25.09.2025

# Auditing in the era of AI

Auditing of Artificial Intelligence

# Auditing in the era of AI

## Auditing of Artificial Intelligence

### Secure & trustworthy AI

- Robustness
  - How does the AI work in sub-optimal conditions/attacks?
- Performance
  - How reliable are the AI results?
- Data Quality
  - Does the training data correspond to reality?
- Data Protection
  - How is sensitive data protected?

### Compliance with EU AI Act

- AI Act Risk Navigator helps to classify your risk  
<https://www.tuev-nord.risk-navigator.ai/?lang=en>

# Auditing in the era of AI

## Auditing of Artificial Intelligence

- Not the topic for today.
- Expert team available at TÜV NORD
  - In case of interest, contact me so that I can forward you to the proper specialists.

# Auditing in the era of AI

## Auditing with the use of Artificial Intelligence

- Some insights into TÜV NORD CERT development studies

# Auditing with the use of Artificial Intelligence

## What about AI?

- AI is working well in automating task or document summaries
- AI is mostly used in Public Cloud scenarios
- Data Protection is not transparently solved
- Reliability is not always given
- Developing complex and local operated solutions is still expensive and needs rare knowledgeable people

# Auditing with the use of Artificial Intelligence

## What about AI in the context of QTSP?

- Laws, Implementing Regulation and normative documents are changing a lot right now, as a result training of available LLMs is not good regarding eIDAS
  - AI system are not, or at least not reliably, up-to-date
  - System need individual training, or latest documents must be used as part of the input to the AI system
- The nesting of normative language and changes of norms within implementing regulation Annexes is a big problem when trying to use AI within assessments
- The Number of QTSPs is limited (as of Sept. 15th 250 active QTSP) – so is the trainable data

# Auditing with the use of Artificial Intelligence

## AI in Assessment Processes

- An QTSP Assessment is split into different stages
  - Document Assessment
  - Onsite Assessment
  - Assessment reporting
  - Certification decision & Certification
- Only some of them are a candidate for AI



# Auditing with the use of Artificial Intelligence

## AI in Assessment Processes

- An QTSP Assessment is split into different stages
  - Document Assessment
  - Onsite Assessment
  - Assessment reporting
  - Certification decision & Certification
- Only some of them are a candidate for AI

# Auditing with the use of Artificial Intelligence

## AI in Assessment Processes

- An QTSP Assessment is split into different stages
  - Document Assessment
  - Onsite Assessment
  - Assessment reporting
  - Certification decision & Certification
- Only some of them are a candidate for AI

# Auditing with the use of Artificial Intelligence

## AI in Assessment Processes

- The Document Assessment stage seems to be the best one to be used with AI
  - TÜV NORD currently running a POC
  - Documents can be analyzed and compared etc. with good results
  - Challenges
    - Stability
    - Hallucination
- But not all documents are “public”, some are under NDA, some are even higher classified, e.g. can only be viewed onsite
- So even local installed LLM systems may not work or need special treatment to make sure the data is protected in all cases.

# Auditing with the use of Artificial Intelligence

## AI in Assessment Processes

- The Reporting stage
  - Notes from the Onsite Assessment can be processed and put into structured documents.
  - However, informal or unstructured note taking can lead to misinterpretation, resulting in incorrect reporting
  - And again, it is sensitive or even classified information

Better use templates that will be filled with the assessment results by a human, who is able to better interpret the results

# Auditing with the use of Artificial Intelligence

## How can the future look like?

- AI is developing fast and there will be new models and opportunities to include AI in the coming future
- After the implementation of the new revision of eIDAS and the establishment of the new services, things may become a bit more stable
- Not even AI knows about the future ;)

# Any questions?

**Matthias Wiedenhorst**

M.: [mwiedenhorst@tuev-nord.de](mailto:mwiedenhorst@tuev-nord.de)

