

Standards as a pathway to AI Act compliance and beyond

Driving Trustworthy AI through Design and Regulation - Nicosia

Dr Sebastian Hallensleben

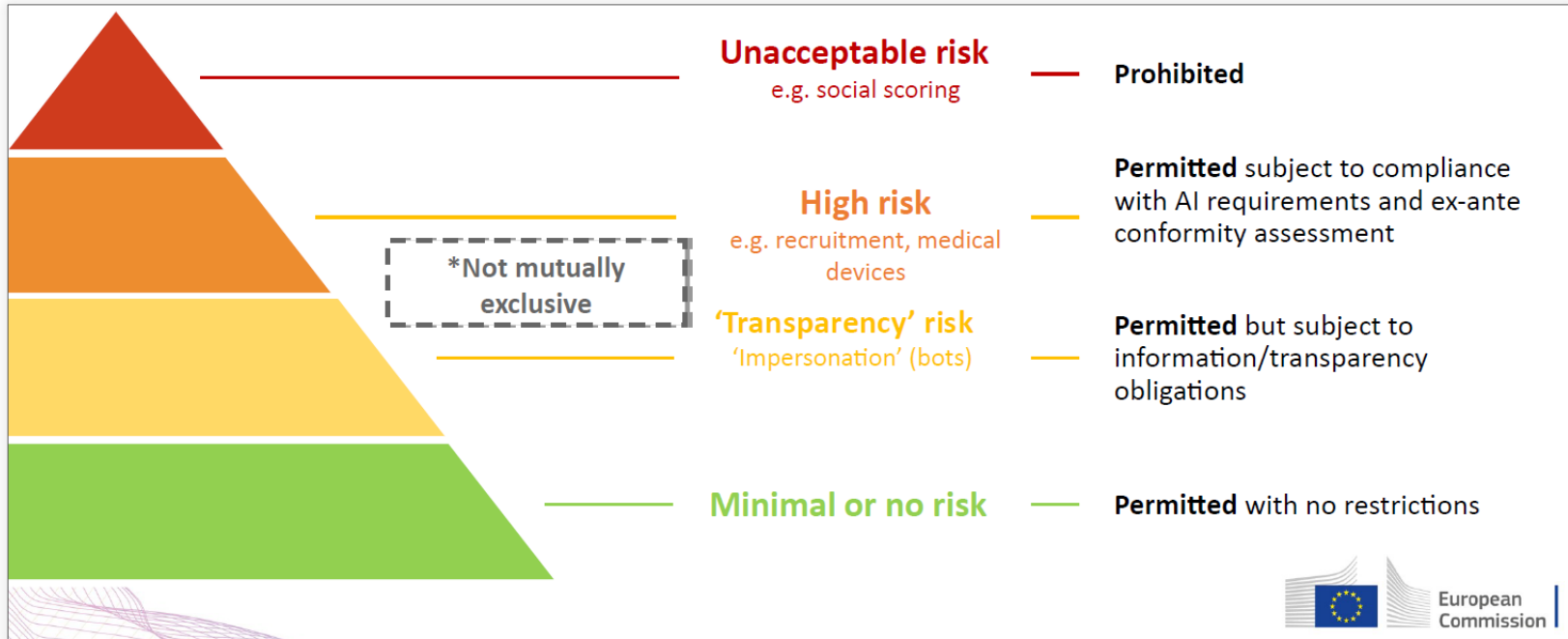
Chair CEN-CENELEC JTC21
Chief Trust Officer, Resaro
Co-Chair AI Risk & Accountability OECD ONE.AI
Programme Chair, Digital Trust Convention
Principal Advisor Digital Trust, KI Park



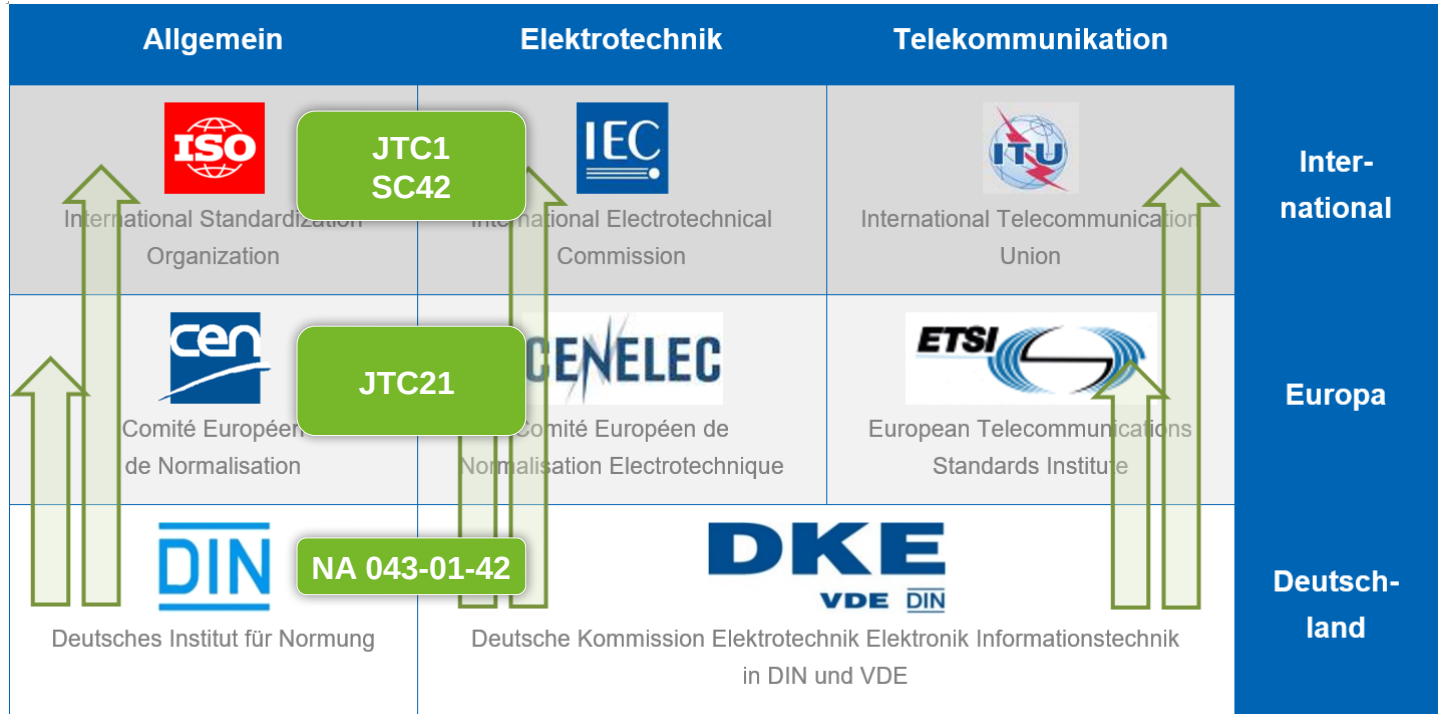
2026-01-27



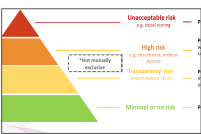
High-risk applications in the AI Act: Broad requirements only ⇒ Details to be defined elsewhere



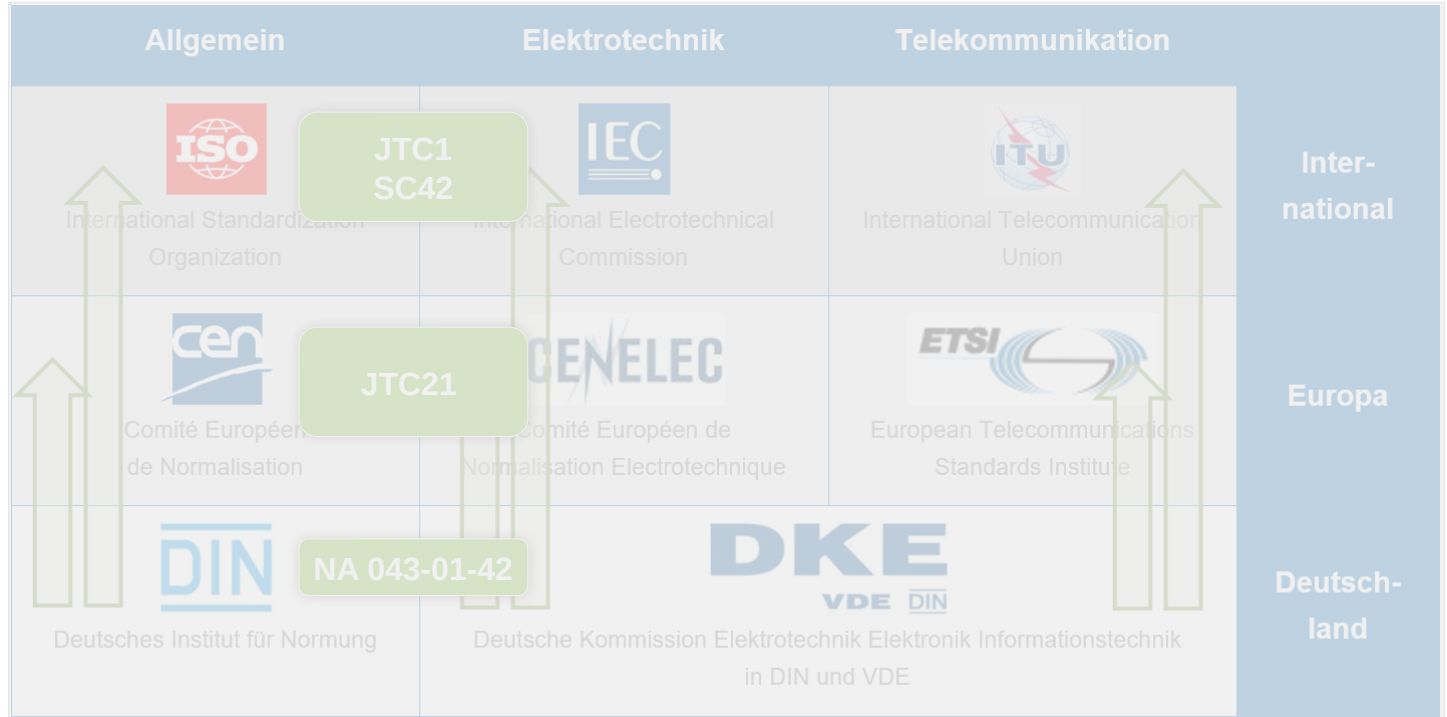
Global three-tier standardisation landscape



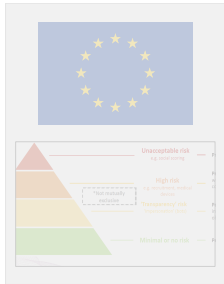
New Legislative Framework



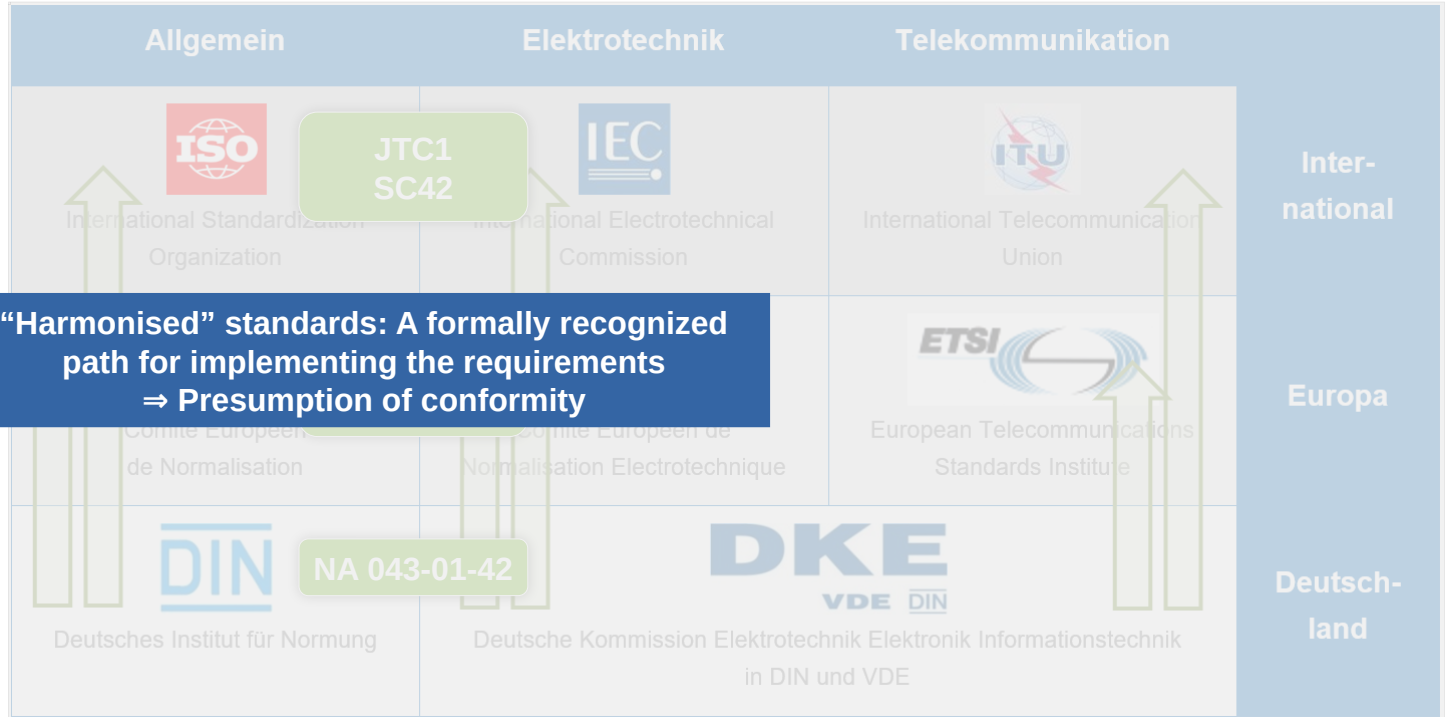
Synergy of regulation and standardisation



**New
Legislative
Framework**



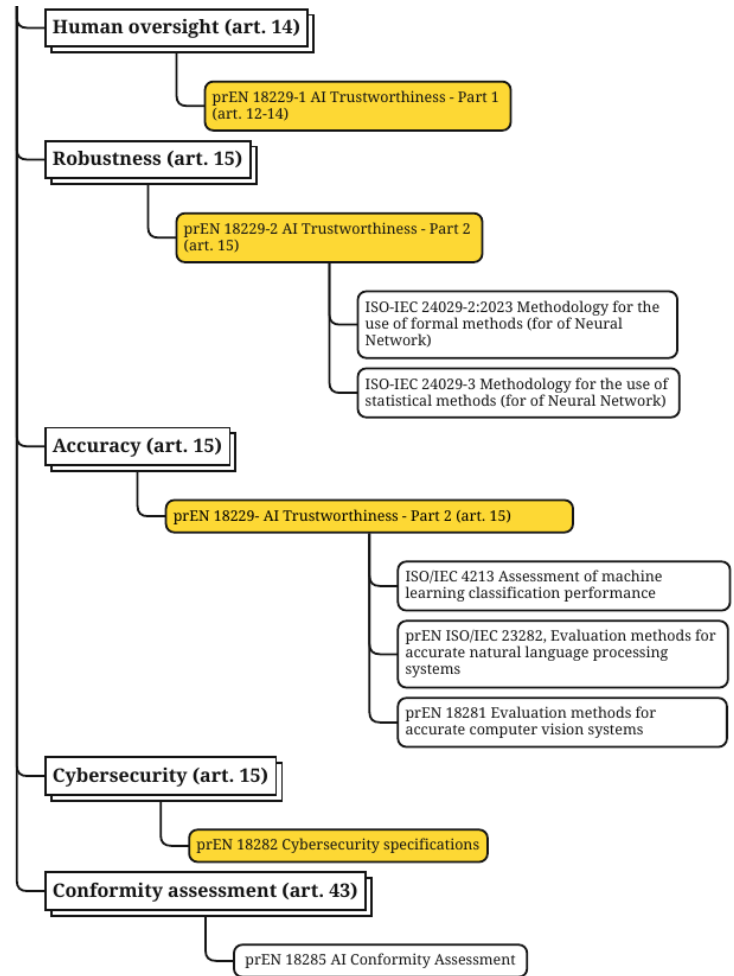
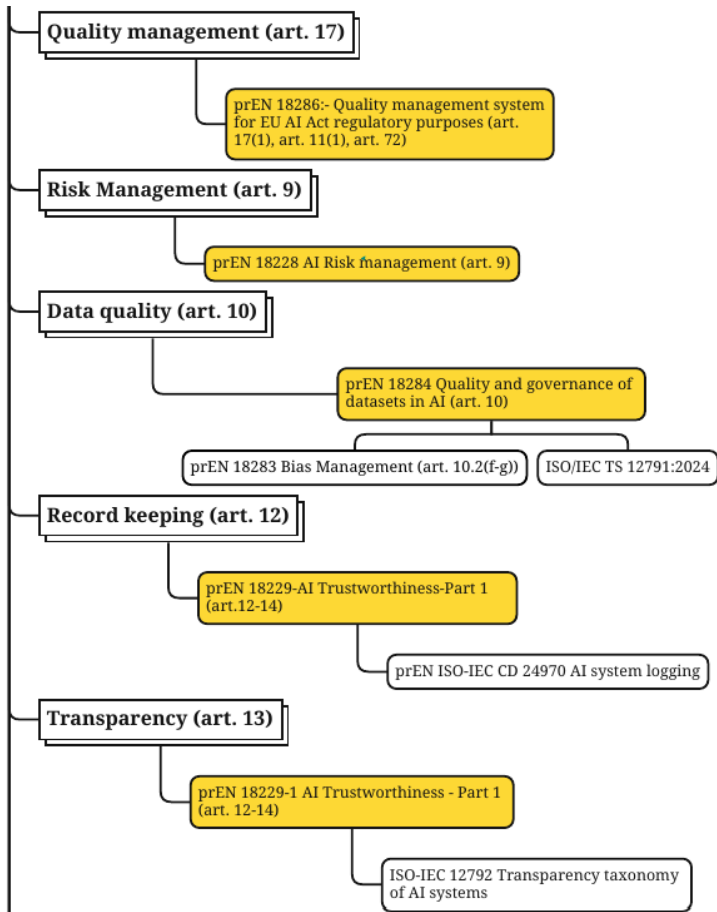
Synergy of regulation and standardisation



Objectives and high-level requirements

New Legislative Framework

“Harmonised” standards: A formally recognized path for implementing the requirements ⇒ Presumption of conformity



JTC21 Working Groups

- **WG1: Strategic Advisory Group**
- **WG2: Operational Aspects**
- **WG3: Engineering Aspects**
- **WG4: Foundational and Societal Aspects**
- **WG5: Cybersecurity**

(in collaboration with ETSI, ENISA and CEN-CENELEC JTC13)

~200 experts directly in JTC21
~25 countries
>1000 experts at national level

Record size due to -

- Breadth of stakeholders and interests
- Breadth of application areas
- High profile of AI

Timeline

- CEN-CENELEC: AI Focus Group since **2019** | JTC21 since **2021**
- AI Act **final**: August 2024
- Public consultation for drafts („**Enquiry Vote**“)
mostly **Nov 2025 to May 2026**
(QMS already concluded)
- Integration of feedback („**Comment Resolution**“)
=> mature content
- Implementation deadline high-risk requirements **Aug 2026** (?)
- Formal processes in CEN-CENELEC and COM / AI Office
for finalisation, harmonisation and OJEU publication

Standardisation has two deliverables

- **Visible:**
a set of interconnected and consistent **technical standards documents**
- **Invisible:**
consensus of “all relevant stakeholders” (=> **legitimacy**)

Standardisation has two deliverables

- **Visible:**
a set of interconnected and consistent **technical standards documents**
- **Invisible:**
consensus of “all relevant stakeholders” (=> **legitimacy**)

Includes many fundamental divergences, e.g. –

- safety and security communities
- EU and non-EU companies
- AI providers and AI deployers
- Large and small companies
- Industry and civil society

Standardisation has two deliverables

- **Visible:** Let's take pride in the ability and the effort to reach common ground
a set of interconnected and consistent technical standards documents
- **Invisible:** consensus of "all relevant stakeholders" (= legitimacy)

- EU and non-EU companies
- AI providers and AI deployers
- Large and small companies
- Industry and civil society

Beyond compliance:

Standards enable **markets** ⇒ **competitiveness** ⇒ **innovation**

Beyond compliance:

Standards enable **markets** ⇒ **competitiveness** ⇒ **innovation**

Compliance

Competitiveness

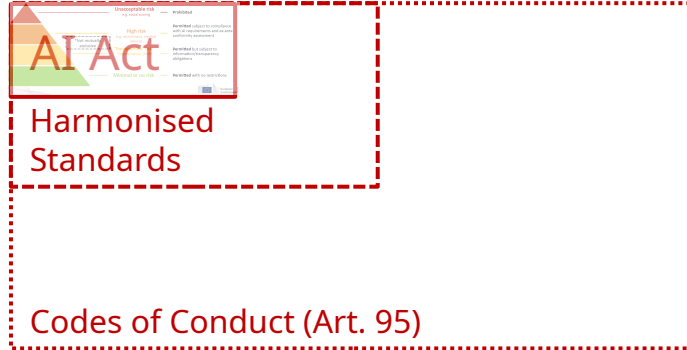
“Ecosystem
of Trust”
(HLEG)
Focus: risk
mitigation



Beyond compliance:

Standards enable **markets** ⇒ **competitiveness** ⇒ **innovation**

Compliance



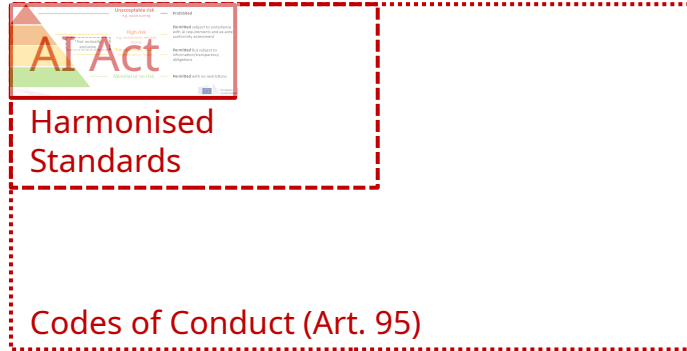
Competitiveness



Beyond compliance:

Standards enable **markets** ⇒ **competitiveness** ⇒ **innovation**

Compliance



Competitiveness

Transparency



Privacy



Accountability



Fairness



Reliability



AI Trust Alliance



Standards enable **markets** ⇒ **competitiveness** ⇒ **innovation**
Widening the scope from trustworthiness to **quality**



Describing AI quality clearly



- When is an AI solution **“good enough”** for use?
- How can **“good enough”** (= a desired level of quality) be described?
- How can you determine whether solution X is better or worse than solution Y?
(→vendor comparison; make vs. buy decision)

Compliance with regulations is not a quality feature - it is the expected baseline

Describing AI quality clearly: Specific to the use case

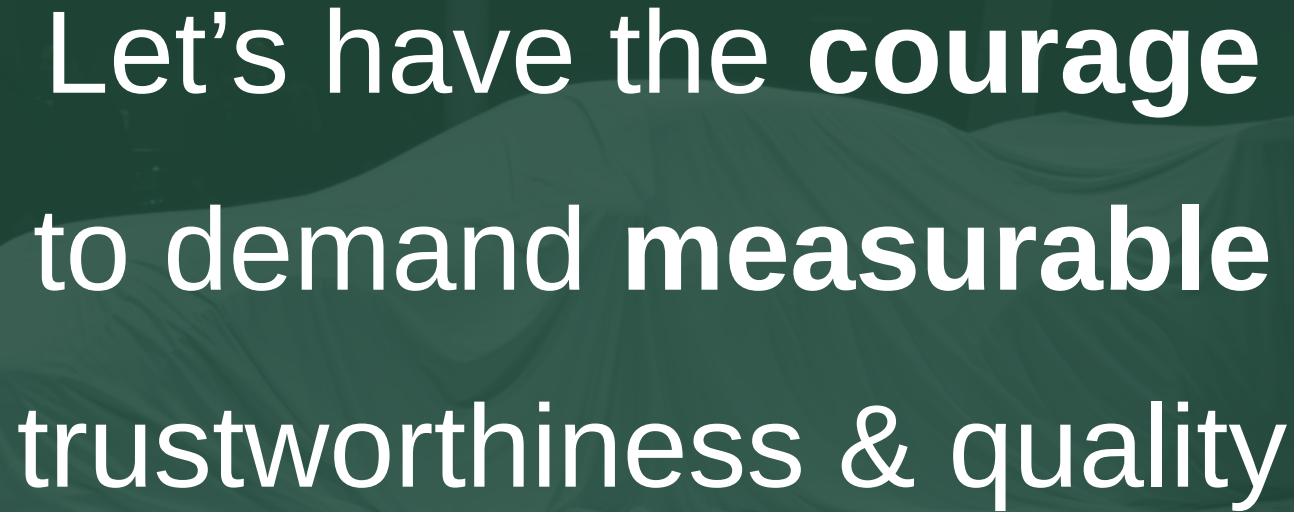


e.g. -

- Internal or external **chat-based support services**
- **Financial fraud detection**
- Detection of **deepfakes**
- **Facial recognition** in public spaces
- Evaluation of **surveillance videos**
- **Agentic** action
- ...

Standards enable **markets** ⇒ **competitiveness** ⇒ **innovation**

Widening the scope from trustworthiness to **quality**



Let's have the **courage**
to demand **measurable**
trustworthiness & **quality**

Let's take **pride**
in the **ability** and the **effort**
to reach **common ground**

Let's have the **courage**
to demand **measurable**
trustworthiness & quality

Let's take **pride**
in the **ability** and the **effort**
to reach **common ground**

Let's have the **courage**
to demand **measurable**
trustworthiness & quality

We win the future
not just by rejecting what we see as wrong –
but by offering a **compelling alternative**

Let's take **pride**
in the **ability** and the **effort**
to reach **common ground**

Let's have the **courage**
to demand **measurable**
trustworthiness & quality

We win the future
not just by rejecting what we see as wrong –
but by offering a **compelling alternative**

... and a smile 