Harmonised standards for the AI Act in the European and OECD context

AI Security Standards: NASK Workshop

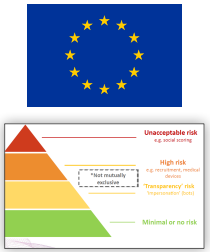
Dr Sebastian Hallensleben

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

2025-05-08

www.linkedin.com/in/sebastianhallensleben sebastian@hallensleben.org

Global three-tier standardisation landscape



New Legislative Framework

	Allgemein	Elektrotechnik	Telekommunikation	
	ISO International Standardization Organization	IEC International Electrotechnical Commission	ITU International Telecommunication Union	Inter-national
	CEN Comité Européen de Normalisation	CENELEC Normalisation Electrotechnique	ETSI Telecommunications Standards Institute	Europa
	DIN Deutsches Institut für Normung	DKE VDE DIN Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE		Deutsch-land

JTC1 SC42

JTC21

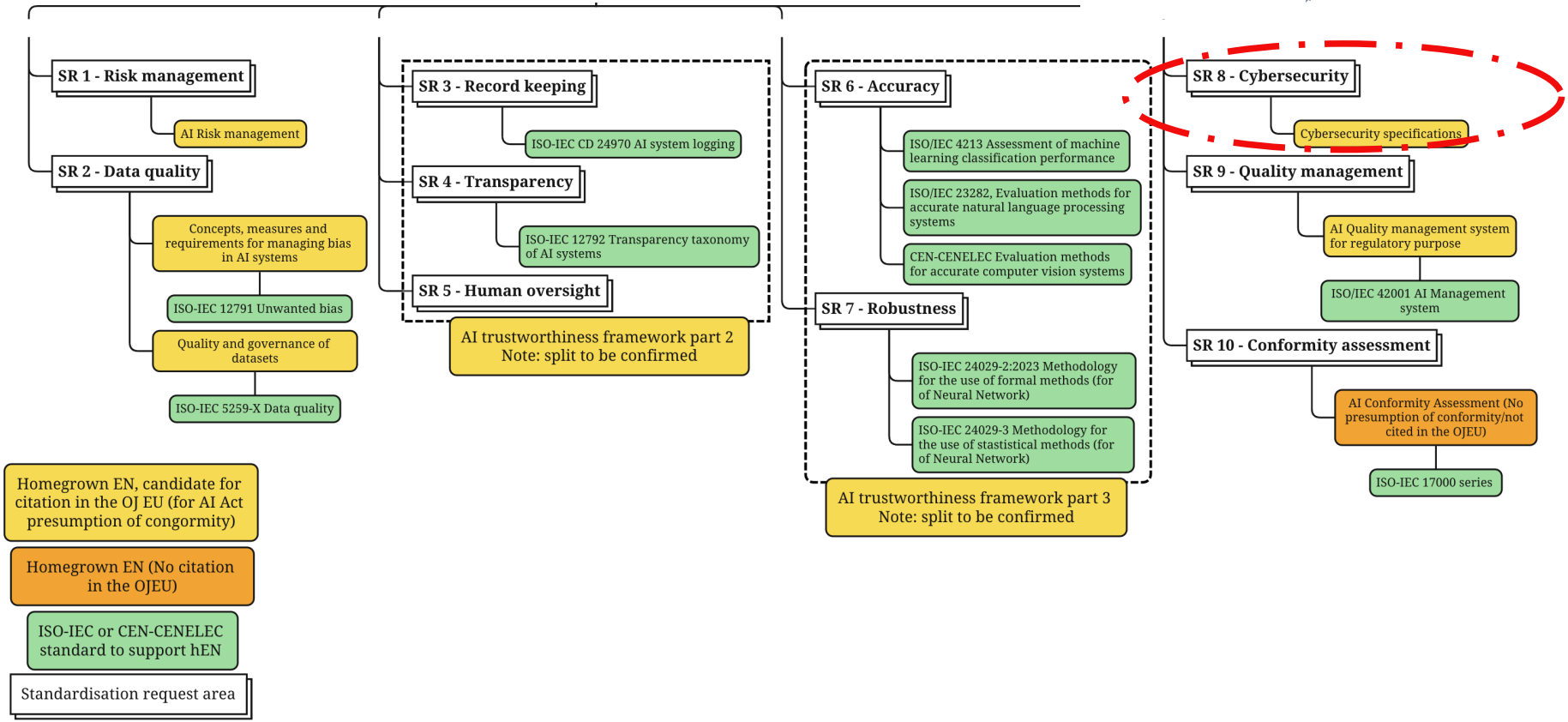
NA 043-01-42

“Mode 4”

Standardisation request of the European Commission

1.	European standard(s) and/or European standardisation deliverable(s) on risk management system for AI systems
2.	European standard(s) and/or European standardisation deliverable(s) on governance and quality of datasets used to build AI systems
3.	European standard(s) and/or European standardisation deliverable(s) on record keeping through logging capabilities by AI systems
4.	European standard(s) and/or European standardisation deliverable(s) on transparency and information provisions to the users of AI systems
5.	European standard(s) and/or European standardisation deliverable(s) on human oversight of AI systems
6.	European standard(s) and/or European standardisation deliverable(s) on accuracy specifications for AI systems
7.	European standard(s) and/or European standardisation deliverable(s) on robustness specifications for AI systems
8.	European standard(s) and/or European standardisation deliverable(s) on cybersecurity specifications for AI systems
9.	European standard(s) and/or European standardisation deliverable(s) on quality management system for providers of AI systems, including post-market monitoring process
10.	European standard(s) and/or European standardisation deliverable(s) on conformity assessment for AI systems

www.linkedin.com/in/sebastianhallensleben sebastian@haller


SR 1 - Risk management
AI Risk management
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
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
AI trustworthiness framework part 2
Note: split to be confirmed
SR 6 - Accuracy
ISO/IEC 4213 Assessment of machine learning classification performance
ISO/IEC 23282, Evaluation methods for accurate natural language processing systems
CEN-CENELEC 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 3
Note: split to be confirmed
SR 8 - Cybersecurity
Cybersecurity specifications
SR 9 - Quality management
AI Quality management system for regulatory purpose
ISO/IEC 42001 AI Management system
SR 10 - Conformity assessment
AI Conformity Assessment (No presumption of conformity/not cited in the OJEU)
ISO-IEC 17000 series
Homegrown EN, candidate for citation in the OJ EU (for AI Act presumption of congormity)
Homegrown EN (No citation in the OJEU)
ISO-IEC or CEN-CENELEC standard to support hEN
Standardisation request area

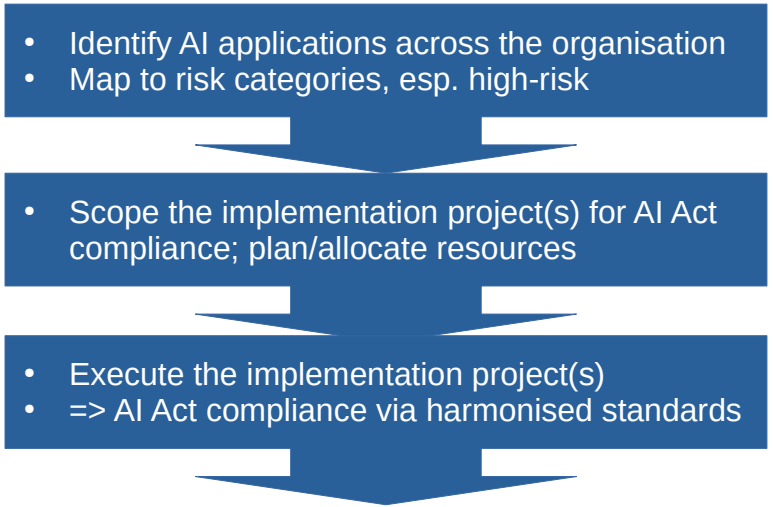
Working Groups

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

- 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)

Timeline

- CEN-CENELEC: AI Focus Group since **2019** | JTC21 since **2021**
- AI Act **final:** August 2024
- Stocktaking review by COM / AI Office **Feb 2025**
  => shared understanding of remaining gaps
- Public consultation for drafts of
  harmonised standards („**Enquiry Vote**“)
  mostly from **Q3 / 2025**
- Integration of feedback („**Comment Resolution**“)
  mostly in **Q4 / 2025** and early 2026 => mature content
- Implementation deadline high-risk requirements **Aug 2026**
- Formal processes in CEN-CENELEC and COM / AI Office
  for finalisation, harmonisation and OJEU publication



www.linkedin.com/in/sebastianhallensleben sebastian@hallensleben.org

JTC21 standards are currently distinct from the Code of Practice

	JTC21 harmonised standards	Code of Practice
Providing implementation steps for …	Requirements on AI systems in high-risk applications – Articles 8 to 15 • **All** types of AI • **Late** stage of value chain	Requirements on General Purpose Models – Articles 53, 55 • Generative AI **only** • **Early** stage of value chain
Development context and process	• Broadly applicable complex set of CEN-CENELEC regulations • Decision making power with standardisation bodies at national level who also provide secretarial support (~25 countries) • Input from ETSI (under Mode 4) • Input from ISO/IEC (under Vienna/Frankfurt agreements) • Ongoing feedback/guidance from EC at working level	• Custom process and structure created for CoP development purposes • Process directed by AI Office with outsourced facilitation support • Decision making power is with the AI Office

Initiation of a standardisation request based on the CoP expected for H2/2025.

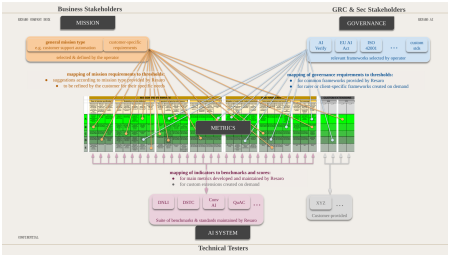
www.linkedin.com/in/sebastianhallensleben sebastian@hallensleben.org

Beyond consolidating horizontal AI governance frameworks: Mission-specific & performance-focused metrics

Currently initiated from within Resaro,
building industry “coalitions of the willing” to develop -

- vertical, mission-specific quality metrics, **including for security**
- thus creating a shared language for business, governance and technical teams to answer questions such as -
  - When is an AI solution “good enough” to go live?
  - Which one of several AI solutions is “better” in a given scenario?

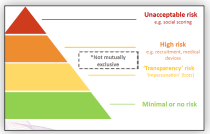
resaro



www.linkedin.com/in/sebastianhallensleben sebastian@hallensleben.org

DDG for Responsible Business Conduct

New Legislative Framework



	Allgemein	Elektrotechnik	Telekommunikation	
	ISO International Standardization Organization	JTC1 SC42 IEC International Electrotechnical Commission	ITU International Telecommunication Union	Inter-national
	cen Comité Européen de Normalisation	JTC21 CENELEC Comité Européen de Normalisation Electrotechnique	ETSI European Telecommunications Standards Institute	Europa
	DIN Deutsches Institut für Normung	NA 043-01-42 DKE VDE DIN Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE		Deutsch-land

Guidelines for Multinational Enterprises on Responsible Business Conduct

- Existing **enforcement mechanism**
- OECD ONE.AI Expert Group on AI Risk & Accountability is working towards adding a chapter on **AI Governance**
- **Points to broad range of existing AI risk management standards and frameworks** for practical implementation, including NIST RMF, ISO 31000, IEEE 7000, IEC Guide 51, ...