AI standardization in Europe

UNECE WP.6
Risk management and green, digital transformation conference

Dr Sebastian Hallensleben

Head of Digitalisation & AI at VDE e.V.

Chair CEN-CENELEC JTC 21

Co-Chair Classification & Risk Assessment OECD ONE.AI

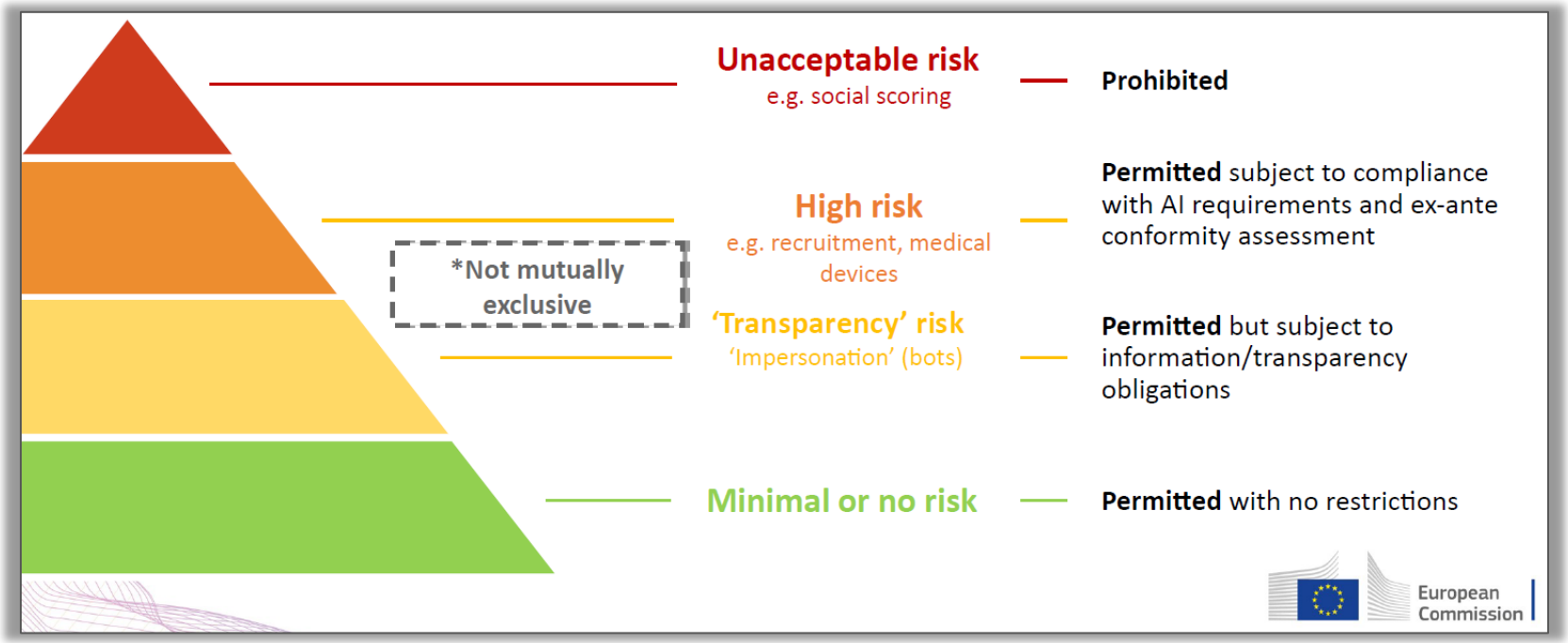
2024-04-02

VDE

Note from UNECE secretariat:

- *The author and the speaker of this presentation confirm that they have authorization to use all photos and visual elements.*
- *The material is either copyright-free or the author / speaker holds the necessary copyright.*
- *The UNECE will remove any material from its events and supporting websites if there is unlawful use of copyrighted material.*
- *The author / speaker takes responsibility for any infringements on copyright and holds the UNECE harmless to this effect.*

Risk in the EU AI Act:
High-level requirements only ⇒ Details to be defined elsewhere



New Legislative Framework - Principles and structure

(as presented by the European Commission)

European Commission

- **Essential requirements** designed to ensure a high-level of protection of public interests. They define the results to be attained, or the hazards to be dealt with, but do not specify the technical solutions for doing so
- **Harmonized standards** detailing technical solutions to meet the essential requirements
  - Voluntary – manufacturers can use other methods
  - Presumption of conformity with the essential requirements they cover
- **Division of responsibilities** along the value & distribution chain of the product
  - Manufacturers, importers, distributors, authorized representatives
- **Conformity assessment procedures**
  - Internal checks
  - Third-party assessment

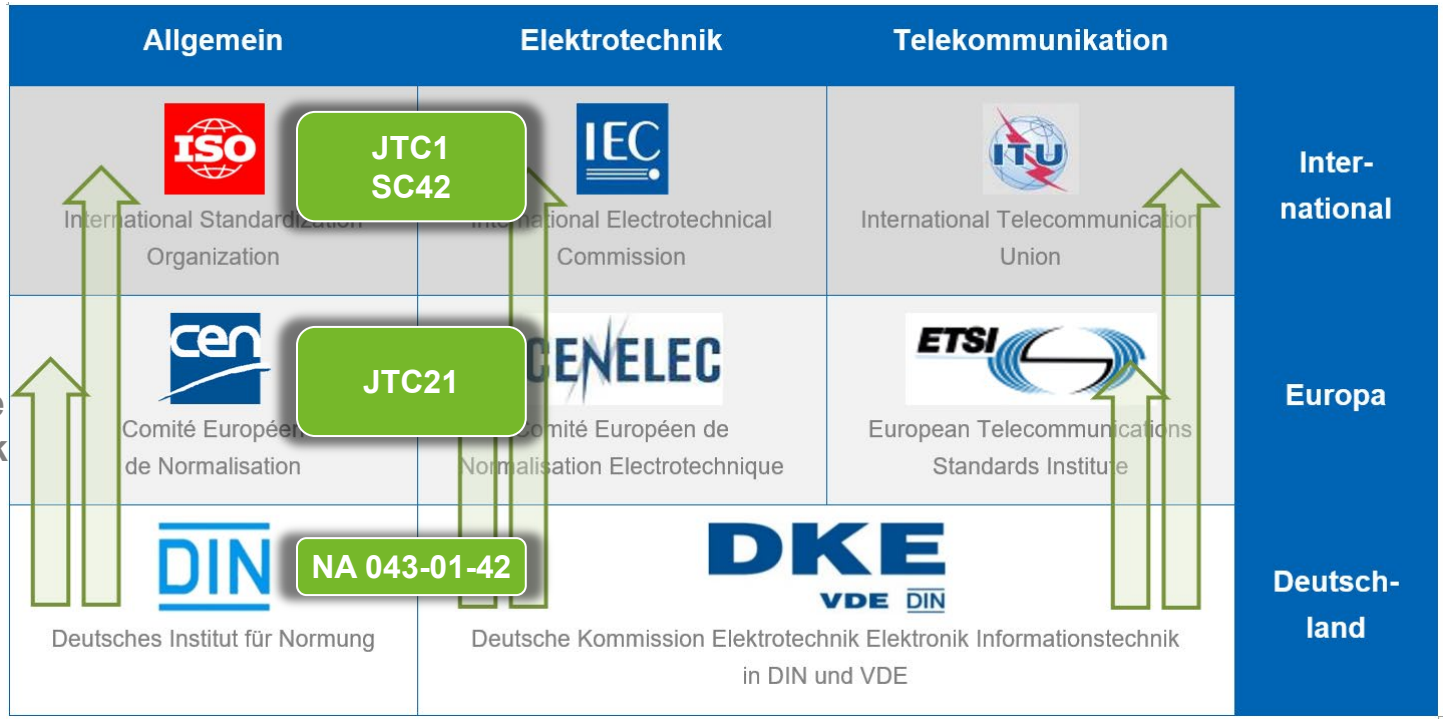
Standardisation request of the European Commission

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

Global three-tier standardisation landscape

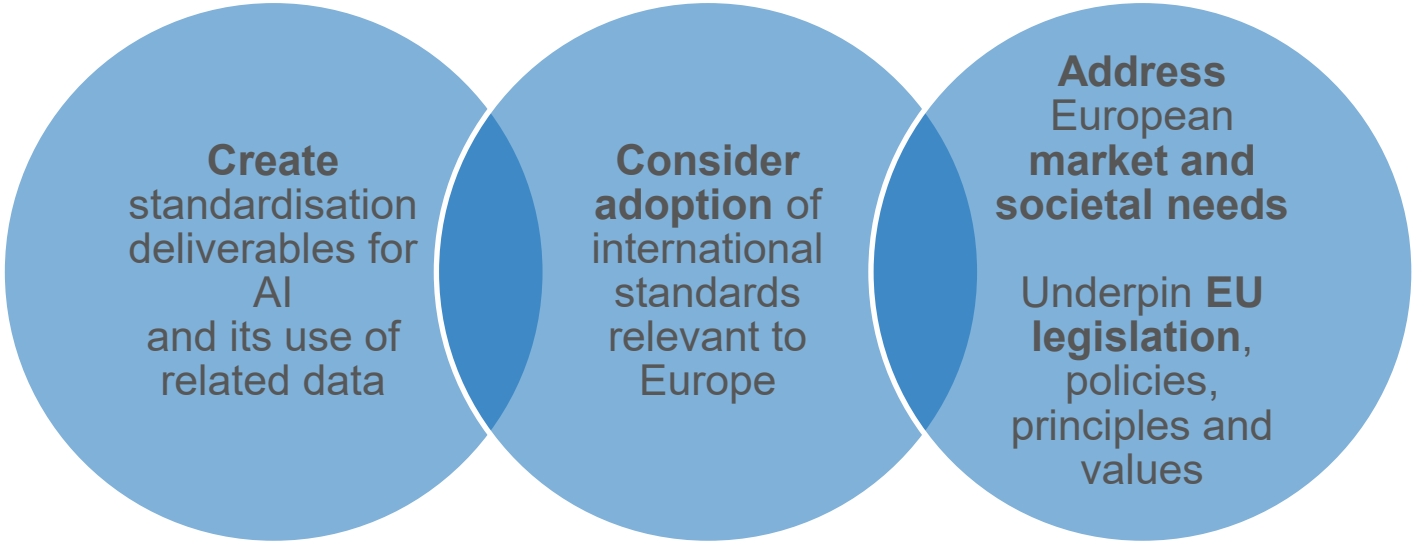
New Legislative Framework

AI Act



Mission of JTC21

> 140 experts
> 24 countries



Working Groups

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

WI Number	Reference	Type of deliverable	WG	Project editor	WP in response to SR	Already in JTC21 WP (according to standards.cencenelec.eu)	Title	Relationship with SC42 standard(s)	Stage code in JTC21	Status in JTC21	Stage code in JTC1	Status of underlying standard in ISO/IEC if applicable	…ting standards …ology (…)	…nagement for AI systems	…nce and quality of …ts used to build AI systems	…keeping through built-in capabilities in AI systems	…parency and information to …rs of AI systems	…n oversight of AI systems	…cy specifications for AI …s	…ness specifications for AI …s	…security specifications for …stems	…uality management system for …rs of AI system, including …market monitoring process	…rmity assessment for AI …s
JT021004	EN ISO/IEC 22989:2023	EN	WG4		-	-	Information technology - Artificial intelligence - Artificial intelligence concepts and terminology (ISO/IEC 22989:2022)	Adoption of 22989	Published	EN published	60	Standard published in 2022. Amendment 1 has been offered for parallel dev. Editor: Wei Wei (IBM, DE)	x										
JT021005	EN ISO/IEC 23053:2023	EN	WG4		-	-	Framework for Artificial Intelligence (AI) Systems Using Machine Learning (ML) (ISO/IEC 23053:2022)	Adoption of 23053	Published	EN published	60	Standard published in 2022. Amendment 1 has been offered for parallel dev. Editor: Milan Patel (Microsoft, UK)	x										
JT021022	prEN ISO/IEC	EN	WG4	Rania Wazir	-	-	Transparency taxonomy of AI systems	Parallel dev, ISO lead	Under Drafting		30	Editor: Rania Wazir (AT)	x										
	ISO/IEC 5259 part 1	EN	WG3	Adam Leon Smith	-	?	Data quality for analytics and machine learning (ML) Overview, terminology, and examples	Adoption of 5259-1	?	Parallel dev had been considered but was too late. NWIP approved by JTC 21 but awaiting clarification of comments before submission to BT for approval	40		x										
			WG3				Guidance for operational design domain and operating conditions of AI systems	Parallel development with ISO lead?		Informal preparatory discussions underway. Still to be discussed in WG4		Under discussion in WG3											
JT021011	prEN ISO/IEC 42001	EN	WG2	Marta Janaszewski	-	-	Information technology - Artificial intelligence - Management system	Adoption of 42001	Preliminary	NWIP to activate PWI approved by JTC 21 (but with No votes from DE/NL and concerns from EC). Now awaiting termination of FDIS voting in SC 42 before submission to BT for approval. Resolution of concerns tbd initially with WG2 convenor and project lead in December	60	Standard published				x						x	x
		EN	WG2		-		Adoption of existing quality management system in the AI Act context	Complementing 42001, building on 25058 and 25059?		Still to be initiated	60	Standards published (25059 Quality Model and 25058 Quality Guidance). However, these standards are not complete and do not contain requirements.		x									
JT021016	prEN ISO/IEC 23894	EN	WG2		-	-	Information technology - Artificial intelligence - Guidance on risk management - ISO/IEC 23894	Adoption of 23894	Under Enquiry	Adoption completed, but remark from Germany still to be discussed in 12/23; need to make sure this does not become a hEN. CEN Enquiry Ballot underway, closing 2024-01-11	60	Standard published		x									
~~JT021007~~	~~prCEN/EN XXX~~	~~EN~~	WG2		-	-	~~AI Risks - Check list for AI Risk Management~~		~~Preliminary~~	Included in NWIP on AI Risk Management (doc. N 472), see item below				x									
?	?	EN	WG2	Renaud di Francesco	-	-	AI Risk Management		Preliminary	CIB closed 2023-12-05, see N4… N534, approved by majority of NCs, waiting for BT approval				x									
JT021021	prEN XXX	EN	WG3	Adam Leon Smith	-	-	AI system logging	Parallel dev, ISO lead (under ballot)	Preliminary	CIB underway for parallel development, closing 2024-03-15, see N533	?	PWI online; detailed NWIP (almost CD level) in preparation				x							
JT021015	prEN ISO/IEC	EN	WG3	Arnault Ioualalen	-	-	Artificial intelligence (AI) - Assessment of the robustness of neural networks - Part 2: Methodology for the use of formal methods	Adoption of 24029-2	Preliminary		60	Same project editor (Arnault Ioualalen)								x	x		
	ISO/IEC 24029-3	EN	WG3		-		Artificial intelligence (AI) - Assessment of the robustness of neural networks - Part 3: Methodology for the use of statistical methods	Parallel dev?		Under development	20	NWIP approved								x			
	24029-4, -5		WG3				Artificial intelligence (AI) - Assessment of the robustness of neural networks - Part 4, 5: Methodology for the use of empirical/other methods	Parallel dev?		Still to be initiated	?	NWIPs in preparation								x			
		EN	WG3		-		Robustness taxonomy for NLP			Still to be initiated. Call for experts for robustness and accuracy did not get much response.										x			
		EN	WG3		-		Robustness taxonomy for computer vision			Still to be initiated										x			
		EN	WG3		-		Guidelines for robustness improvement			Still to be initiated										x			
		EN	WG3		-		Guidelines for robustness threshold definition			Still to be initiated										x			
		EN	WG3		-		Robustness assessment for non-neural AI systems (including other ML and symbolic AI)			Still to be initiated										x			
JT021012	prEN XXX	EN	WG3	Lauriane Aufrant	-	-	Accuracy of NLP systems	Parallel dev, ISO lead	Preliminary	NWIP to activate PWI as a parallel project with SC 42 lead approved by JTC 21, but is awaiting final approval by BT	?	Parallel dev approved, allocated to JWG5							x				
		EN	WG3		-		Accuracy for computer vision			Still to be initiated									x				
		EN	WG3		-		Guidelines for accuracy improvement			Still to be initiated									x				
		EN	WG3		-		Guidelines and requirements for accuracy threshold definition			Still to be initiated									x				
		EN	WG3		-		Accuracy of classification systems			Still to be initiated		Need to investigate how to leverage ISO/IEC TS 4213 as an EN							x				
		EN	WG3		-		Accuracy of AI systems for regression, recommendation and clustering			Still to be initiated									x				
		EN	WG4		-		Transparency of AI systems in the AI Act context			Still to be initiated. Complementing 12792. Alternatively, instead of a dedicated work item, integrating into the AI trustworthiness framework has been suggested.							x						
JT021008	prEN XXX	EN	WG4	Piercosma Bisconti	-	-	Artificial Intelligence trustworthiness framework		Preliminary	CIB underway, closing 2024-01-23, see N527						x	x	x	x	x	x		
JT021020	prEN ISO/IEC 8183	EN	WG3	Domenico Natale	-	-	Information technology — Artificial intelligence — Data life cycle framework	Adoption of 8183	Under Approval	Adoption was approved when it was at the FDIS stage. ISO/IEC 8183 has now been published, and prEN ISO/IEC 8183 should therefore be circulated by the CCMC for the final yes/no voting.	60	Published in 2023			x								
	ISO/IEC 5259 part 2	EN	WG3	Adam Leon Smith	-	?	Data quality for analytics and machine learning (ML) Data quality measures	Adoption of 5259-2	?	Parallel dev had been considered but was too late. NWIP approved by JTC 21 but awaiting clarification of comments before submission to BT for approval	40				x								
	ISO/IEC 5259 part 3	EN	WG3	Adam Leon Smith	-	?	Data quality for analytics and machine learning (ML) Data quality management requirements and guidelines	Adoption of 5259-3	?	Parallel dev had been considered but was too late. NWIP approved by JTC 21 but awaiting clarification of comments before submission to BT for approval	40				x								
	ISO/IEC 5259 part 4	EN	WG3	Adam Leon Smith	-	?	Data quality for analytics and machine learning (ML) Data quality process framework	Adoption of 5259-4	?	Parallel dev had been considered but was too late. NWIP approved by JTC 21 but awaiting clarification of comments before submission to BT for approval	40				x								
JT021007	prCEN/CLC/TR XXX	TR	WG3	Domenico Natale	-	?	Data Governance and quality for AI in the European context		?	Updated scope approved 2023-11-06/07					x								
	ISO/IEC 42006	EN	WG2		-		Requirements on bodies performing audit and certification of AI management systems	Adoption of 42006?		Still to be initiated	40	42006 at DIS stage, editor Suzanne Kook											x
		EN	WG2		-		Requirements on bodies performing audit and certification of AI systems			might not be needed; adaptation of 42006 might be sufficient?													x
	ISO/IEC 29119-11	EN	WG2		-		Testing of AI systems	Adoption of ISO/IEC 29119-11?		Still to be initiated	?	29119-11 has been a TR first and is now continuing to TS after having been held up for a year. Can also draw on ETSI work, DSI work. European specificities expected.											x
		EN	WG2		-		Competence requirements on AI systems auditors and professionals	n/a		Preparation underway for an NWIP (Q1/24?)													x
		EN	WG2		-		Conformity assessment framework in the context of the AI Act			NWIP planned (Q1/24?) take inspiration from cybersecurity conformity assessment; alignment with CASCO / blue guide tricky													x
	ISO/IEC 27000 series		WG5		-		Entire JTC 13; https://…			Some parts of the series are already adopted as ENs	60	Published									x		
	ISO/IEC 27090	EN	WG5		-		Guidance for addressing security threats and failures in artificial intelligence systems	tbd with JTC13; SC27 and ETSI		in focus	20	NWIP started in SC27, work at an early stage (20:00)									x		
	ISO/IEC 27091	EN	WG5 ?		-		Artificial Intelligence — Privacy protection	tbd with JTC13/SC 27 and ETSI		Requires discussion on where this would fit.	20	NWIP started in SC27, work at an early stage (20:60)									x		
JT013002	EN ISO/IEC 27001:2023	EN	WG5		-		ISO/IEC 27001:2022 (EN ISO/IEC 27001:2023) Information technology - Security techniques - Information security management systems - Requirements incl. Annex A with overview of controls (27002)	Basic Cybersecurity for AI [illegible]	Published (JTC13)	to be discussed with JTC13/SC 27 and WG 2		published in 2023; it is the main standard for information security management framework based on ISO/IEC High level structure for management systems		x	x	x					x	x	x
	EN ISO/IEC 27002:2023		WG5				ISO/IEC 27002:2022 related to Annex A from ISO/IEC 27001 Information security, cybersecurity and privacy protection - Information security controls (ISO/IEC 27002:2022)		Published (JTC13)	published, need to discuss with JTC 13		Detailed instruction about the controls from ISO 27001 Annex A									x		
	ISO/IEC 27005:2022		WG5				ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection. Guidance on managing information security risks.			published, need to discuss with JTC 13/SC27 and WG2, also in relation to 23894		in JTC1/SC27		x									
	ISO/IEC TR 6114:2023	TR	WG5				ISO/IEC TR 6114:2023 Cybersecurity. Security considerations throughout the product life cycle				60	in JTC1/SC27											
	ISO/IEC AWI TS 27115	TS	WG5				ISO/IEC AWI TS 27115 Cybersecurity evaluation of complex systems Introduction and framework overview				20												
	ISO/IEC 15408:2022 series 1-5		WG5				ISO/IEC 15408-1:2022 - serie Information security, cybersecurity and privacy protection Evaluation criteria for IT security.			should be discussed with JTC 13 /SC 27 and WG2	60												
…ar outside of the work programme in response to the Standardization Request or submitted September 2023																							
JT021006	prEN XXX	EN	WG4	Laurence Devillers		-	AI-enhanced nudging	Parallel dev, ISO lead	Under Drafting	Circulation of 1stWD, parallel dev suggested by WG4 convenor with dual editorship Europe / non-Europe (India) and agreed in WG4, but need to at least informally agree to keep coherence of scope and timeline. Fresh NWIP needed to remove European references. - Existing work in WG4 already quite mature.		Parallel development approved and formally suggested to JTC21											
JT021002	prCEN/CLC/TR XXX	TR	WG3	Lauriane Aufrant		-	Artificial Intelligence - Overview of AI tasks and functionalities related to natural language processing	Parallel dev, ISO lead	Under Drafting	Parallel development agreed in WG4. CIB underway, closing 2024-02-28, see N543		Parallel development approved and formally suggested to JTC21											
JT021018	prCEN/CLC/TR XXX	TR	WG4	Valeria Lisino		-	Information Technology - Artificial Intelligence - Green and Sustainable AI	Parallel dev rejected	Under Drafting	Circulation of 1stWD (text already mature), parallel dev rejected by WG4; suggest adoption by WG4		Parallel development had been formally suggested to JTC21											
JT021001	prCEN/CLC/TR 17894	TR	WG2	Emilia Tantar		-	Artificial Intelligence Conformity Assessment	Parallel dev rejected	Under Drafting	CIB underway, closing 2024-01-08, see N526		Parallel development had been formally suggested to JTC21											
JT021019	FprCEN/CLC ISO/IEC/TS 12791	TS	WG3	Adam Leon Smith		-	Information technology - Artificial intelligence - Treatment of unwanted bias in classification and regression machine learning tasks	Parallel dev, ISO lead	Under Approval	FV underway, closing 2024-02-01		Awaiting ISO to launch DTS voting											
JT021013	prEN XXX	EN	WG4	Enrico Panai		-	Competence Requirements for AI ethicists professionals		Preliminary	CIB underway, closing 2024-02-12													
JT021017	CEN/CLC ISO/IEC/TR 24027:2023	TR				-	Information technology - Artificial intelligence (AI) - Bias in AI systems and AI aided decision making	Adoption of 24027	Published	TR published		?											
JT021018	CEN/CLC ISO/IEC/TR 24029-1:2023	TR				-	Artificial Intelligence (AI) - Assessment of the robustness of neural networks - Part 1: Overview	Adoption of 24029-1	Published	TR published		?											
JT021014	prEN ISO/IEC	EN?	WG3	Adam Leon Smith		?	Software engineering - Systems and software Quality Requirements and Evaluation (SQuaRE) - Quality model for AI systems	Adoption of 25059	?	NWIP to activate PWI approved by JTC 21 but is awaiting approval by BT													

Structuring of cybersecurity work items still under discussion between JTC21/WG5, JTC13 and ETSI.

Entries shown here are provisional.

How can we build solid European harmonised standards in ~ 2 years (instead of 3-5 years)?

- Adopt or Adapt from ISO/IEC; Collaborate with ETSI
  (where available)
- Adapt from other standardisation and similar organisations,
  e.g. IEEE, IETF, W3C, OECD, GAIA-X, BDVA, …
  (where available and legal)
- Build on research and open consortial specs
  (where available)

Challenges in (AI) standardisation as an almost integral part of regulation (I)

- **Legitimacy**

  Theory: Consensus of „all relevant stakeholders“
  including companies of all sizes, academia, civil society,
  broad spectrum of countries, whole AI lifecycle, ...

  Practice: Who has got time, technical specialists and process knowledge?
  Documents vs. people

- **Very divergent interests**

  Global companies shape European standards
  Specific European perspectives and interests; sovereignty

Challenges in (AI) standardisation as an almost integral part of regulation (II)

- **Policy making vs. standardisation**
  Temptation to continue political battles in standardisation committees.
  Need to respect outcome of political processes.
- **International standards designed for a different purpose**
  Becomes a problem when these standards are considered for adoption in Europe.
  Differences in testability, enforcability, links to regulation
- **Personal talents needed**
  People with **technical** expertise
  People with **process** expertise
  People with **domain** expertise (health, energy, ...)
  People who **can write** (!)
  People who **can build consensus** (!!)

Participating in JTC21

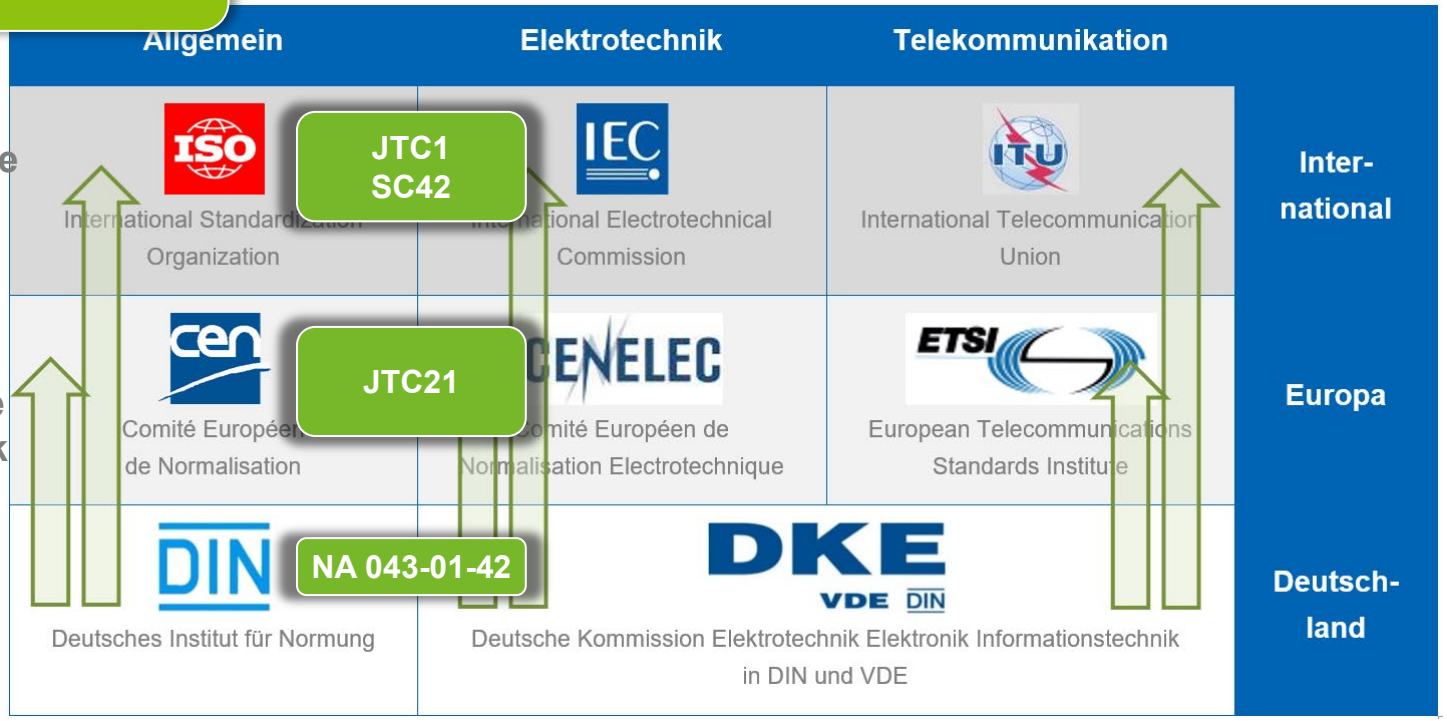
- **Through national AI mirror committees**
- **Through Annex 3 organisations**
- **Indirectly through liaisons**
  including other technical committees, associations, networks etc.
- **Through ETSI**
  Mode 4 cooperation in place, including (but not limited to) cybersecurity

- AI Risk Assessment
- G7 Hiroshima / Generative AI

DDG for Responsible Business Conduct

New Legislative Framework

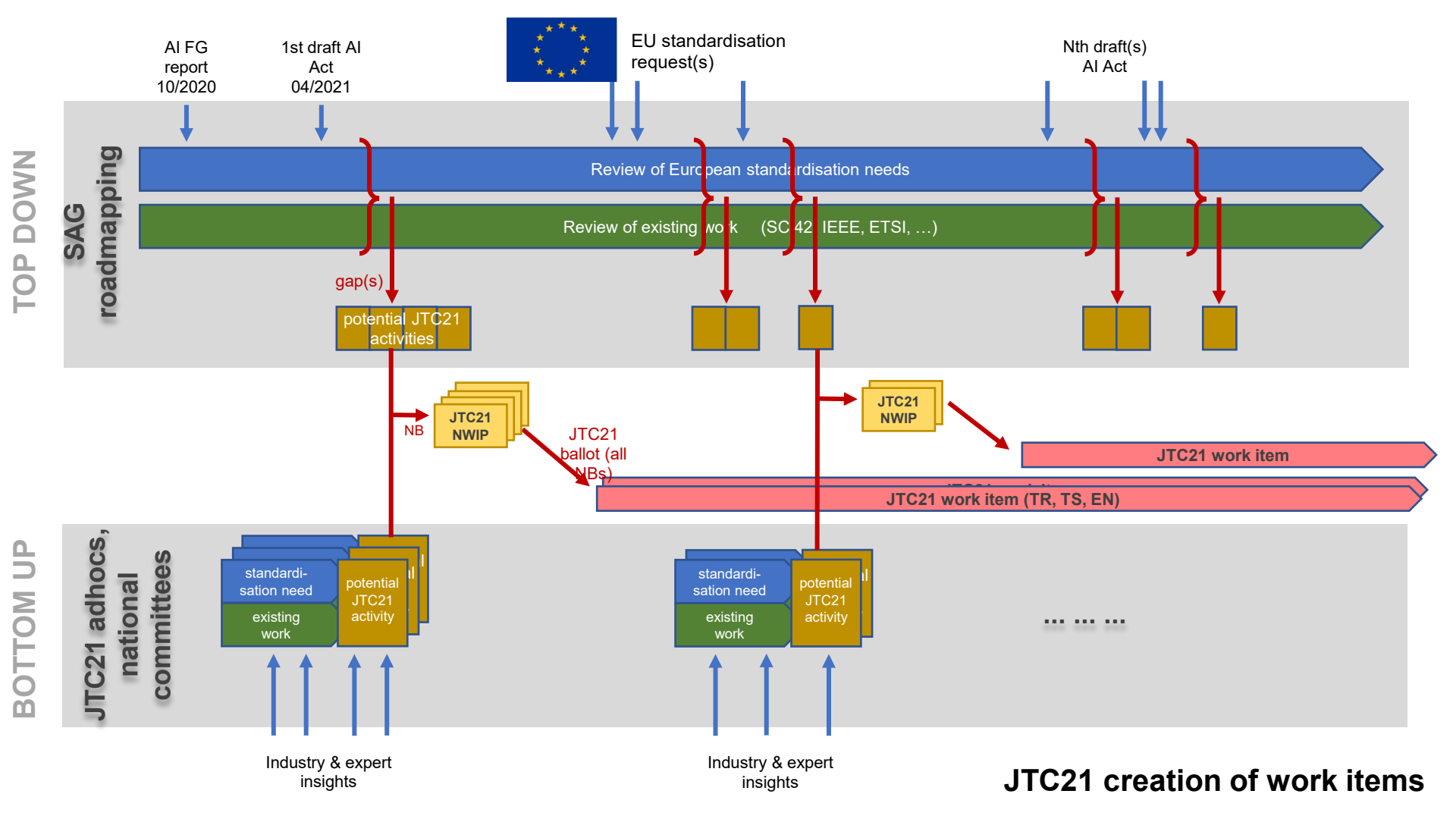
Draft AI Act



Thank you!

Dr Sebastian Hallensleben
Head of Digitalisation and AI

Tel: +49 170 791 6306
E-Mail: sebastian.hallensleben@vde.com


AI FG report 10/2020
1st draft AI Act 04/2021
EU standardisation request(s)
Nth draft(s) AI Act
TOP DOWN
SAG roadmapping
Review of European standardisation needs
Review of existing work (SC 42, IEEE, ETSI, …)
gap(s)
potential JTC21 activities
NB
JTC21 NWIP
JTC21 ballot (all NBs)
JTC21 NWIP
JTC21 work item
JTC21 work item (TR, TS, EN)
BOTTOM UP
JTC21 adhocs, national committees
standardi-sation need
existing work
potential JTC21 activity
standardi-sation need
existing work
potential JTC21 activity
… … …
Industry & expert insights
Industry & expert insights
JTC21 creation of work items