6 Article by article mapping of AI Act to ETSI Standardization programme

6.1 Mapping AI act to ETSI

Table 2: Article by article mapping to ETSI standards work

Article	Heading	Summary of Primary text	ETSI mapping
Chapter I, General provisions			
1	Subject matter	The purpose of this Regulation is to improve the functioning of the internal market and promote the uptake of human-centric and trustworthy Artificial Intelligence (AI), while ensuring a high level of protection of health, safety, fundamental rights enshrined in the Charter, including democracy, the rule of law and environmental protection, against the harmful effects of AI systems in the Union and supporting innovation.	This is addressed by ETSI's Directives and by the establishment of ETSI as an ESO under Regulation 1025/2012 [i.38] and subsequent revisions.
2	Scope	Identifies who is addressed by the regulation.	Not of direct relevance to ETSI as ETSI produces standards in order to allow those addressed by the scope to meet their obligations set by the regulation.
3	Definitions	Defines terms used in the document.	Mapped across ETSI's deliverables into a format that meets ETSI's drafting rules. Definitions in ETSI deliverables are not normative. All of the published terms used in ETSI's documents are listed on ETSI's TEDDI tool (https://webapp.etsi.org/Teddi/).
4	AI literacy	Providers and deployers of AI systems shall take measures to ensure, to their best extent, a sufficient level of AI literacy of their staff and other persons dealing with the operation and use of AI systems on their behalf, taking into account their technical knowledge, experience, education and training and the context the AI systems are to be used in, and considering the persons or groups of persons on whom the AI systems are to be used.	This is addressed in part in Annex A of the present document. The text in clause 4.3 of the present document also applies wherein it is identified that many of the general purpose reports prepared by ETSI can be seen as making provision for building that literacy.
Chapter II: Prohibited AI practices			
5	Prohibited AI practices	Lists practices that are prohibited.	As noted in clause 4.3 the mandate is framed as what cannot be done, whereas for standardization it has to be framed somewhat differently. This means what measures can be provided that, when followed, prevent the prohibited practices being placed in the market. Some of the mandates allow techniques to be applied only in very particular contexts. This may not be a standards issue unless the AI facility is sufficiently autonomous to be able to select its functionality based on context.

Article	Heading	Summary of Primary text	ETSI mapping
Chapter III: High Risk AI Systems			
SECTION 1: Classification of AI systems as high-risk			
6	Classification rules for high-risk AI systems	Rules for classifying and therefore determining if a system is high-risk.	As noted in clause 5.4 of the present document the scope statement of a standard, and the statement of purpose of a product (as defined in ETSI TS 104 224 [i.23]), will allow some indication of the likelihood of the resultant system being defined as high-risk.
7	Amendments to Annex III		As above.
SECTION 2: Requirements for high-risk AI systems			
8	Compliance with the requirements	States that all other parts of the section are mandatory and proof of compliance is required.	Not required.
9	Risk management system	A risk management system shall be established, implemented, documented and maintained in relation to high-risk AI systems. The risk management system shall be understood as a continuous iterative process planned and run throughout the entire lifecycle of a high-risk AI system, requiring regular systematic review and updating.	ETSI produces a number of documents aimed at containing risk. The application of the Cyber Security Controls series of ETSI TR 103 305 [i.36] (a multipart standard) to systems addresses all the lifecycle aspects requested and has applied those to AI in ETSI TR 104 030 [i.26]. At the more detailed technical assessment of risk the ETSI TS 102 165-1 [i.37] approach applies. The specific assessment of risk as applied to market placement of a product identified in ETSI TR 103 935 [i.34] may also apply.
10	Data and data governance	High-risk AI systems which make use of techniques involving the training of AI models with data shall be developed on the basis of training, validation and testing data sets that meet the quality criteria referred to in paragraphs 2 to 5 whenever such data sets are used.	In part this is addressed by the transparency and explicability obligations in ETSI TS 104 224 [i.23], and in the actions identified in the supply chain report (ETSI TR 104 048 [i.25]) and also by the traceability actions given in ETSI TR 104 032 [i.24].
11	Technical documentation	The elements required are defined in Annex IV and has to include a DoC as defined by Article 47.	This requires best practice of auditing of design and of the supply chain. Several standards exist that address this and are classified in ETSI TR 104 029 [i.2].
12	Record-keeping	Allow for the automatic recording of events over the lifetime of the system.	As stated in clause 4.3 of the present document the mandate is to automate recording of events over the duration of the lifetime of the system. While technical specifications for the security framework of AI computing platform prepared by ETSI TC SAI can support the mechanism of recording keeping by protect the integrity of the logs collected to guarantee the procedure for transparency and provision of information to deployers described in Article 13.
13	Transparency and provision of information to deployers	High-risk AI systems shall be designed and developed in such a way as to ensure that their operation is sufficiently transparent to enable deployers to interpret a system's output and use it appropriately.	The requirements stated in ETSI TS 104 224 [i.23] apply to both static and runtime transparency and explicability.

Article	Heading	Summary of Primary text	ETSI mapping
14	Human oversight	High-risk AI systems shall be designed and developed in such a way, including with appropriate human-machine interface tools, that they can be effectively overseen by natural persons during the period in which they are in use.	It is noted that Article 14 may inhibit the placement on the market of some autonomous systems and particularly of Agentic-AI systems. The discipline of Functional Safety (FS) applied to such systems may allow their deployment without direct involvement of "human in the loop" but rather allow for reasonable oversight by natural persons. The adoption of FS approaches in AI is an item of open study in ETSI.
15	Accuracy, robustness and cybersecurity	High-risk AI systems shall be designed and developed in such a way that they achieve an appropriate level of accuracy, robustness, and cybersecurity, and that they perform consistently in those respects throughout their lifecycle.	The topic of metrics for accuracy, robustness and cybersecurity is a topic gaining interest in ETSI and other SDOs. An initial requirement for this is provided as part of the transparency and explicability document, ETSI TS 104 224 [i.23].
SECTION 3: Obligations of providers and deployers of high-risk AI systems and other parties			
16	Obligations of providers of high-risk AI systems	As per the title.	Addressed across all of ETSI's AI output.
17	Quality management system	Providers of high-risk AI systems shall put a quality management system in place that shall be documented in a systematic and orderly manner in the form of written policies, procedures and instructions.	This is consistent with the guidance given for application of the Critical Security Controls of ETSI TR 103 305 [i.36] and ETSI TR 104 030 [i.26].
18	Documentation keeping	Requires records to be maintained for 10 years after placement on the market.	Not covered specifically in ETSI's AI portfolio but the general controls of ETSI TR 103 305 [i.36] apply.
19	Automatically generated logs	In each case the article title is deemed self-describing.	See clause 5.4 of the present document.
20	Corrective actions and duty of information		New work items establishing the AI Common Incident Expression (AICIE) alongside the development of the Universal Cybersecurity Information Exchange Framework (UCYBEX) apply.
21	Cooperation with competent authorities		Not applicable.
22	Authorised representatives of providers of high-risk AI systems		In ETSI TS 104 224 [i.23] (see also clause 5.4 of the present document) it is mandated that the liable party is identifiable across the supply chain.
23	Obligations of importers		Not an obvious domain for technical standards.
24	Obligations of distributors		
25	Responsibilities along the AI value chain		This is covered to an extent by each of ETSI TR 104 032 [i.24] and ETSI TR 104 048 [i.25]. It is also addressed in part in the transparency and explicability document ETSI TS 104 224 [i.23] in ensuring understanding of the value chain.
26	Obligations of deployers of high-risk AI systems		Not directly applicable.
27	Fundamental rights impact assessment for high-risk AI systems		The risk analysis methods developed in ETSI (e.g. ETSI TS 102 165-1 [i.37]) address harm in abstract terms and encourage assessment of rights of the stakeholders.

Article	Heading	Summary of Primary text	ETSI mapping
SECTION 4: Notifying authorities and notified bodies			
28 to 39	Various	Identifies specific actions of notifying authorities and notified bodies.	Not particularly of concern to SDOs but of particular interest to the process of making products and services available to the market. The SDO activity in this is addressed in Section 5 of the Act.
SECTION 5: Standards, conformity assessment, certificates, registration			
40	Harmonised standards and standardisation deliverables	Reinforces the role of hENs giving presumption of conformity.	As stated in clause 4.2 above "*an SDO cannot simply choose to publish an hEN, rather an hEN has to be written against specific actions of the EU*" , therefore ETSI at the time of preparation of the present document is not active in preparing hENs but will give assistance to relevant ESOs as stated in clause 5.2 above.
41	Common specifications	The Commission may adopt, implementing acts establishing common specifications for the requirements set out in Section 2 of this Chapter (Requirements for high-risk AI systems).	No current action (no implementing acts).
42	Presumption of conformity with certain requirements	Describes the normal process associated to presumption of conformity.	No specific actions or mapping at this time.
43	Conformity assessment		
44	Certificates		
45	Information obligations of notified bodies		
46	Derogation from conformity assessment procedure		
47	EU declaration of conformity		
48	CE marking		
49	Registration		
CHAPTER IV TRANSPARENCY OBLIGATIONS FOR PROVIDERS AND DEPLOYERS OF CERTAIN AI SYSTEMS			
50	Transparency obligations for providers and deployers of certain AI systems	Providers shall ensure that AI systems intended to interact directly with natural persons are designed and developed in such a way that the natural persons concerned are informed that they are interacting with an AI system, unless this is obvious from the point of view of a natural person who is reasonably well-informed, observant and circumspect, taking into account the circumstances and the context of use.	This is addressed by ETSI TS 104 224 [i.23] (see also clause 5.4 of the present document) for both static and run time conditions of the AI system.

Article	Heading	Summary of Primary text	ETSI mapping
CHAPTER V GENERAL-PURPOSE AI MODELS			
51	Classification of general-purpose AI models as general-purpose AI models with systemic risk	Various (applies much of prior chapters to models that are not specifically identified as high risk).	As for mappings in prior chapters.
52	Procedure		
53	Obligations for providers of general-purpose AI models		
54	Authorised representatives of providers of general-purpose AI models		
55	Obligations of providers of general-purpose AI models with systemic risk		
56	Codes of practice	The AI Office shall encourage and facilitate the drawing up of codes of practice at Union level in order to contribute to the proper application of this Regulation, taking into account international approaches.	ETSI has recently completed ETSI TS 104 223 [i.35] that has been developed from the UK Code of Practice after a public consultation involving many EU and global stakeholders.
CHAPTER VI MEASURES IN SUPPORT OF INNOVATION			
57 through 63	Various	The measures support a regulatory sandbox to allow stakeholders to develop and innovate in a controlled environment where regulators can facilitate testing whilst optimising regulatory oversight.	Not directly applicable but may be used in collaboration with the "proofs of concept" sandbox outlined in ETSI TR 104 067 [i.19].
CHAPTER VII GOVERNANCE			
64 to 69	Various	Establishes the AI Office and associated bodies.	No direct standards action expected, however ETSI may wish to ensure that communication from the AI Office and associated bodies is communicated to ETSI members.
CHAPTER VIII EU DATABASE FOR HIGH-RISK AI SYSTEMS			
71	EU database for high-risk AI systems listed in Annex III	The Commission shall, in collaboration with the Member States, set up and maintain an EU database containing information relating to the registration of high-risk AI systems.	No specific ETSI activity is foreseen.
CHAPTER IX POST-MARKET MONITORING, INFORMATION SHARING AND MARKET SURVEILLANCE			
72	Post-market monitoring by providers and post-market monitoring plan for high-risk AI systems		This is being addressed by the creation of new work items in both TC SAI and in TC CYBER to report and share vulnerability information, misbehaviour, and other risk factors. This work will specify the AI Common Incident Expression (AICIE) and work alongside the development of the Universal Cybersecurity Information Exchange Framework (UCYBEX).
73	Reporting of serious incidents		
74 to 94	Various	Addresses the organisation of market surveillance and how it interacts with other stakeholders.	

Article	Heading	Summary of Primary text	ETSI mapping
CHAPTER X CODES OF CONDUCT AND GUIDELINES			
95	Codes of conduct for voluntary application of specific requirements	The AI Office and the Member States shall encourage and facilitate the drawing up of codes of conduct, including related governance mechanisms, intended to foster the voluntary application to AI systems.	ETSI has recently completed ETSI TS 104 223 [i.35] that has been developed from the UK Code of Practice after a public consultation involving many EU and global stakeholders that may be instrumental in achieving the objectives of this article.
96	Guidelines from the Commission on the implementation of this Regulation	The Commission shall develop guidelines on the practical implementation of this Regulation [i.1].	As above.
CHAPTER XI DELEGATION OF POWER AND COMMITTEE PROCEDURE			
97	Exercise of the delegation	Addressed to EU.	Not applicable to ETSI.
98	Committee procedure		
CHAPTER XII PENALTIES			
99-101	Various	Identifies the penalties if a provider fails to comply to the requirements set out by the legislation.	Not strictly relevant to SDOs. Whilst SDO members may be subject to the identified penalties the role of the SDO here is to offer technical means that limit the risk of being subject to penalties.
CHAPTER XIII FINAL PROVISIONS			
102 - 110	Amendments to existing regulations	Identifies where existing regulation is directly impacted by the AI Act [i.1].	This will be further evaluated by TC SAI and OCG AI and actions given to relevant ETSI TBs where required.
111	AI systems already placed on the market or put into service and general-purpose AI models already placed on the marked	Large-scale IT systems that have been placed on the market or put into service before 2 August 2027 shall be brought into compliance with this Regulation by 31 December 2030.	No specific action from ETSI.
112	Evaluation and review	The Commission shall assess the need for amendment of the list set out in Annex III and of the list of prohibited AI practices laid down in Article 5, once a year following the entry into force of this Regulation.	No specific action from ETSI.
113	Entry into force and application	Applies from 2nd August 2026 with some exceptions: Articles 1 through 5 apply from 2nd February 2025 (i.e. in force now) Chapter III section 4 and others apply from 2nd August 2025. Article 6(1) applies from 2nd August 2027.	No specific action from ETSI. The harmonised standards required (see clause 5.2 of the present document) have to take account of these dates as hENs should be available to give presumption of conformity prior to the relevant in force dates.

6.2 Mapping ETSI TC SAI and ISG AI output to AI act

Table 2 can be presented in a different way that looks at some specific output of ETSI, in this instance from TC SAI, and mapping from the output back to specific articles of the AI Act [i.1]. Prior to this a summary of the security principles for AI, defined in ETSI TS 104 223 [i.35], is given. The intent of ETSI TS 104 223 [i.35] as indicated by its title is to define "Baseline Cyber Security Requirements for AI Models and Systems" and thus is intended to ensure, in addition to security of the AI model and system, that users of ETSI TS 104 223 [i.35] are able to prepare their products and services to be placed on the market and to conform to any applicable regulation including the AI Act [i.1].