

Scope discussion for ORC AI SIG

Step 1: Map the possible projects by looking at AI compliance from five angles, below

Step 2: Extract priorities from that mapping

The five angles (below) are Roles, Obligations, Organisations, Big Topics, Small Topics.

1.Roles

Providers	
Deployers	
Product manufacturers	
Importers & distributors	
Data centres (infrastructure/compute) California	

2.AI Act obligations

Prohibited Practices & AI Literacy 2 February 2025	
General-Purpose AI (GPAI) Rules 2 August 2025	
Transparency Obligations (Deployer-Facing) 2 August 2026	
Watermarking & New Prohibitions 2 December 2026	
Standalone High-Risk Systems (Annex III)	

2 December 2027	
Embedded High-Risk Systems (Annex I) 2 August 2028	

3. Who are we missing?

Hugging Face	
Mistral	
Black Forest Labs	
LUMI	
Check this list: https://www.microsoft.com/en-us/corporate-responsibility/topics/open-weight/	

4. Topics big enough for a white paper

Inventory of knowledge/resources	
What does Annex 1 of the CRA mean for an AI system; how can these requirements be met if the software is built by an AI agents	
Is there any noteworthy or significant overlap between how products are affected by the AI Act	

and the CRA? E.g., are product manufacturers obligated under the CRA to vulnerabilities in open-weight models to the model maintainer, and are open-weight model maintainers affected by Steward obligations?	
Current state and interplay between CRA hENs and AI hENs	

5. FAQ questions:

Should models be included in software? (e.g. no, but why?)	
What open source 'stewards' of agentic harnesses need to do in terms of compliance across both CRA & AI ? same question then for manufacturers that put these harnesses in production	
Solving social issues with licences, this is raised by the code of practice on transparency, and we got it fixed there, but this comes up repeatedly, so let's document it (no decision yet on whether to go broad enough to comment on RAILS)	
Definitions for things like: • AI system •	
When does an AI model become a product? GGUF & YAML	
