EU AI Act on High-Risk AI Systems: Technical Requirements & Solutions

**Philipp Bohlen, Artur Dox, David Drexlin,
Dimitrije Kovacic, Nicolai Pietrzyk, Lennart Schulze**
IMBIT - WWI2018E

DHBW
Duale Hochschule
Baden-Württemberg
Stuttgart

Research Scope

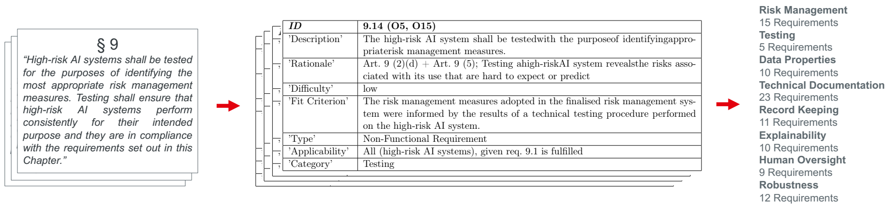
Artificial Intelligence, despite the exponential potential it unfolds for industry, science, and society, has been attributed to pose severe risks, such as erroneously processing personal data and making inexplicable influential decisions autonomously. After proposals by technical bodies, think tanks, intergovernmental organizations, and corporate entities, the European Union, in April 2021, was the first to conclusively answer the calls for a binding regulation, subsumed under the 'Ecosystem of Excellence and Trust in AI', addressing these threats with a proposal to define the rights, obligations, and constraints for stakeholders of AI systems in its member states[1].

However, the specific technical implications from legal regulations in technological sophisticated domains can be shallow and ambiguous, leaving developers and providers with uncertainty on how to act. In addition, discussions on the proposal are concerned with its sufficiency, granularity, and feasibility. To assist providers of high-risk AI systems aiming to comply and to reveal unresolved issues in the current draft of the regulation, a thorough technical analysis is conducted:

- *Which technical requirements for high-risk AI systems arise from the proposal?*
- *Which applicable software solutions can support satisfying these requirements?*
- *To what extent do they contribute to compliance and which coverage gaps remain?*

Key Results

1 A requirement analysis of articles 9 - 15 identified as relevant yielded 95 requirements composed to eight semantic categories as shown in more detail below.



§ 9
"High-risk AI systems shall be tested for the purposes of identifying the most appropriate risk management measures. Testing shall ensure that high-risk AI systems perform consistently for their intended purpose and they are in compliance with the requirements set out in this Chapter."

ID	**9.14 (O5, O15)**
'Description'	The high-risk AI system shall be testedwith the purposeof identifyingappropriaterisk management measures.
'Rationale'	Art. 9 (2)(d) + Art. 9 (5); Testing ahigh-riskAI system revealsthe risks associated with its use that are hard to expect or predict
'Difficulty'	low
'Fit Criterion'	The risk management measures adopted in the finalised risk management system were informed by the results of a technical testing procedure performed on the high-risk AI system.
'Type'	Non-Functional Requirement
'Applicability'	All (high-risk AI systems), given req. 9.1 is fulfilled
'Category'	Testing

Risk Management
15 Requirements
Testing
5 Requirements
Data Properties
10 Requirements
Technical Documentation
23 Requirements
Record Keeping
11 Requirements
Explainability
10 Requirements
Human Oversight
9 Requirements
Robustness
12 Requirements

2 Subsequently, based on these categories, 36 viable software solutions were identified which support satisfying the functional and non-functional requirements of at least one category to some degree if employed in a high-risk AI system. For an overview, the interested reader is referred to an extensive results dossier via the QR-code.

3 Finally, evaluating the three most academically relevant software solutions per category resulted in a total of 111 evaluations for 37 applicable requirements. The individual weighted fulfillment support scores aggregated by software solution and category range between 10% and 100% with an overall average of 33.8%, as displayed below.

Testing (4 req.)	**Score**
Amazon Sage Maker	33.33%
Watson OpenScale	58.33%
Azure ML	33.33%

Record Keeping (10 req.)	**Score**
TensorBoard	23.33%
Amazon CloudWatch	36.67%
DataDog	10.00%

Human Oversight (6 req.)	**Score**
SHapley Additive exPlanations (SHAP)	22.22%
Local Interpretable Model-Agnostic Explanation (LIME)	16.67%
MLflow	38.89%

Data Properties (7 req.)	**Score**
IBM SPSS Modeler	55.56%
SAP Data Services'	55.56%
Informatica Data Quality	25.93%

Explainability (1 req.)	**Score**
SHapley Additive exPlanations (SHAP)	66.67%
Local Interpretable Model-Agnostic Explanation (LIME)	66.67%
AIX360 Toolkit	100.00%

Robustness (9 req.)	**Score**
Foolbox Native	47.62%
IBM Adversarial Robustness Toolbox'	'38.10%'
CNN-Cert	23.81%

Conclusion

The EU AI Act proposal imposes a plenitude of obligations on high-risk AI systems. A total of 95 identified technical requirements can be observed by developers to facilitate compliance. While proven software solutions may aid in this endeavour, a dedicated solution focusing on non-functional and periphery management tasks such as human oversight and data governance is needed, notwithstanding substantial manual efforts.

Methodology

1 To translate regulatory obligations into formal software requirements, requirement engineering was performed in a five-step procedure[2] where the demand was elicited from the technologically relevant articles of the legal source through Semantic Parameterization[3] linguistic analysis.

2 The resultant requirements specification based on IEEE 29148 was thus semantically subdivided and non-AI-specific requirement groups were excluded. For the remaining groups, viable software solutions were researched in a systematic literature review[4] extracting details about solutions from academic and industrial publications, as well as each solution's academic relevance.

3 For each of the three most academically recognized solutions per category, a high-risk AI system employing it was verified regarding the concerned requirements through a documentation-based technical review process[5]. A solution can weakly, moderately, or strongly support fulfillment of a requirement, producing a weighted total score.

Future Work and Perspective

The AI Act proposal encourages the definition of technical specifications and standards to facilitate compliance with it, for whose complex agreement process this work may serve as first input. Agreeing with other evaluations, a revision of the draft must be more precise to become feasible. In response, new solutions to ease compliance shall be developed so as not to stall innovation in academia and industry.

References

» [1] "Proposal for a regulation of the European parliament and of the council laying down harmonised rules on artificial intelligence and amending certain union legislative acts," European Commission, 2021

» [2] B. Nuseibeh and S. Easterbrook, "Requirements engineering: a roadmap," in *Proceedings of the Conference on the Future of Software Engineering*, 2000, pp. 35–4

» [3] T. D. Breaux, M. W. Vail, and A. I. Anton, "Towards regulatory compliance: Extracting rights and obligations to align requirements with regulations," in *14th IEEE International Requirements Engineering Conference,* 2006, pp. 49 58.

» [4] J. Biolchini, P. G. Mian, A. C. C. Natali, and G. H. Travassos, "Systematic review in software engineering," *System Engineering and Computer Science Department COPPE/UFRJ, Technical Report ES 679/05*, 2005.

» [5] *IEEE Standard for Software Reviews and Audits*, IEEE Std. 1028-2008, 2008

bit.ly/AI-Act-Req-Paper-2021

Kontakt

Duale Hochschule Baden-Württemberg Stuttgart

Paulinenstraße 50
70178 Stuttgart

Studiengangsleitung: Prof. Dr. Marcus Vogt

Alle Informationen finden Sie unter: **www.dhbw-stuttgart.de**