*Legal Knowledge and Information Systems*
*J. Savelka et al. (Eds.)*

*doi:10.3233/FAIA241261*

# Design of a Quality Management System Based on the EU AI Act

Henryk MUSTROPH, Stefanie RINDERLE-MA
*Technical University of Munich, TUM School of Computation, Information and Technology, Garching, Germany*
ORCiD ID: Henryk Mustroph https://orcid.org/0009-0005-1946-1979, Stefanie Rinderle-Ma https://orcid.org/0000-0001-5656-6108

**Abstract.** The EU AI Act requires providers of high-risk AI systems to establish a Quality Management System (QMS) to monitor and document the AI system's design, quality, and risk. This paper introduces a new design concept for a QMS as a SaaS web application and demonstrates its feasibility with an implemented prototype. It connects directly to the AI system for verification and documentation and enables the orchestration and integration of various sub-services, each tailored to specific EU AI Act requirements. The prototype connects to the Phi-3-mini-128k-instruct LLM as an example AI system and includes a risk and a data management sub-service. The prototype is evaluated through an assessment of implemented requirements and feedback from IT, AI, and legal experts.

**Keywords.** EU AI Act, Quality Management System, AI Compliance Management

## 1. Introduction

Over recent years, the rise of Artificial Intelligence (AI) has introduced rapid advancements and heightened risks, particularly in critical sectors like medicine, finance, and law, where AI increasingly participates in or even controls decision-making processes. To have risks under control, the European Union (EU) Commission introduced the EU AI Act (AIA) in 2021, which came into legal force on 1 August 2024. Since 2021, researchers from the legal tech, and information systems community have been working on standardized and unified implementations of the AIA. Many are mainly concerned with developing theoretical ideas, processes, and frameworks on how AI compliance management can be organized in a standardized and organized way (cf. [1,2,3,4]). However, more research is needed on practical tools for efficiently implementing the AIA and involving humans in the AI compliance management process. For instance, a Quality Management System (QMS) responsible for verifying compliance is essential for demonstrating adherence to AIA regulations, particularly for high-risk AI systems. Therefore, this paper proposes a design concept for an all-in-one QMS solution illustrated in Figure 1. The goal is to offer a QMS as a Software-as-a-Service (SaaS) web application, which includes several sub-services that function as independent systems. These sub-services are organized into three core phases of the AI system lifecycle: *pre-development*, *post-development & pre-release*, and *post-release*. Each sub-service can be

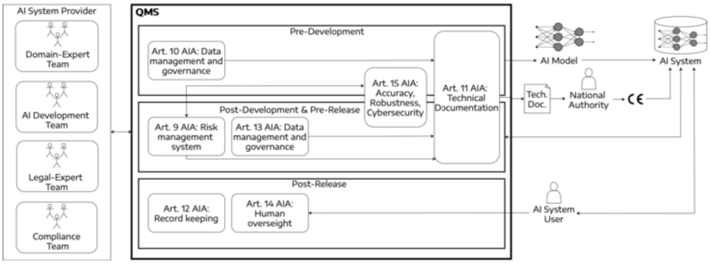
AI System Provider
Domain-Expert Team
AI Development Team
Legal-Expert Team
Compliance Team
QMS
Pre-Development
Art. 10 AIA: Data management and governance
Art. 15 AIA: Accuracy, Robustness, Cybersecurity
Art. 11 AIA: Technical Documentation
Post-Development & Pre-Release
Art. 9 AIA: Risk management system
Art. 13 AIA: Data management and governance
Post-Release
Art. 12 AIA: Record keeping
Art. 14 AIA: Human oversight
AI Model
AI System
Tech. Doc.
National Authority
CE
AI System User

Figure 1. Proposed design concept for a QMS based on the EU AI Act

individually designed to implement specific requirements of the AIA for high-risk AI systems. The QMS shall assist AI system providers in managing compliance, verification, and documentation processes for AI systems. It shall connect with the AI systems to perform technical assessments directly within the QMS. The sub-services shall interact with each other, allowing data to be transferred between them. For example, data from the sub-service addressing Art. 9 AIA can be incorporated into technical documentation, which can then be submitted to national authorities as proof of compliance. Such a QMS can enhance the traceability and reliability of AI compliance management, making it more transparent and allowing for continuous improvement through process mining techniques, as recommended by [5]. The paper begins with a review of related work (Sect. 2), followed by a description of the QMS prototype, including its requirements and architecture (Sect. 3). It then presents the evaluation (Sect. 4) and concludes with final remarks (Sect. 5).

## 2. Related Work

A summary of the AIA is given, followed by related work dealing with the AIA.

**EU AI Act:** The AIA [6] aims to regulate the development, deployment, and use of AI systems (Art. 3(1) AIA) and GPAI models (Art. 3(63) AIA) within the EU. The AIA categorizes AI systems into four risk classes, i.e., unacceptable risk (Art. 5 AIA), high risk (Art. 6 AIA), limited risk, and low risk. High-risk AI systems must adhere to the most challenging requirements (Chap. 3 Sect. 2 AIA). They must demonstrate through technical evaluation that despite being classified as high-risk, measures are in place to limit risks effectively through their whole lifecycle. For that, a QMS (Art. 17 AIA) must be established, which aims to structure a process to control all listed high-risk AI system requirements, verify the AI system design, and assure its quality. Legal experts note that many uncertainties remain in the AIA. [7] emphasizes that the AIA lacks specificity for implementing high-risk AI system requirements. [7,8] highlight the heavy bureaucratic demands and substantial resources needed for AI compliance management.

**EU AI Act in Literature:** Literature was searched, published in legal-tech (such as *JURIX*, *AI & Law*, *ICAIL*, and *AI and Ethics*), and information systems (such as *ICPM*, and *BPM*) journals and proceedings to identify theoretical, technical, and practical approaches to efficiently implement the AIA. Approaches for efficient, simplified risk class categorization under the AIA have been presented [9,10]. Some literature was found describing structured approaches to efficiently implement requirements for high-risk AI systems under the AIA. This includes strategies for Art. 9 AIA [11,12,13,14], as well as methods to enhance AI explainability to make black-box models more transparent, supporting compliance with Art. 13 AIA [15] and Art. 14 AIA [16]. Additionally, work discussing technical metrics to quantitatively assess AI systems' risks and limitations are presented as required in Art. 9 and 15 AIA [17,18,19]. Furthermore, research has been conducted to develop theoretical frameworks and processes for AI auditing, ensuring alignment with legal regulations like the AIA and ethical principles [1,2,3,20,21]. The business process management community has taken up the AIA in recent research. [4] use process modeling and execution to support reliable AI Fundamental Right Impact Assessment (cf. Art. 29a AIA). [5] emphasize the advantages of process mining for optimizing AI compliance management processes. Furthermore, practical AI compliance management systems like the proposed QMS approach have been introduced. For example, [22] present careAI, a web-based application that provides questions and checklists to evaluate an AI system's risks, limitations, and benefits. [23] offer capAI, a framework to reliably structure and conduct AI system conformity assessments. In contrast to the design concept proposed in this paper, these tools are more akin to project management frameworks and tools and do not enable technical assessments.

## 3. Quality Management System Design

The proposed QMS aims to support the AI compliance management process. First, the high-level requirements for structuring and implementing the QMS are outlined, followed by a description of the QMS architecture, designed to be modular and scalable, enabling connections to AI systems and featuring individual sub-services tailored to AIA requirements. The initial prototype QMS based on the proposed design concept connects to the Phi-3-mini-128k-instruct Large Language Model (LLM) [24] as an example AI system and includes a risk management (RMS) sub-service (cf. Art. 9 AIA) and a data management and governance (DMDGS) sub-service (cf. Art. 10 AIA). LLMs were chosen for this prototype due to their popularity and the availability of pre-trained, open-source models on Hugging Face[1]. To demonstrate the prototype QMS's capability for technical assessments on the connected LLM, three performance metrics, one gradient-based robustness metric, and one gradient-based explainability metric are implemented, further detailed in the technical report [25]. The prototype's code can be found in the repository [2] published on GitHub.

**Requirements:** The QMS requirements are grouped into *Legal Requirements* (LRs) and *System Design Requirements* (SDRs). The LRs shall primarily be based on the AIA, specifically covering high-risk AI system requirements outlined in Art. 9-15 AIA for each sub-service. Additionally, more detailed sub-service requirements can be elicited using information from different legal acts, ISO standards, or scientific literature. The SDRs, designed to support the QMS and sub-service implementation, are categorized into three sub-types: *human involvement*, *architecture*, and *computation and memory*. First, the user interface (UI) design and interaction specifications should encourage human involvement in checking and documenting AI systems. Second, architectural requirements should ensure a modular design, a smooth flow of data and communication between the sub-services, and easy maintenance. Third, computational requirements

[1] https://huggingface.co

[2] https://github.com/henryk-mustroph/first_version_qmsAIA.git

should guarantee the efficient execution of technical metrics, even for large AI systems such as LLMs, to maintain optimal memory consumption and performance. The high-level requirements are detailed in the technical report [25].

**Architecture:** The QMS architecture is based on a microservice design (cf. [26]). The prototype QMS consists of an RMS, a DMDGS, and a user authentication service containing their backend and database. The architecture of the prototype QMS is illustrated in Figure 2. Users can interact with the UI implemented on the frontend. An API Gateway backend service orchestrates all user requests from the frontend and forwards each request to the corresponding backend system. This data transfer structure and orchestration reduce complexity and improve modularity because adding sub-services to the QMS does not alter existing data transfers. In the initial prototype, the RMS verification component connects to the Phi3-mini-128k-instruct LLM. Technical metrics are implemented to demonstrate that the AI system can be quantitatively assessed within the RMS and, therefore, within the QMS. To enable a flexible implementation that supports various AI systems (e.g., LLMs), AI characteristics (e.g., performance, robustness, explainability), and specific methods based on these characteristics (e.g., gradient-based token importance for LLM explainability), the Strategy Pattern, a behavioral software design pattern [27] (p. 506), is used. Different model classes represent various AI systems, while distinct strategies represent AI characteristics, ensuring a flexible and extendable design. Additionally, all backends contain a communication component for frontend-backend-database communication and data transfer.

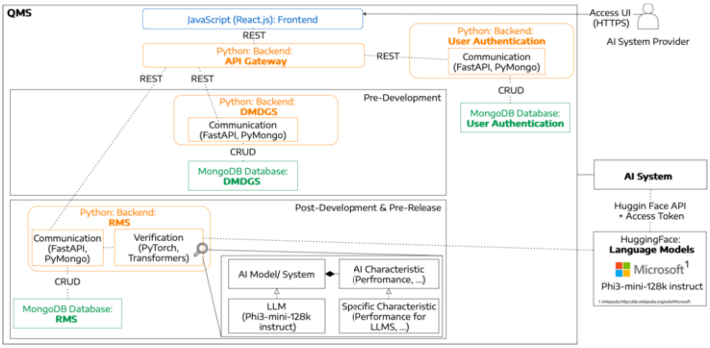
QMS
JavaScript (React.js): Frontend
REST
Python: Backend: API Gateway
REST
REST
REST
Python: Backend: User Authentication
Communication (FastAPI, PyMongo)
CRUD
MongoDB Database: User Authentication
Access UI (HTTPS)
AI System Provider
Pre-Development
Python: Backend: DMDGS
Communication (FastAPI, PyMongo)
CRUD
MongoDB Database: DMDGS
AI System
Huggin Face API + Access Token
HuggingFace: Language Models
Microsoft¹
Phi3-mini-128k instruct
Post-Development & Pre-Release
Python: Backend: RMS
Communication (FastAPI, PyMongo)
Verification (PyTorch, Transformers)
CRUD
MongoDB Database: RMS
AI Model/ System
AI Characteristic (Perfromance, ...)
LLM (Phi3-mini-128k instruct)
Specific Characteristic (Performance for LLMS, ...)

**Figure 2.** Prototype QMS Architecture

## 4. Evaluation

The prototype QMS is accessible at https://power.bpm.cit.tum.de/qmsAIA/. First, the requirements and implementation of the initial prototype are evaluated. Next, the design of the prototype is assessed through a workshop with IT and AI experts and an interview with a legal expert.

**Requirements:** The proof-of-concept prototype demonstrates the feasibility of the proposed QMS design concept that connects to an AI system for technical assessments and incorporates multiple sub-services, each serving a specific purpose. Human involvement is facilitated through a web-based, service-oriented application. The QMS prototype utilizes a microservice architecture, enabling a modular and loosely coupled design to integrate multiple sub-services. However, computational and memory demands pose challenges, particularly for huge AI models such as LLMs. For instance, the Phi-3-mini-128k-instruct, with 3.8 billion parameters, requires 30.4 GB of memory for a single forward and backward pass at full float32 precision. Reducing precision to float16 halves this requirement. The NVIDIA RTX 4090 GPU, with 24 GB of memory, can accommodate this LLM, which requires 15.2 GB in float16 to compute the implemented robustness and explainability metrics. The RMS is implemented based on the ISO 31000 guidelines [28] suggested by [13]. The RMS process includes component selection, risk identification, analysis, assessment, and mitigation activities. Additionally, it incorporates design principles such as human involvement and standardized structures outlined in [3] and utilizes technical metrics in the risk analysis step to assess the AI system's performance, robustness, and explainability. The DMDGS follows no specific verified design and is kept basic. Future work will focus on developing comprehensive, complete, and verifiable sub-services. To achieve this, ontology-based, vectorized database schemes may be implemented as proposed by [29], enabling the detailed design of sub-services tailored to AIA requirements and enriched with relevant information from associated ISO standards. This approach will facilitate the implementation, and execution of verified processes through workflow engines, as advocated by [4].

**IT, AI, and Legal Experts:** Following the guidelines provided in [30], a workshop with seven experts in information systems, business process management, and AI was conducted. A presentation and prototype QMS live demo were provided, continuing with a focus-group discussion. Five of seven experts in the workshop agreed that such a QMS would help increase efficiency when technically assessing AI systems, even if they mentioned that complex tasks might require manual inspection. LLMs whose outputs have no pre-defined ground truth could be challenging to check automatically within the QMS. Additionally, an interview with a legal expert following a qualitative content analysis (QCA) was performed according to [31]. The legal expert evaluated the prototype positively. It was mentioned that the QMS has a sound, precise design and is, therefore, easy to use, even for auditors with legal expertise but possibly less AI expertise, such as potential auditors for national authorities or internal compliance team members and auditors. Furthermore, it was confirmed that the QMS should be broad enough to accommodate and document all types of AI systems, including those not classified as high-risk, simplifying any AI system's internal compliance management process. Since only eight experts from different domains have been asked, future work will expand the evaluation by engaging a larger group of experts.

## 5. Conclusion

This paper introduces a design concept for an all-in-one QMS as a web application that simplifies compliance verification and documentation for AI systems. Unlike most existing QMS tools, which primarily serve as project management tools to guide compliance processes, this design enables direct assessment of AI systems within the QMS. The concept is demonstrated with a proof-of-concept prototype. Future work will further develop the various sub-services and conduct a broader evaluation to make the QMS even more comprehensive.

## References

[1] Clarke R. Principles and business processes for responsible AI. Computer Law and Security Review. 2019;35(4):410-22. doi:10.1016/j.clsr.2019.04.007.

[2] Mökander J, Schuett J, Kirk HR, Floridi L. Auditing large language models: a three-layered approach. AI and Ethics. 2023:1-31. doi:10.1007/s43681-023-00289-2.

[3] Ortega E, Tran M, Bandeen G. AI Digital Tool Product Lifecycle Governance Framework through Ethics and Compliance by Design†. In: IEEE Conference on Artificial Intelligence - CAI. IEEE; 2023. p. 353-6. doi:10.1109/CAI54212.2023.00155.

[4] Novelli C, Governatori G, Rotolo A. Automating Business Process Compliance for the EU AI Act. In: Legal Knowledge and Information Systems - JURIX. IOS Press; 2023. p. 125-30. doi:10.3233/FAIA230955.

[5] Pery A, Rafiei M, Simon M, van der Aalst WMP. Trustworthy Artificial Intelligence and Process Mining: Challenges and Opportunities. In: Process Mining Workshops - ICPM. Springer; 2021. p. 395-407. doi:10.1007/978-3-030-98581-3_29.

[6] European Union. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (Artificial Intelligence Act). Publications Office of the European Union; 2024. Official Journal of the European Union. Available from: http://data.europa.eu/eli/reg/2024/1689/oj.

[7] Bormhard/ Siglmüller. AI Act – das Trilogergebnis. Recht Digital - RDi. 2024;2:45-96.

[8] Schallbruch M. EU-Regulierung der Künstlichen Intelligenz: Informationstechnische Systeme im Fokus neuer rechtlicher Anforderungen. Datenschutz und Datensicherheit - DuD. 2021;45:438-43.

[9] Hanif H, Constantino J, Sekwenz M, van Eeten M, Ubacht J, Wagner B, et al. Tough Decisions? Supporting System Classification According to the AI Act. In: Legal Knowledge and Information Systems - JURIX. IOS Press; 2023. p. 353-8. doi:10.3233/FAIA230987.

[10] Golpayegani D, Pandit HJ, Lewis D. To Be High-Risk, or Not To Be - Semantic Specifications and Implications of the AI Act's High-Risk AI Applications and Harmonised Standards. In: ACM Conference on Fairness, Accountability, and Transparency - FAccT. ACM; 2023. p. 905-15. doi:10.1145/3593013.3594050.

[11] Novelli C, Casolari F, Rotolo A, Taddeo M, Floridi L. Taking AI risks seriously: a new assessment model for the AI Act. AI and Society. 2023:1-5. doi:10.1007/s00146-023-01723-z.

[12] Xia B, Lu Q, Perera H, Zhu L, Xing Z, Liu Y, et al. Towards Concrete and Connected AI Risk Assessment (C2AIRA): A Systematic Mapping Study. In: IEEE/ACM 2nd International Conference on AI Engineering - Software Engineering for AI - CAIN. IEEE; 2023. p. 104-16. doi:10.1109/CAIN58948.2023.00027.

[13] Tjoa S, Temper PKM, Temper M, Zanol J, Wagner M, Holzinger A. AIRMan: An Artificial Intelligence (AI) Risk Management System. In: International Conference on Advanced Enterprise Information System - AEIS. IEEE; 2022. p. 72-81. doi:10.1109/AEIS59450.2022.00017.

[14] Nagbøl PR, Müller O, Krancher O. Designing a Risk Assessment Tool for Artificial Intelligence Systems. In: 16th International Conference on Design Science Research in Information Systems and Technology - DESRIST. Springer; 2021. p. 328-39. doi:10.1007/978-3-030-82405-1_32.

[15] Sovrano F, Sapienza S, Palmirani M, Vitali F. A Survey on Methods and Metrics for the Assessment of Explainability under the Proposed AI Act. In: Legal Knowledge and Information Systems - JURIX. IOS Press; 2021. p. 235-42. doi:10.3233/FAIA210342.

[16] Górski L, Ramakrishna S. Challenges in Adapting LLMs for Transparency: Complying with Art. 14 EU AI Act. In: Legal Knowledge and Information Systems - JURIX. IOS Press; 2023. p. 275-80. doi:10.3233/FAIA230974.

[17] Giudici P, Centurelli M, Turchetta S. Artificial Intelligence risk measurement. Expert Syst Appl. 2024;235:121220. doi:10.1016/j.eswa.2023.121220.

[18] Bhaumik D, Dey D. An Audit Framework for Technical Assessment of Binary Classifiers. In: 15th International Conference on Agents and Artificial Intelligence - ICAART. SCITEPRESS; 2023. p. 312-24. doi:10.5220/0011744600003393.

[19] Steimers A, Bömer T. Sources of risk and design principles of trustworthy artificial intelligence. In: International Conference on Human-Computer Interaction - HCI. Springer; 2021. p. 239-51.

[20] Ellul J, Pace G, McCarthy S, Sammut T, Brockdorff J, Scerri M. Regulating artificial intelligence: a technology regulator's perspective. In: 18th International Conference on Artificial Intelligence and Law - ICAIL. ACM; 2021. p. 190–194. doi:10.1145/3462757.3466093.

[21] Simbeck K. They shall be fair, transparent, and robust: auditing learning analytics systems. AI Ethics. 2024;4(2):555-71. doi:10.1007/S43681-023-00292-7.

[22] Thelisson E, Verma H. Conformity assessment under the EU AI act general approach. AI Ethics. 2024;4(1):113-21. doi:10.1007/S43681-023-00402-5.

[23] Floridi L, Holweg M, Taddeo M, Amaya J, Mökander J, Wen Y. CapAI-A procedure for conducting conformity assessment of AI systems in line with the EU artificial intelligence act. Available at SSRN 4064091. 2022.

[24] Abdin MI, Jacobs SA, Awan AA, Aneja J, Awadallah A, Awadalla H, et al. Phi-3 Technical Report: A Highly Capable Language Model Locally on Your Phone. CoRR. 2024;abs/2404.14219. doi:10.48550/ARXIV.2404.14219.

[25] Mustroph H, Rinderle-Ma S. Design of a Quality Management System based on the EU Artificial Intelligence Act. CoRR. 2024;abs/2408.04689. doi:10.48550/ARXIV.2408.04689.

[26] Nadareishvili I, Mitra R, McLarty M, Amundsen M. Microservice architecture: aligning principles, practices, and culture. " O'Reilly Media, Inc."; 2016.

[27] Brügge B, Dutoit AH. Object-oriented software engineering - using UML, patterns and Java (2. ed.). Prentice Hall; 2004.

[28] International Organization for Standardization. ISO 31000:2018 - Risk management — Guidelines. International Organization for Standardization - ISO; 2018. Available from: https://www.iso.org/iso-31000-risk-management.html.

[29] Hernandez J, Golpayegani D, Lewis D. An Open Knowledge Graph-Based Approach for Mapping Concepts and Requirements between the EU AI Act and International Standards. CoRR. 2024;abs/2408.11925. doi:10.48550/ARXIV.2408.11925.

[30] Thoring K, Müller RM, Badke-Schaub P. Workshops as a Research Method: Guidelines for Designing and Evaluating Artifacts Through Workshops. In: 53rd Hawaii International Conference on System Sciences - HICSS. ScholarSpace; 2020. p. 1-10. Available from: https://hdl.handle.net/10125/64362.

[31] Gläser J, Laudel G. Experteninterviews und qualitative Inhaltsanalyse als Instrumente rekonstruierender Untersuchungen. 3rd ed. Wiesbaden: VS-Verl; 2009.