Introducing an AI Governance Framework in Financial Organizations

Best Practices in Implementing the EU AI Act

Sergio Genovesi
SKAD AG, Frankfurt am Main, Germany

Abstract

To address the challenges of AI regulation and the EU AI Act's requirements for financial organizations, we introduce an agile governance framework. This approach leverages existing organizational processes and governance structures, integrating AI-specific compliance measures without creating isolated processes and systems. This framework combines immediate measures to address urgent AI compliance cases with the development of a broader AI governance. It starts with an assessment of requirements and risks, followed by a gap analysis; after that, appropriate measures are defined and prioritized for organization-wide execution. The implementation process includes continuous monitoring, adjustments, and stakeholder feedback, facilitating adaptability to evolving AI standards. This procedure guarantees not only adherence to current regulations but also positions organizations to be well-equipped for prospective regulatory shifts and advancements in AI applications.

2012 ACM Subject Classification General and reference → Empirical studies

Keywords and phrases AI Governance, EU AI Act, Gap Analysis, Risk Management, AI Risk Assessment

Digital Object Identifier 10.4230/OASIcs.SAIA.2024.9

Category Practitioner Track

Acknowledgements Many thanks to Dennis Kautz and Kim Strunk for their valuable feedback and insights. Thanks to Felix Broßman, Daniel Schulz und Helge Krill for their trust and support.

1 AI Regulation and the Financial Sector

Artificial Intelligence (AI) is transforming the financial sector by powering advisory services, enhancing risk management, and improving compliance and fraud detection. AI drives innovation through automated data analysis and personalized marketing and sales strategies while boosting operational efficiency. However, AI's rapid integration into business processes brings substantial challenges regarding regulatory complexities and potential legal issues [7]. Implementing AI can create unanticipated risks, necessitating tailored approaches for safe operation. Moreover, AI incidents can impact public perception and pose reputational concerns. Traditional risk management approaches lack the required technical depth and fall short in addressing the various AI implications, highlighting the need for specialized AI governance practices.

In the European context, to use and deploy AI in the financial sector, it is necessary to navigate a complex regulatory environment – recently intensified by the addition of the EU AI Act [12]. The EU AI Act joins a suite of important existing regulations, such as the General Data Protection Regulation (GDPR) [8], the Digital Markets Act [9], the Data Act [11] and the Data Governance Act [10], as well as sector-specific rules and standards such as the EBA Guidelines [2] or, in Germany, the German Banking Act [1] and the BaFin minimal requirement for risk management (MaRisk) [6], collectively shaping the responsible deployment and management of the digital infrastructure and services in the financial sector.

The EU AI Act adopts a risk- and technology-based regulatory approach, introducing different risk categories for AI systems, ranging from unacceptable, high, or systemic risk to limited risk. High-risk applications, used in sensitive fields like credit scoring or recruiting, which could have adverse effects on individuals and society, will be subject to transparency, data governance, and risk and quality management requirements – among others. Sanctions for non-compliant organizations are strict, with fines reaching €35 million or up to 7% of global annual turnover, emphasizing the critical need for financial organizations to enhance their governance structures and implement rigorous monitoring and audit procedures.

These requirements build upon those for data technology and IT assets introduced by the aforementioned regulations, adding AI-specific obligations. For instance, Article 10 of the EU AI Act, which regulates Data and Data Governance, aligns with GDPR provisions regarding the processing of personal data while introducing data governance practices aimed at training, validation, and testing datasets for AI systems.

In the context of establishing a systematic risk management framework, the MaRisk requirements already set an important benchmark concerning risk assessment and management for IT systems, including both technical and organizational measures to ensure the integrity, availability, authenticity, and confidentiality of the data. While addressing new AI-specific threats is a defining feature of the AI Act, the overlaps concerning "classic" IT risks affecting AI systems as well as the design of risk management frameworks are evident. The EU AI Act itself encourages the integration of AI-specific risk management measures within existing frameworks (see, for example, Article 9, paragraph 10). As we will see more specifically in the next section, these overlaps allow organizations to include new AI specific compliance measures in their existing compliance frameworks.

2 Implementing an AI Governance Strategy in Financial Organization

2.1 Assigning responsibilities within existing functions

Since the AI governance requirements of the EU AI Act intersect with several operational fields that are already subject to a variety of regulations, a strategic incorporation of new organizational measures across different departments is necessary.

To individuate the most suitable business processes and departments for the implementation of AI requirements in specific operational fields, it is possible to refer to the three lines of defence (LoD) model – a widespread risk governance framework in financial organizations [3]. According to Engels et al., "[t]he 3LoD model caters for coordination of control responsibilities among various stakeholders [...]. This is achieved by allocating and delineating distinct roles and mandates to business and operational functions in the 1st LoD, internal control and standard setting functions in the 2nd LoD as well as internal audit in the 3rd LoD". [3, p. 97]. Focusing specifically on the internal controls established by different functions in the 2nd LoD, it is possible to highlight possible overlaps and synergies between existing controls and new measures. This analysis facilitates a thematic clustering and helps delineate precise task, enabling a clearer division of responsibilities for assigning working packages necessary for implementing specific requirements.

The following list includes operational fields within the 2LoD that according to our analysis are affected by the EU AI Act, and briefly describes to what extent:

- **Information Security / Risk Management** faces significant implications, including the need for AI-specific asset categorization and vulnerability assessments, as well as the management of unique AI risks and a reevaluation of compliance measures.

- **Operational Risk Management** must calculate and allocate sufficient resources for potential AI-related damages and consider insurance options specifically for AI risks, acknowledging that AI can introduce new variables and uncertainties into the operational risk framework.
- **Data Governance** is a critically impacted area, necessitating new measures addressing the accuracy of output, possible biases in training data, and the overarching management of data quality, among other things.
- **Outsourcing and Vendor Management** is affected not only by the necessity for robust contractual clauses that cover AI specifics but also by the heightened attention to supply chain risks and the requirement for continuous risk analysis and monitoring of service level agreements (SLAs) in relation to AI suppliers and vendors.
- **Compliance** functions will need to adjust existing practices to ensure adherence to new legal AI regulations and requirements, and stay up to date with the latest standards to ensure AI trustworthiness. Especially concerning Generative AI use cases, it will be important to understand the implications for copyright and trademark laws concerning training data and generated content.
- **Data Protection** teams are responsible for ensuring the proper management of personal data within AI systems, overseeing transnational data processing activities, and maintaining the security of sensitive data categories.

Effective collaboration between the aforementioned functions and IT and other specialized departments is crucial for the successful adherence to AI regulatory requirements. Moreover, communication among affected stakeholders to coordinate implementation measures in case of partial overlap is key to optimizing the division of tasks and ensuring the success of the new governance strategy. This cross-departmental cooperation is likely to feature the utilization of decentralized risk management modules as integral components of the frontline risk management strategy. To ensure that all relevant risks are addressed, the organization's management board may decide to appoint a new role to supervise the progress of work. This role can be integrated into existing departments and added to the responsibilities of current positions.

2.2 Agile Implementation Methodology

Recognizing the overlap with other ongoing risk governance processes, the proposed approach does not create additional structures dedicated to AI governance and EU AI Act compliance, but integrates and expands upon existing frameworks. This integration ensures that the measures taken are rooted in the existing operational structure, promoting a seamless transition to an AI-ready compliance and risk management strategy.

Adopting this strategy initiates with a comprehensive briefing and planning phase. This step involves a thorough scoping of the organization's needs and strategic goals, defining the level of ambition, and identifying key stakeholders. Informed by this insight, project planning and governance are established and consolidated in a collaborative kick-off with all stakeholders.

This is followed by an assessment phase dedicated to understanding the applicable regulatory environment and the identification of AI-specific risks. At this stage, the status quo with regard to AI governance is investigated as well. These assessments lay the groundwork for the gap analysis phase, where existing governance is evaluated against new regulatory standards, allowing for the precise definition and prioritization of necessary measures that span across all levels of the organization.

Once defined, the new measures are systematically implemented. During the implementation phase, regulatory developments are closely monitored to ensure ongoing alignment and fast adjustment to new standards and requirements. Finally, the process naturally progresses to an optimization phase, which aims at bringing iterative enhancements to the organization (including communication strategies and customized training). This phase allows for the establishment of a Continuous Improvement Process (CIP) for the ongoing development of AI governance, rounding off with the comprehensive completion of the project and assimilation of stakeholders' feedback.

This strategy adopts an agile framework, incorporating both bottom-up and top-down procedures. Bottom-up workflows address immediate compliance needs by focusing on AI use cases necessitating urgent action. Simultaneously, an overarching AI governance framework is designed based on a top-down analysis of the EU AI Act requirements and of the identified compliance gaps, pinpointing necessary enhancements to organizational processes and systems.

In applying this agile methodology, strategy developers ensure a prompt response to immediate compliance requirements while constructing a comprehensive, resilient, and sustainable AI governance infrastructure that is well-equipped for future advancements.

2.3 Examples: Best Practices and First Steps within different 2nd LoD functions

In this section, examples of first steps in implementing the EU AI Act requirements in two different 2LoD are presented. The functions considered are Information Security and Risk Management, and Outsourcing and Vendor Management.

Information Security and Risk Management

To comply with the AI Act, organizations must first assess AI-specific risks and undertake a risk classification for each AI system in use or development. Since IT risk assessments are usually performed by information security departments, the classification of AI systems and the attribution of adequate risk management controls can be integrated into the existing Information Security Management System (ISMS) and supported by the Governance, Risk, and Compliance (GRC) software already in place.

To facilitate the governance objective of identifying and classifying AI specific risks, the following first steps can be taken:

- Expand the threat catalogue in order to include potential threats and vulnerabilities associated with AI systems. In order to do so, the ENISA Threat Landscape reports published in 2020 [4] and 2023 [5] can be taken as a reference. This task involves evaluating AI specific points of vulnerability and new kind of cyberattacks targeting AI inherent weaknesses.
- Update the Configuration Management Database (CMDB) and the IT Asset Inventory to include AI-specific risk by introducing new IT asset categories that explicitly classify AI systems based on their risk levels. Considering the definitions included in Article 3, 6, 50 and 51 of the EU AI Act, the following categories should be included: AI system, high-risk AI system, general purpose AI system, general purpose AI system with systemic risk, AI system with transparency obligations. Additionally, any AI systems that fall under the forbidden practices outlined in Article 5 must be immediately discontinued.

- Compare current risk management measures with AI-specific ones to assess the necessity of adjusting existing cybersecurity protocols for mitigating AI-related threats. If current measures already fulfill the AI Act requirements (such as those concerning IT documentation and logging activities), introducing new controls should be avoided to prevent redundancies in the ISMS. Only unaddressed requirements necessitate new controls.

Once high-risk-systems are correctly flagged in the ISMS and in the GRC software, it is possible to implement adequate risk management measures to ensure the systems meet the EU AI Act requirements. To achieve this, it is necessary to focus on several key actions that integrate AI-specific controls and processes into existing information security frameworks. These actions include:

- Identify specific controls for AI systems and map these controls to relevant use cases within the organization. In alignment with the agile implementation strategy presented above, as well as with the EU AI Act provisions for risk management systems (Art. 9), the feasibility of integrating these controls into existing risk management systems should be evaluated.
- Establish a system for ongoing compliance assessment to ensure adherence to established controls. Whenever possible, automate the steps of the compliance assessment to increase efficiency.
- Establish clear decision-making processes, with a special focus on risk acceptance. This entails consulting relevant internal stakeholders throughout the AI system life-cycle to assign specific roles and responsibilities.

Outsourcing and Vendor Management

Many IT products and services used by financial organizations are not developed internally but are provided by third-party vendors. Thus, implementing the EU AI Act requirements necessitates robust due diligence and effective management of these third-party relationships to ensure compliance and mitigate risks associated with outsourcing and vendor management.

To facilitate the governance objective of third-party due diligence, the following first steps can be taken:

- Flag AI-related third-party relationships within the organization's contract database or outsourcing register. This helps in identifying all relevant stakeholders who contribute to or influence AI systems used by the organization.
- Adjust third-party assessment processes by incorporating AI-specific risk categorization and requirements. This involves refining existing risk assessment methods to address the unique risks associated with AI technologies.
- Enforcing requirements in third-party relationships by creating specific contract clauses for AI systems that cover data processing, security requirements, limitation of liabilities, and other critical aspects as mandated by the EU AI Act.

Regarding the governance objective of managing third-party AI systems, the following actions should be taken:

- Create the necessary information basis by establishing links between relevant systems, such as the ISMS and the contract database or outsourcing register, to ensure information is consistently updated and accessible to those managing third-party relationships.
- Identify, assess, and manage third-party AI-risks on an ongoing basis. This involves regular third-party risk assessments, followed by appropriate risk management measures.
- Conduct routine audits and reporting activities concerning relevant contractual partners to check for non-compliance with the EU AI Act.

3 Conclusion

Adapting to the EU AI Act requires financial organizations to integrate AI-specific compliance measures into their existing governance frameworks. By leveraging an agile implementation strategy, organizations can address immediate regulatory requirements and build a robust AI governance structure for the long term.

The regulatory landscape for AI is expected to evolve, with new rules and challenges emerging as AI technologies advance. Financial organizations should prepare for continuous adjustments to their governance practices and anticipate further regulatory changes. By adopting a flexible and integrated approach to AI governance, they can ensure compliance with the current EU AI Act requirements while preparing for future regulatory and technological advancements.

References

1 Bundesregierung. Gesetz über das kreditwesen (kredwg), 2023. Available online: https://www.gesetze-im-internet.de/kredwg/index.html (Accessed: 2024-08-24).

2 European Banking Authority (EBA). Revised guidelines on outsourcing arrangements, 2019. Available online: https://www.eba.europa.eu/activities/single-rulebook/regulatory-activities/internal-governance/guidelines-outsourcing and PDF: https://www.eba.europa.eu/sites/default/files/documents/10180/2551996/38c80601-f5d7-4855-8ba3-702423665479/EBA%20revised%20Guidelines%20on%20outsourcing%20arrangements.pdf (Accessed: 2024-08-24).

3 Dr. Oliver Engels, Marc Peter Klein, Peter Gürtlschmidt, Dr. Georg Lienke, and Rei Tanaka. The three lines of defence model: Key success factors for effective risk management. In *Non-Financial Risk Management in the Financial Industry*, pages 71–88. Frankfurt School Verlag, 2022. Available at: https://www.frankfurt-school-verlag.de/programm/non_financial_risk_management.html. URL: https://www.frankfurt-school-verlag.de/programm/non_financial_risk_management.html.

4 European Union Agency for Cybersecurity (ENISA). Artificial intelligence cybersecurity challenges, 2020. Available online: https://www.enisa.europa.eu/publications/artificial-intelligence-cybersecurity-challenges (Accessed: 2024-09-12).

5 European Union Agency for Cybersecurity (ENISA). Enisa threat landscape 2023, 2023. Available online: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023 (Accessed: 2024-09-12).

6 Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin). Rundschreiben 05/2023 (ba) - mindestanforderungen an das risikomanagement - marisk, 2023. Available online: https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Rundschreiben/2023/rs_05_2023_MaRisk_BA.html (Accessed: 2024-08-24).

7 Dr. Jochen Papenbrock, Dr. John Ashley, Dr. Georg Lienke, Florian Seiferlein, and Norbert Gittfried. Optimising effectiveness and efficiency: Deployment of artificial intelligence in non-financial risk management. In *Non-Financial Risk Management in the Financial Industry*, pages 213–239. Frankfurt School Verlag, 2022. Available at: https://www.frankfurt-school-verlag.de/programm/non_financial_risk_management.html. URL: https://www.frankfurt-school-verlag.de/programm/non_financial_risk_management.html.

8 European Union. Regulation (eu) 2016/679 of the european parliament and of the council of 27 april 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/ec (general data protection regulation), 2016. Available online: https://eur-lex.europa.eu/eli/reg/2016/679/oj(Accessed: 2024-09-12).

9 European Union. Regulation (eu) 2022/1925 of the european parliament and of the council of 14 september 2022 on contestable and fair markets in the digital sector and amending directives (eu) 2019/1937 and (eu) 2020/1828 (digital markets act), 2022. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32022R1925(Accessed: 2024-09-12).

10 European Union. Regulation (eu) 2022/868 of the european parliament and of the council of 30 may 2022 on european data governance and amending regulation (eu) 2018/1724 (data governance act), 2022. Available online: https://eur-lex.europa.eu/eli/reg/2022/868/oj(Accessed: 2024-09-12).

11 European Union. Regulation (eu) 2023/2854 of the european parliament and of the council of 13 december 2023 on harmonised rules on fair access to and use of data and amending regulation (eu) 2017/2394 and directive (eu) 2020/1828 (data act), 2023. Available online: https://eur-lex.europa.eu/eli/reg/2023/2854(Accessed: 2024-09-12).

12 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, 2024. Available online: https://eur-lex.europa.eu/eli/reg/2024/1689/oj(Accessed: 2024-09-12).