International Journal of Computational and Experimental Science and ENgineering (IJCESEN)

Vol. 11-No.2 (2025) pp. 3414-3819
http://www.ijcesen.com

ISSN: 2149-9144

Copyright © IJCESEN

Research Article

AI Governance and Responsible AI Frameworks for Enterprise Software Systems

Pavan Koppula*

Salesforce CRM, Enterprise AI Solutions, Google, Austin, Texas, USA
*** Corresponding Author Email:** pavan.koppula92@gmail.com

Article Info:

DOI: 10.22399/ijcesen.5559
Received : 05 February 2025
Revised : 26 March 2025
Accepted : 28 March 2025

Keywords

AI Governance,
Responsible AI,
Enterprise Software,
EU AI Act,
NIST AI RMF,
ISO/IEC 42001

Abstract:

This research study examines the area of AI governance and responsible AI frameworks in enterprise software solutions with regard to global trends in adoption, comparison of different frameworks, elements of governance, and organisational influence. The research methodology is secondary analysis based on academic literature, industry reports, regulations, and case studies. From the research findings, there is a difference in global adoption, which includes strict enforcement of the EU AI Act in Europe, voluntary adoption of the NIST AI Risk Management Framework in North America, and inconsistent adoption in the Asia Pacific region.
Comparative analysis reveals the distinctions regarding scope and enforceability in various frameworks, such as ISO/IEC 42001 and OECD AI Principles, whereas governance-related elements, like bias detection, explainability, audit trails, and human oversight, are seen as crucial control mechanisms. In addition, case examples of Air Canada's responsibility regarding a chatbot and iTutorGroup's hiring policy demonstrate the risks that arise when governance frameworks are not strong enough. Thus, the research concludes that integrated frameworks consisting of regulatory compliance, technical controls, and organisational accountability provide a higher level of compliance and reputation management.

1. Introduction

Integration of AI technologies into the software systems of enterprises is widespread today, with the global investment in AI predicted to surpass USD 500 billion in 2027. However, governance mechanisms encouraging responsible use of AI are missing. According to Gartner, 30% of interactions between enterprises and generative AI will be performed through autonomous agents by 2028, while 79% of IT managers are sceptical about the validity of the results of AI owing to their biased and unexplainable nature. The compliance guidelines offered by the EU AI Act and ISO/IEC 42001 are hard to implement, and in India, where spending on AI has grown by 119% per year, only 22% of companies have risk assessment procedures (Golpayegani *et al*. 2022). This situation illustrates the need for the integration of governance principles into the architecture of the enterprise. For instance, Air Canada faced the issue of liability for misleading information about the fare policy presented by a chatbot. Moreover, iTutorGroup had to pay a settlement of USD 365,000 for discrimination against employees caused by the AI technology.
The problem statement revolves around the absence of an integrated governance framework that combines technical controls with organisational responsibility. The use of AI technology by companies often does not go through a proper oversight process, resulting in shadow AI systems, biased decisions, and legal issues. The responsible AI framework should incorporate all of the above-mentioned elements into one.

2. Related Work

In the literature on AI governance and responsible AI frameworks in the context of enterprise software systems, one can see how there is an intersection between regulatory requirements, corporate responsibility, and socio-technical security. Academics emphasise the importance of governance not only to mitigate risks related to biases, opaqueness, and regulations but also to promote innovation. In this regard, the European Union AI Act is often cited as an innovative regulation which imposes different tiers of

obligations regarding transparency, documentation, and human supervision (Laux *et al*. 2024). Other paradigms, such as Responsible Innovation Theory and Socio-Technical Systems Theory, also demonstrate that it is important to include ethics both in technology and organisational architectures. By 2027, enterprise AI investments will exceed USD 500 billion. According to Gartner research, 79% of IT professionals do not trust results generated by AI because of biases and explainability issues.

Case studies demonstrate the consequences of bad governance practices. Such as, the problem of liability of Air Canada's chatbot was an example of the risk associated with la ack of regulation of AI communication technology, while ITutorGroup had to pay $365,000 due to discrimination in hiring that resulted from its compliance issues (eeoc.gov, 2023). Guidelines for implementing accountability include, for example, the NIST AI Risk Management Framework and ISO/IEC 42001. However, they are not used on a global scale. It has been noted by scholars that organisations tend to deploy AI quickly without any governance and, therefore, operate in a shadow AI environment. One of the main problems associated with responsible AI implementation is that businesses usually do not have comprehensive strategies, which include both technical and accountability measures and, as a result, generate bias and decrease stakeholder trust (Haefner *et al*. 2023).

3. Research Methods

Secondary research methodology has been employed in this research to analyse the issues relating to the governance of AI and responsible AI frameworks in enterprise software systems. The sources of secondary data were chosen from academic peer-reviewed journal articles, industry reports, regulations and organisational case studies to ensure that the study encompasses all practices of AI governance on a global level (Kuo, 2022). The source materials for this study have been collected from the Gartner surveys, OECD reports on the policies related to AI, ISO/IEC 42001 standards, and compliance reports pertaining to the EU AI Act. This methodology assisted in making a comparison of different perspectives and identifying some common issues of AI governance, including bias, lack of transparency and regulatory exposure. There are many benefits of using secondary data. Some of them are access to large-scale data sets and validation of the evidence without the constraints of primary data collection.

4. Key findings and data analytics

Global Adoption of AI Governance Frameworks in Enterprise Software Systems

As indicated by the latest study, only 12% of businesses across the world have advanced AI governance practices despite the fact that the use of AI is universal in ERP, HR, and cloud technologies. In Europe, with the implementation of the EU AI Act, the uptake of AI governance practices has become very high since businesses have developed a risk-tiered compliance approach to avoid €35 million penalties or 7% of their revenues. In North America, the uptake of AI has been seen among businesses because of the presence of the voluntary AI Risk Management Framework formulated by NIST (Bonney *et al*. 2024). According to the latest executive survey by Morgan Stanley involving 200 executives, 56% consider data risk as the primary risk factor, whereas 41% concentrate on human oversight in the case of risky AI applications. In the APAC region, national AI governance guidelines are present in Singapore and Japan. However, the rapid increase in investments in AI in Indian enterprises is not supported by the governance models. As per the case analysis of IEEE Global Enterprise AI Governance Review, enterprises usually adopt a hybrid approach consisting of regulatory compliance as well as voluntary standards.

Comparative Evaluation of Major AI Governance Frameworks

As far as the comparative evaluation of the governance frameworks for AI is concerned, there seem to be significant differences in their scope, enforcement, and application. As regards the most comprehensive governance framework in its scope, the EU's AI Act deserves special attention due to the risk-based model and the consequences of not adhering to the rules. As regards the US, NIST's AI Risk Management Framework envisages a voluntary approach and risk management (AI, 2024).

Alignment with Ethics and Global Agreement are important aspects of the OECD AI Principles, yet there is no technology framework in this case. As is known from research, firms tend to apply all the above principles at once for their compliance with regulations, flexibility, and ethics. Therefore, European businesses apply the EU AI Act alongside ISO, while US businesses refer to the NIST RMF (Cotteleer *et al*. 2021).

Governance Components Required for Enterprise AI Systems

Some elements of governance required in enterprise AI are those of ensuring technology, accountability, and compliance. The detection of any biases is

important in order to mitigate the danger of biased outputs and can be explained through an example of hiring policies in iTutorGroup. Explainability creates a framework for trust in AI, given the fact that Gartner found 79% of IT leaders do not trust AI.Incorporating transparency into audit trails ensures accountability and compliance with ISO/IEC 42001 auditing frameworks (ABBAS *et al*. 2024). The involvement of humans in the monitoring process reduces liability concerns, as is clear from the example of Air Canada's chatbot incident. There are independent review boards as well that help in improving accountability through recognition of ethical and operational risks. It is clear that organisations lacking these characteristics face several risks to their reputation and other areas.

Responsible AI Practices Across the Enterprise AI Lifecycle

Responsible AI techniques should be applied through the entire lifecycle of enterprise AI, including data gathering, model building, deployment, and monitoring. It is stressed in the literature that the process of data governance is a precondition that requires appropriate procedures to be followed regarding the quality, provenance, and fairness of data. The model development stage requires practices such as testing for bias, explainability techniques, and testing for adversarial robustness. The deployment stage requires practices such as human-in-the-loop monitoring and drift detection. Case examples include Microsoft, which adopted the Responsible AI standard, including enterprise lifecycle checkpoints such as fairness checks and transparency (Bontempelli *et al*. 2022). In another case, IBM adopted an AI Ethics Board, ensuring a review of the enterprise AI lifecycle before deployment. It will prevent discriminatory output from AI, regulatory violations and reputation risks.

AI Risk Categories and Mitigation Strategies in Enterprise Software

Enterprise AI systems' risk mitigation may be related to risks in such areas as bias, security vulnerabilities, explainability gaps, regulatory risks, and operational drift. Risks associated with biases can be mitigated by means of fairness audits and bias detection techniques, as it is seenin thee case of TutorGroup hiring discrimination. Security vulnerabilities of AI systems can be mitigated using adversarial testing and encryption techniques, as revealed in the results of the MIT CSAIL adversarial testing research. Risks associated with explainability gaps can be mitigated through the use of an interpretability framework since 79% of IT leaders do not trust AI system outputs without transparency, according to Gartner (Roberts *et al*. 2021). Regulatory risks should be mitigated by means of following tier requirements under the EU AI Act, while operational risks should be mitigated by means of retraining pipelines and systems monitoring, as it is suggested by Google AI drift detection research.

5. Proposed Integrated AI Governance Framework for Enterprise Software Systems

The development of a governance framework in enterprise AI will have to strike a balance between compliance, technical solutions and accountability aspects. Academics have suggested an integrated three-level framework with the inclusion of the compliance aspect with the help of regulations such as the EU AI Act, audibility using ISO/IEC 42001, and flexibility of risk management using NIST AI RMF (Ee *et al*. 2024). The incorporation of mechanisms such as the inclusion of tools for bias detection, explainability, audit trail and an independent oversight board will be required for the enterprise AI governance process. The discussion of case studies on Air Canada and IBM's lifecycle governance strategy highlights the importance of human intervention and the effectiveness of an integrated governance strategy, respectively.

Expected Organisational Outcomes of Responsible AI Governance

Organisations that embrace responsible AI governance frameworks derive organisational advantages that can be measured, including compliance, trust, and resilience. Research shows that firms using governance in their processes suffer less from sanctions and litigation. Gartner research reveals that firms embracing explainability practices have a 41% higher stakeholder trust score compared to those that do not use governance. Case studies of IBM and Microsoft reveal that responsible AI governance accelerates adoption due to less resistance and scepticism. Independent audit trail processes and oversight committees contribute to accountability, while bias detection systems facilitate diversity benefits. Adherence to regulatory requirements such as the EU AI Act and ISO/IEC 42001 boosts credibility in the market. Responsible governance also enables innovation by experimenting within proper governance.

6. Proposed Framework

The proposed framework integrates governance through regulations, governance through technology and organisation into one comprehensive AI governance framework for enterprises. The European Union AI Act will ensure that regulatory compliance is met through the use of risk classification, transparency,

documentation, and human interaction. ISO/IEC 42001 provides additional governance structures, auditability and accountability, while NIST AI RMF provides flexibility in risk identification, assessment, management, and monitoring (Aiyankovil *et al*. 2024). The enterprise governance boards and cross-functional committees provide the strategic governance and decision-making processes. All these governance frameworks cover all aspects of the AI process right from its inception, planning, data governance, development, deployment, monitoring, and maintenance.

7. Discussion

The findings reveal that the right governance of AI in enterprise software calls for a multidimensional approach that looks into factors like lifecycle management, risk management, regulatory compliance, and accountability, among other factors. As far as lifecycle management practices are concerned, there is a need to incorporate different mechanisms at various stages, including data collection and deployment processes (Pehlivan *et al*. 2024). The process bears a semblance to that which is demanded under the EU AI Act, which calls for human intervention and transparency in the case of high-risk AI applications. The risks that include biases, security and operational drift prove the need for an organised risk management process. The proposed integrated governance model consists of the integration of standards like ISO/IEC 42001 and NIST AI RMF as regards auditability and flexibility in risk management, respectively, and corporate governance frameworks like governance boards and cross-departmental committees. With this integration, companies will be able to avoid fragmented governance leading to the creation of shadow AI and risks related to non-compliance (Bogucka *et al*. 2024). The corporate implications of the proposed governance can be seen in increased compliance, trust of stakeholders, and reputation resilience, as evidenced by the statistic provided by Gartner, according to which there is a 41% increase in trust scores when explainability protocols are applied. The cases of IBM and Microsoft are clear evidence of the importance of embedded governance.

Limitaion

This study relied exclusively on secondary data sources, which limited the ability to capture real-time organisational practices and internal governance mechanisms. While industry reports and case studies provided validated evidence, the absence of primary data restricted deeper insights into enterprise-specific implementation challenges and contextual variations across sectors.

Table 1: *Comparative Landscape of Enterprise AI Governance Models*

Framework	Scope	Strengths	Limitations
EU AI Act	Regulatory law	Risk-tiered compliance, strong enforcement	High compliance costs
NIST AI RMF	Voluntary model	Flexible adoption, risk focus	Limited enforcement power
ISO/IEC 42001	International standard	Structured governance, auditability	Slow adoption globally
OECD AI Principles	Ethical guidelines	Global consensus, ethical focus	Lack of technical detail

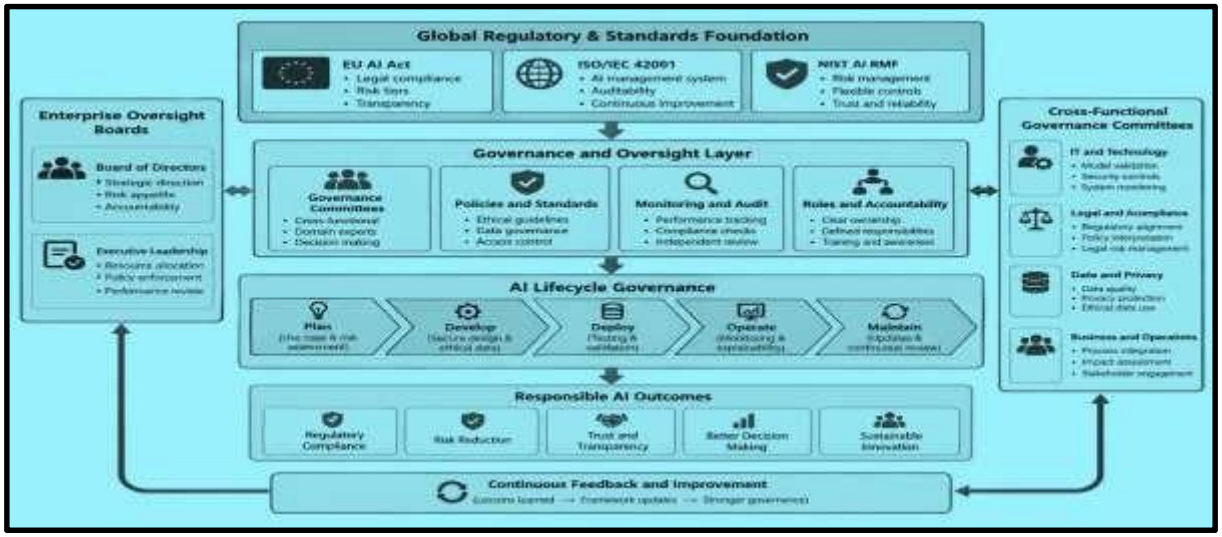


Figure 1: *Proposed Integrated Multi-Layered AI Governance Model*

Table 2: *Core Oversight Mechanisms for Responsible Enterprise AI*

Component	Purpose	Evidence
Bias detection	Prevent discriminatory outputs	iTutorGroup hiring case
Explainability	Build trust in AI decisions	Gartner survey showing 79% mistrust
Risk-tiered oversight	Align with regulatory obligations	EU AI Act compliance tiers
Transparent audit trails	Ensure accountability	ISO/IEC 42001 audit structures
Human oversight	Prevent liability risks	Air Canada chatbot dispute

8. Conclusions

The research shows that responsible governance in enterprise software systems is not only a necessity but also a strategy for sustainable innovation. As the research reveals, lifecycle management, risk classification, and an integrated framework are key elements in minimising bias, enhancing explainability, and attaining compliance. The provisions of the EU AI Act, ISO/IEC 42001, and NIST AI RMF combined make up the foundations of embedding responsibility and transparency in enterprise software systems. The cases of Air Canada and iTutorGroup demonstrate the outcomes of poor governance, while the organisational structures of IBM and Microsoft reveal the benefits of good governance. Thus, responsible AI governance produces real-world outcomes including increased stakeholder trust, reputational resilience, and regulatory exposure.

Author Statements:

- **Ethical approval:** The conducted research is not related to either human or animal use.
- **Conflict of interest:** The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper
- **Acknowledgement:** The authors declare that they have nobody or no-company to acknowledge.
- **Author contributions:** The authors declare that they have equal right on this paper.
- **Funding information:** The authors declare that there is no funding to be acknowledged.
- **Data availability statement:** The data that support the findings of this study are available on request from the corresponding author. The data are not publicly available due to privacy or ethical restrictions.
- **Use of AI Tools:** The author(s) declare that no generative AI or AI-assisted technologies were used in the writing process of this manuscript.

References

1. ABBAS, A. A. H. S. (2024). Ethical and Responsible Artificial Intelligence in High-Risk Industries: A Results-Oriented Governance and Assurance Framework. *International Journal For Multidisciplinary Research*. https://www.academia.edu/download/125647281/61913.pdf
2. AI, N. (2024). Artificial intelligence risk management framework: Generative artificial intelligence profile. *NIST Trustworthy and Responsible AI Gaithersburg, MD, USA*. https://pathologyinnovationcc.org/s/R8b_1722118549750.pdf
3. Aiyankovil, K. G., Lewis, D., & Hernandez, J. (2024, September). Mapping data governance requirements between the European Union's AI Act and ISO/IEC 5259: a semantic analysis. In *NeXt-generation Data Governance workshop 2024*. https://openreview.net/pdf?id=5ilvDyTkbg
4. Bogucka, E., Constantinides, M., Šćepanović, S., & Quercia, D. (2024, October). Co-designing an AI impact assessment report template with AI practitioners and AI compliance experts. In *Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society* (Vol. 7, No. 1, pp. 168-180). https://ojs.aaai.org/index.php/AIES/article/download/31627/33794
5. Bonney, K., Breaux, C., Buffington, C., Dinlersoz, E., Foster, L. S., Goldschlag, N., ... & Savage, K. (2024). *Tracking firm use of AI in real time: A snapshot from the Business Trends and Outlook Survey* (No. w32319). National Bureau of Economic Research. https://www.nber.org/system/files/working_papers/w32319/w32319.pdf
6. Bontempelli, A., Giunchiglia, F., Passerini, A., & Teso, S. (2022). Human-in-the-loop handling of knowledge drift: A. Bontempelli et al. *Data Mining and Knowledge Discovery*, *36*(5), 1865-1884. https://link.springer.com/content/pdf/10.1007/s10618-022-00845-0.pdf
7. Cotteleer, M. J., Goldenberg, S. S., Wing, I., Alliyu, O., Kania, S., Mujumdar, V., & Sniderman, B. (2021, November). Cybersecurity Requirements for AM Systems: New Enforcement in DoD Environments, and Resources for Implementation. In *Proceedings of the 2021 Workshop on Additive Manufacturing (3D Printing) Security* (pp. 49-60).

https://dl.acm.org/doi/pdf/10.1145/3462223.3485624

8. Ee, S., O'Brien, J., Williams, Z., El-Dakhakhni, A., Aird, M., & Lintz, A. (2024). Adapting cybersecurity frameworks to manage frontier AI risks: A defense-in-depth approach. *arXiv preprint arXiv:2408.07933*. https://arxiv.org/pdf/2408.07933
9. eeoc.gov, (2023). *iTutorGroup to Pay $365,000 to Settle EEOC Discriminatory Hiring Suit.* Retrieved from https://www.eeoc.gov/newsroom/itutorgroup-pay-365000-settle-eeoc-discriminatory-hiring-suit
10. Golpayegani, D., Pandit, H. J., & Lewis, D. (2022, December). Comparison and analysis of 3 key AI documents: EU's proposed AI Act, assessment list for trustworthy AI (ALTAI), and ISO/IEC 42001 AI management system. In *Irish Conference on Artificial Intelligence and Cognitive Science* (pp. 189-200). Cham: Springer Nature Switzerland. https://link.springer.com/content/pdf/10.1007/978-3-031-26438-2_15.pdf
11. Haefner, N., Parida, V., Gassmann, O., & Wincent, J. (2023). Implementing and scaling artificial intelligence: A review, framework, and research agenda. *Technological Forecasting and Social Change*, *197*, 122878. https://www.sciencedirect.com/science/article/pii/S0040162523005632
12. Kuo, C. L. (2022). Peer review for academic research. *Archives of Otorhinolaryngology-Head & Neck Surgery (AOHNS)*. https://scitemed.com/article/4093/scitemed-aohns-2022-00155
13. Laux, J., Wachter, S., & Mittelstadt, B. (2024). Trustworthy artificial intelligence and the European Union AI act: On the conflation of trustworthiness and acceptability of risk. *Regulation & Governance*, *18*(1), 3-32. https://onlinelibrary.wiley.com/doi/pdfdirect/10.1111/rego.12512
14. Pehlivan, C. N. (2024). Report: The EU artificial intelligence (AI) act: An introduction. *Global Privacy Law Review*, *5*(1). https://papers.ssrn.com/sol3/Delivery.cfm?abstractid=5368880
15. Roberts, A., Maennel, O., & Snetkov, N. (2021, September). Cybersecurity test range for autonomous vehicle shuttles. In *2021 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)* (pp. 239-248). IEEE. https://www.researchgate.net/profile/Nikita-Snetkov/publication/355766269_Cybersecurity_Test_Range_for_Autonomous_Vehicle_Shuttles/links/6239bb8ebc48180e3431ff30/Cybersecurity-Test-Range-for-Autonomous-Vehicle-Shuttles.pdf