World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(REVIEW ARTICLE)

Check for updates

Risk and compliance paper what role does Artificial Intelligence (AI) play in enhancing risk management practices in corporations?

Tina Akpevben Aror [1,*] and Munashe Naphtali Mupa [2]

[1] *St John's University New York.*
[2] *Hult International Business School.*

World Journal of Advanced Research and Reviews, 2025, 27(01), 1072-1080

Publication history: Received on 01 June 2025; revised on 08 July 2025; accepted on 10 July 2025

Article DOI: https://doi.org/10.30574/wjarr.2025.27.1.2607

Abstract

Artificial Intelligence (AI) is gradually transforming the corporate risk management and compliance landscape, as it allows making decisions in a more timely and correct way. This paper evaluates the new role being played by AI in promoting effective risk management and compliance processes in organizations through the manner in which the AI technologies with the ability to collect, analyze, process, and evaluate information, including machine learning, natural language processing, and predictive analytics, are being applied with the purpose of identifying, evaluating, and mitigating the various risks. Whether it is financial fraud detection, cybersecurity, operational interruptions, or compliance, the AI tools are increasing the speed of risk detection, increasing data analysis potential, and creating support for real-time monitoring and forecasting.

The paper examines how AI aids in automating repetitive risk management and compliance tasks, thus enabling risk managers to concentrate on the high-level monitoring. As well as listing the advantages, the processes and all those concerned with the adoption of AI in the sphere of risk management and compliance are also spoken about, with the discussion touching upon data quality, model transparency, and governance. The analysis indicates that when integrated in a proper manner, AI can enhance risk management and compliance of an organization and its resilience in a rapidly complicated and more uncertain business-based environment.

Keywords: Artificial Intelligence; Compliance; Corporations; Management; Risk

1. Introduction

Artificial Intelligence (AI) is the ability of machines, including computers, to think and learn unassisted like human beings. It can also be regarded as the simulation of human intelligence in machines, and this has turned out to be a significant discovery in technology. With the help of AI technologies, machines could handle big volumes of data, recognize the trends, and adjust to new information received, and thus will be able to perform the tasks that are similar to the human cognitive processes" (Stryker et al., 2024). Monreale, 2024: To get a better idea about the concept of AI, we should first examine the meaning of such words as "artificial" and "intelligence" separately. Artificial can be described as something done by the human hand as a nature replica. Intelligence speaks of mental activities, e.g., skills to learn, reason, know, understand, comprehend knowledge, and apply knowledge and experience to solve problems. Thus, the two terms combined result in the volume of Artificial Intelligence as the combination of methods, tools, and technologies that enable a machine to simulate human-like behaviors, imitating their cognitive processes to solve a certain task that is usually hard for a human being.

* Corresponding author: Tina Akpevben Aror

The University of Illinois Chicago (UIC) Online Masters in Engineering, 2025, subsequently breaks down AI into various domains of specialization, each specializing in a distinct aspect of mimicking human intelligence, and reads: Machine learning (ML) is one branch of AI that entails the development of algorithms that allow computers to learn and make decisions based on data without specific programming. Neural Networks and Deep Learning Inspired by the structure of the human brain, neural networks are networks made up of interconnected nodes (neurons) that process data. Deep learning Internships and placements with companies that specialize in deep learning, where computer vision is a way of training machines to read and analyze visual data of the world and see activities such as face recognition and object detection, and expert systems, which are AI programs that emulate the decision-making capabilities of a human expert, which are applied in areas such as medical diagnosis or financial forecasting.

Thomas Mike, 2025, in an article highlights the development trend of Artificial Intelligence (AI), and according to him, the development has witnessed impressive progress since its first appearance in the early 1950s, starting with mere game-playing systems to advanced, multidimensional systems that touch many facets of contemporary life. OpenAI releases Generative Pre-Trained Transformer 1 (GPT-1) in 2018 and seems to create a new era in AI. GPT-1 used 117 million parameters to produce human-like text given context, which demonstrated the possibilities of pre-trained transformers. It is on this base that OpenAI released GPT-4o in March 2025, a first-person multimodal model that can process and create pictures, sound, and text in real time. GPT-4o is an improved version of its predecessors in terms of writing, coding ability, and solutions to problems, demonstrating how fast AI abilities are advancing.

Risk management has been defined in so many ways, and in short, risk management is the identification and measurement of risks faced by an organization that are bound to lead to its fall and the process of controlling as well as alleviating those losses. Risk management is an important factor of any organization regardless of the industry it is based in, and it has become highly developed with the passage of time. AI is important in enabling organizations to discover datasets, spot trends in the datasets that may result in the discovery of the risks that may be present, and aid in making informed decisions to contain the identified risks.

In 2024, an estimation is that 78% of organizations have incorporated some level of Artificial Intelligence (AI) in their operation, meaning that a paradigm shift toward automation of business has been achieved. The usage of AI-based chatbots and computer assistants has allowed industries to automate simple interactions with customers and employees and save human resources to work on other activities that require higher levels of complexity. Moreover, because AI can handle and examine huge datasets, it can quickly produce usable insights that can be visualized in simple forms. This makes decision-making faster and allows business leaders to make sound decisions devoid of long manual data analysis. Implementation of AI technologies is rationalizing the business to simplify its operations, better treat the customer, and promote the fast strategic decision-making process in diverse companies (Thomas, 2025).

2. The Role of AI in Risk Management and Compliance

Artificial Intelligence (AI) could expand the effectiveness of the seven elements of an effective compliance program (structure and oversight, policies and procedures, risk assessment and due diligence, training and communication, monitoring and measurement, discipline and incentives, and reporting and investigation process) in a remarkable way when implemented as a risk management and compliance program. The ability of organizations to mitigate risks also becomes more effective when they integrate AI into their risk management procedures and compliance program, thereby facilitating regulatory compliance as well as contributing to the culture of constant enhancement.

AI-based tools will assist with drafting, updating, and monitoring compliance policies since they scrutinize big amounts of regulatory data to make sure it is coordinated with the applicable laws and standards. They also assist in making the wording of law simple and easy to interpret and hence assist the organizations in making understandable and comprehensive policies. AI can assist individuals in ensuring compliance with real-time reporting dashboards, which assist in monitoring compliance rates and areas of problems and providing recommendations on corrective measures to be taken. Compliance data can also be analyzed by machine learning models, and patterns that reveal insight can be given to the compliance committees during the major decision-making. Such systems are able to simulate real-life situations, and employees can train the responses to compliance and issues in a controlled setting.

Social anonymity and open communication are also hallmarks of AI chatbots, as people in compliance positions can use them to ask compliance-related questions anonymously. Such chatbots are able to give immediate replies, which can relieve the compliance teams and make sure that the information is given consistently. Surveillance and constant monitoring of transactions and operations can be done using AI systems, and this can assist in detecting anomalies that might point out there is some breach of compliance. Compliance with the automation of routine audits allows the AI to concentrate on more complicated challenges, hence better effectiveness and efficiency of the compliance in general. AI

can also be used to analyze the disciplinary actions to detect patterns and consistency of enforcing and implementing the standards of compliance. This discussion serves the purpose of streamlining rules of order and equality within the organization. AI can help in studying the root cause of compliance issues and provide recommendation steps to fix them when they are identified. It can also use predictive analytics to determine the possible risks of non-compliance in the future and use it to prevent them.

Compliance with regulations, especially when it comes to changing regulations, is one of the important factors any business should take as a key consideration. This is a serious burden that will be taken away by Artificial Intelligence (AI) automating the monitoring and reporting tasks. Utilization of AI systems in sifting through large volumes of regulatory materials within a short time helps them to detect new requirements or modifications that require alterations by a corporation so that they can be compliant. A subbranch of AI, machine learning (ML), is particularly good at pattern matching and identifying anomalies, which are important areas of compliance. It will be able to perform an analysis of past data to determine possible risks to regulatory compliance so that they can be dealt with in advance. New regulatory data can also be processed and used to train ML algorithms to make them better at identifying problems with compliance. With the help of AI and ML, incorporated in compliance structures, companies can not only optimize their compliance with existing regulations but also provide a proactive approach to swiftly adjusting to the modifications and maintaining the mandatory credibility of their operations in the long term" (Ladurantie 2024).

Real-time anomaly detection is one of the main characteristics of AI compliance monitoring tools. This ability is important in detecting the existence of lesser operating procedures that could have been an indication of a compliance breach. As long as AI systems keep a close monitor on transactions, communications, and other operational data, they should be capable of flagging activities that seem to be unusual or out of the predetermined standards within a short amount of time. Such proactive measures are useful not only in avoiding the breach of compliance but also in reducing the possible consequences of such a breach by speeding up the ability to respond to it. Application of future analytical and risk assessment tools within AI compliance frameworks enables organizations to predict future risks in order to prevent them. These tools review past and up-to-date data to determine trends and patterns that may happen, resulting in a lack of compliance. This way, the companies can be strategically prepared to counter them before they occur, as they are expected to analyze them. Predictive analytics implements a proactive strategy and turns compliance into a proactive strategy." (Certa, 2024)

Another major intervening problem in which AI is also involved is in document management and review. The AI-based tools would help to quickly analyze the contracts, policies, and other legal documents to detect the gaps, like the lack of the provision or the inapplicable language, which would simplify the process of reviewing the compliance and reduce the chance of human error. Also, AI technologies can track other activities of the employees, such as their communications, financial transactions, and other activities, to identify the compliance breaches. AI has the capacity to identify abnormalities or suspicious trends with speed because continuous monitoring of data is possible, and therefore the business can undertake immediate controlling actions. Using AI allows organizations to be aware of any changes in regulations as it monitors updates in the relevant sources and issues timely alerts and compliance suggestions so that businesses are updated as per the latest regulations and requirements (Pimentel 2024).

Collapse of the Enron A US corporation in the year 2001 is an essential benchmark of what happens when corporate negligence in compliance, regulatory gaps, and corporate illegitimate business practices have extreme repercussions. In the case of Enron, which involved the manipulation of the financial statement, exploitation of rules to make the company appear profitable at a given time, and deceiving investors, the fraud resulted in the collapse of the company. The factor of an efficient regulatory framework, good corporate governance structure, and transparency comes out in the problem of the Enron downfall. The negligence of the top management and the possibility to enable and inability to ensure that the auditing firm Arthur Andersen achieved independence of it's auditing also served to achieve success in the execution of the fraud. Other regulatory authorities outside, such as the SEC, did not even realize that fraud was going on until it was late, even after there were numerous red flags. It is believed that the WorldCom fraud, only a year after Enron in similar predicaments, gave rise very rapidly to the introduction of the Sarbanes-Oxley Act (SOX) in 2002, which brought about much-needed changes to the corporate governance and financial reporting" (Fitzpatrick, 2025). One of the ways that severe impacts might have been made to the detection and prevention of the fraudulent operations that resulted in the downfall of Enron and WorldCom was by integrating Artificial Intelligence (AI) into the risk management and compliance structures. It was an opportunity to integrate AI into every component of their risk management and compliance program to increase the capabilities to mitigate risks, observe regulatory requirements, and develop a charge of continuous process improvement. These would have furnished them with tools they needed to detect and prevent the fraud they were involved in, thus leading to their decline.

The current highly changing regulatory environment has changed the common duty of compliance into a strategic necessity. The ever-growing complexity of financial crimes calls for sophisticated tools to improve the identified risks, deplete fraud, and comply with regulations. The conventional approaches to compliance usually fail to be effective, which results in inefficiencies, high costs, and excessive rates of false positives. Artificial Intelligence (AI) is transforming compliance because it provides solutions that are highly accurate, process automations, identify real-time anomalies, and deliver compliance risks with high accuracy. Compliance tools enhance the ability of financial institutions and companies to work with large amounts of data fast, find patterns that signify its involvement in fraudulent operations, and make sure the company complies with complicated regulatory rules. By providing AI-based support to the compliance strategy, it will be possible to not only manage the related risks but also integrate efficiency in operations and ensure an effective defense against financial crimes. (Tookitaki, 2025)

AI has a significant contribution to the improved risk management process at a corporate level as it assists with enhanced risk detection, analysis, prediction, and alleviation capabilities. Artificial Intelligence is also completely transforming how companies handle risks because of its ability to improve predictions, automate tasks, and deliver insights in real time. Innovations in AI are having a critical role in the paradigm shift of risk management. Their capacity to derive knowledge out of the amount of data agents are currently confronted with is essential, and the capacity of machine learning to derive knowledge out of data will make it less time-consuming and more effortless compared to the traditional rule-based system, which involves continuous writing, tuning, and updating of the rules. These machine learning methods will improve the process in many ways, including finding long-term trends of risky customer transaction-based behavior and learning over the review's actions taken by risk managers to reduce the number of the hits that have to be reviewed manually (Becker 2025). The AI is reshaping risk management in businesses to include beneficial tools such as detecting, predicting, compliance, cybersecurity, and decision-making. With the further development of AI technologies, their involvement in the risk management strategies will be crucial to the organizations to help them navigate through the complex world of risk" (Dwillis and Dwillis 2024).

Risk management is becoming an important consideration for businesses, especially in highly regulated industries. According to the recent surveys, now specialists in corporate tax and legal departments in companies focus on risk identification and reduction priority. This focus is justified because the companies, which have to work within numerous regulatory frameworks and cover different areas operated by different jurisdictions and administration levels, have a problem maintaining compliance with the changing regulatory standards. Some of the consequences of non-compliance include a possible meltdown of reputation, a loss of customer confidence, and huge fines. In the past, companies have had to rely on specialized teams on compliance as a way of navigating their way through. Nevertheless, this practice is not so sustainable, as it is limited by resources and pressure to reduce expenses. In addition, the categories of external threats, like data exposure, cybersecurity threats, risks connected with the field of AI, and geopolitical risks, require significant resources and attention to guarantee organizational resilience. In order to deal with these challenges, more and more organizations are making use of Artificial Intelligence (AI) when it comes to risk management.

3. Artificial Intelligence Integration in Other Sectors

Artificial Intelligence (AI) also transforms the safety management of high-risk sectors such as construction due to the tendency to focus not on the reactive response to risks but on their proactive mitigation. Examples of such shifts can be found in platforms like FYLD, which uses AI to examine historical safety information and combine that information with live data in order to draw patterns that may be predictive of risks. As an example, when the data shows that some tasks or conditions, such as specific weather conditions, the use of a certain type of tool, or high-traffic areas, increase the occurrence of injury, FYLD can send a timely message, and real-time alerts can be provided to field managers, and they can be able to provide preventive measures" (Barron-Smith 2025).

This predictive ability plays a key role in the development of an anticipatory safety culture beyond compliance into an active prevention of incidents prior to their occurrence. This is because in industries that perform the same task over and over, where complacency may mean death or serious injury, AI-guided systems such as FYLD offer workers real-time recommendations they can act on, with the best interest of keeping them focused and engaged with staying safe. These kinds of instant feedback devices work to prevent the risks of complacency in safety approaches, which may follow after sustained repetition of task-related activity in highly hazardous situations. The implementation of AI into the safety processes enables organizations to develop a culture of never-ending consciousness that helps make safety maintenance an integrated process, even at the times when regular operations are carried out. The usage of FYLD has proved to carry physical improvements and have a significant decrease in the occurrence of accidents and the number of injuries, more than 20%. This is a central testimony to the power of AI in the field of workplace safety. The full potential of AI in safety management boils down to the fact that it enables organizations to shift from a reactive to a

proactive safety approach by predicting and preventing risk based on past and current data analysis" (Barron-Smith 2025).

The financial services industry is also experiencing a revolution with the help of Artificial Intelligence (AI) and machine learning (ML). Through the use of these technologies, financial institutions are able to make better decisions and to be more efficient and less costly. The AI and ML algorithms have the potential of analyzing large volumes of both structured and unstructured data to determine patterns and deviations, thereby making risk assessment more precise. This permits a proactive risk mitigation approach through informed decision-making. Banks and other financial organizations use AI to identify fraud by tracking the activity in transactions and noticing abnormal patterns. The ML models have the possibility to counter the urgently emerging fraud schemes, guaranteeing high security of financial crimes. Compliance could be automated with the help of AI systems, as it involves constantly checking the changes in regulation and lack of compliance of internal policies with the new laws. Such automation minimizes the chances of not adhering and the penalty that comes with it. AI will facilitate real-time surveillance of financial activities, which will help institutions to manage new risks. Also, strategic insights contribute to proper decision-making with the help of AI-driven insights that allow for precise predictions and trend analysis. The AI models are less biased and make creditworthiness decisions more accurate by using many aspects of varied data. The use of AI tools to detect suspicious activities with the help of transaction data and analyze information increases the efficiency of the AML programs (Artificial Intelligence in Risk Management, 2021).

4. Challenges of Artificial Intelligence in Risk Management and Compliance

The adoption of Artificial Intelligence (AI) into compliance systems entails not only notable benefits but also a number of issues that would have to be overcome by organizations in order to implement them successfully and ethically. Big data usually has a lot of data required in the application of AI systems and hence poses a serious issue concerning data privacy and security. Organizations should make certain that AI applications can be used according to data protection laws and restrictions, including the General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA), and that is not an easy task at all. Organizations will need to consider putting in place solid data governance policies that will allow them to govern their data in a responsible manner and will minimize threats related to uncontrolled data leakage or misuse. The integration of AI in compliance can be the crucial section and might require significant resources. It requires substantial once-offs, specialized technical expertise and a lot of knowledge on how to best apply AI on specific compliance cases.

The efficiency of AI can be optimized in the field of compliance, whereas it has a danger of giving too much power to automated systems that can produce decisions on the behalf of an organization. Some overdependency can lead to annihilation of human reason and supervision and can even lead to lack of details or morality. It is essential to find a balance between the observations made by AI and the human knowledge that should be done in such a way that context-related changes can be accounted by the decisions made regarding compliance. The international regulation of AI is yet to be developed, and some standards and principles may be found in various jurisdictions. This makes it a challenge for an organization that tries to remain in compliance because they have to trudge through a multifold and dynamic set of regulations. It is also essential to remain up to date and flexible to be able to react adequately to new regulatory changes and have continuous compliance with them. When introducing AI in compliance tasks, one should pay significant attention to ethical principles. The AI systems should be created and installed to promote justice, clarity, and accountability, eliminating prejudices and discharging unfair results. It is crucial to create ethical standards and governance processes that would make AI applications reflect organizational principles and social norms. (Ladurantie, 2024)

AI systems need the accuracy, completeness, and quality of the data to perform adequately. Data quality might be so bad that it can cause unreliable results, an issue that will jeopardize the effectiveness of compliance. Most organizations use legacy systems, which cannot support the modern AI systems. Such incompatibility makes integration difficult, and it may slow the processing of real-time data that is required in monitoring compliance. AI models can act as black boxes so that stakeholders have no clue as to how decisions are made. This is the main source of this lack of transparency, which can trigger trust concerns and difficulties when it comes to fulfilling regulatory requirements that require explainability. Regulatory frameworks keep on changing. The AI compliance systems should be dynamic and adjustable to adapt to the changes without making significant overhauls (Certa, 2024). The solution to these difficulties is active and informed problem solving, which involves technological advancement, strategic thinking, and ethical awareness. Through this, the organizations will be able to embrace the power of AI in terms of compliance without much risk.

The problem is that in the modern state of the hurry, AI promotes the potential issues with the tendency to realize first the innovation without sufficient investment in the organizational culture and risk management infrastructure inside

the different organizations. The ensuing imbalance may cause much business and social damage. Data breaches or the misuse of an AI system may lead to a backlash by citizens, regulatory punishment, and the loss of the trust of stakeholders. The AI companies need to adopt good measures to prevent such events to curb those risks. Such frameworks as the National Institute of Standards and Technology (NIST) AI Risk Management Framework (AI RMF) have been created in order to understand and mitigate the risk of AI. Nonetheless, organizations are allowed to restructure these frameworks according to their requirements. As an example, the dangers of AI in healthcare are different compared to those of construction. Thus, companies should implement the most appropriate risk management practices that can effectively facilitate the AI applications challenges. The risk management system should be implemented systematically, and this proves to be very difficult in cases where organizations are unfamiliar with minding AI.

Implementing maturity models can help in this effort by mapping out a structured process: this will involve ethical awareness and the creation of guidelines (policies and procedures that reflect their commitment to ethics), incorporating the instructions into daily work, and establishing an ethical culture within the organization. Unless they have clear milestones and continually review the progress, companies are in danger of slipping into the trap of doing little more to appear ethical other than making statements that do not become reality. This disconnect may turn out to have outcomes to such an extent as is the case with Enron, in which failure to practice ethics with core commitment endowed the company with failure. When pursuing responsible AI governance, businesses can avoid the pitfalls of AI with all the complexity of innovation that a responsible AI can bring to the fore (Winecoff, 2024).

5. Artificial Intelligence risk management framework

According to the National Institute of Standards and Technologies (NIST, 2023), the potential of Artificial Intelligence (AI) technologies is immense in transforming society and enhancing the lives of people in various sectors, including commerce, healthcare, transportation, cybersecurity, and environmental stewardship. They will be able to support economic growth and scientific innovations to achieve better wellness in the world. Nevertheless, along with these benefits, AI creates a set of risks that may significantly impact people, institutions, groups, society, and the earth. Such risks are quite opposed to risks involved in traditional technology. The NIST states that the risks of AI are unique, as such systems can evolve in unexpected ways as the data they learn is altered, thereby undermining their operation and reliability. AI systems are socio-technically complicated to detect failures because of the high levels of complexity and the fact that they are fashioned by human patterns in part and societal phenomena and the context in which they are deployed. The main issue is to manage the risk, which can be done through efficient AI risk management that is vital to creating the responsible development and use of AI systems that involve decisions made in the AI life cycle adhering to human values, social responsibility, and sustainability objectives.

The deliberate management of the AI risks enhances the trustworthiness of the AI systems and drives the population to be confident; therefore, the development of several structures by the NIST assists all kinds of organizations to achieve their objectives regarding cybersecurity and other related problems, as it gives insight into activities and results. The AI Risk Management Framework (hereinafter referred to as the AI RMF), as described in the National Artificial Intelligence Initiative Act of 2020, is a voluntary, scalable framework to assist businesses in all types of industries to design, develop, implement, and utilize Artificial Intelligence irresponsibly. It equips AI actors, organizations, and individuals engaged at some point in the AI system lifecycle to engage in practices that wring maximum benefits out of AI coupled with the minimum amount of harm possible.

The AI RMF is flexible and practical, and instead of striving to meet all the aspects of the document, it is intended to adjust itself to changes in technology so that AI technologies become beneficial to society and guard against adverse effects. NIST AI RMF was developed as a reflection of inputs by the private and the governmental sectors to manage risks to individuals, an organization, andsociety being manifested by the use of Artificial Intelligence. It is voluntary and aimed at enhancing the capacity to fold in a trustworthiness aspect into the design, development, application, and assessment of AI products, services, and systems. The Frames was identified through a consensus-based, open, transparent, and collaborative process that held a request for information, several draft versions subject to public comment, numerous workshops, and other solicitations of input. It is created to supplement, match, and reinforce the work of other AI risk management initiatives.

Machine learning (ML) models are becoming a more common component in Artificial Intelligence (AI) solutions in diverse fields, in particular because they have significantly better predictive performance than conventional statistical techniques (Giudici et al., 2023). The issue is, however, that these models can also be viewed as black boxes, and in order to figure out what decision process occurs, it is difficult to comprehend. There is a lot of concern on this lack of transparency in regulated where transparency and accountability would be useful to its compliance. These challenges

are forcing the regulatory standards to adapt to them not only to respond to concerns about guaranteeing accuracy and explainability, but also to the robustness of the standards, their cybersecurity, their fairness, their sustainability. To deal with all these complicated requirements, companies are incorporating end-to-end AI risk management frameworks. This kind of frameworks applies concepts of explainable AI (XAI), such that a decision made by an AI system can be described transparently and simply understood by affected populations. XAI is an essential part of building the trust, adherence to compliance, and proactive auditing and monitoring of AI systems. Development and implementation of AI incorporate such aspects into the process thus guiding organizations to traverse the grey world of regulating AI. Concentrating on the principles of transparency, resilience, and ethics, corporations may take the opportunities provided by AI and mitigate risks connected with this technology and the control over the emergence of new standards.

6. NIST privacy framework

The NIST Privacy Framework is a flexible, voluntary framework that is intended to help organizations of all scopes to manage the risks around privacy in a holistic manner. It is technologically neutral and can fit many sectors, laws, and jurisdictions and is therefore a resource that can be used in a variety of organizational situations. Its power principles are as follows: Privacy integration, whereby the framework encourages organizations to consider privacy in designing and implementing systems, products, and services that affect individuals. Transparent communication, where it promotes clear communication about the privacy practices within and between organizations, resulting in increased trust among them and Cross-organizational collaboration, its framework, facilitates executive collaboration, legal teams, and IT professionals through the development of profiles, the selection of tiers, and the attainment of specified objectives. The framework is advantageous because it helps to gain trust by providing ethical decision-making opportunities in the development of products and services, utilizing data in an optimal fashion with minimal negative impact effects on individuals and society, supporting the needs to achieve current compliance requirements and anticipate future changes in a changing technological environment, and facilitating including conversations with individuals, business partners, assessors, and regulators with respect to privacy practices.

The framework acknowledges that AI systems may also pose serious privacy risks, including but not limited to the following: the model is trained on data that was obtained without consent with limited privacy precautions, inferred or disclosed personal data, attacked personal data such as data inference or via data reconstruction, prompts injection, and membership inference. By integrating the privacy factors in the creation and implementation of AI systems, an organization can lessen these risks and safeguard the privacy of individuals.

7. Conclusion

Artificial Intelligence (AI) is an area that becomes more and more in the spotlight of regulators and industry leaders, with an emphasis on practical implementations and risks. AI can also reshape almost every aspect of corporate business services (Crimes and LLP, 2025) and bring about a positive change, as long as it is implemented wisely and with a strong regulatory structure in place, yet it can be extremely dangerous in the absence of effective governance. Although lots of AI companies publicly profess their recital on ethical principles and goal to society, historical experience has demonstrated that such proclamations and specifications are not adequate without any action. The Enron demise proves to be a good lesson. Regardless of the values it claimed to enhance, the company had managed to create a spirit of valuing things more than values; this has contributed to what can be described as the largest corporate scandal in modern history. To avoid reoccurrence of such failures, AI organizations need to have elaborate risk management strategies and practices at the organizational and technical levels. This involves putting proper governance mechanisms in place, disclosure of decision-making processes, ensuring that there is an atmosphere of organizational culture that encourages ethical practices, and lastly, clear accountability to every entity. All these will help ensure that the AI companies will not put themselves in the danger of being like such companies as Enron that, despite their innovations, are only remembered through their ethical failures.

To address these complexities, risk management and compliance leaders are advised not to only pay attention to the technological side of AI but also consider investing in the establishment of the organizational culture that will emphasize the aspect of ethical considerations and constant learning. By doing so, they will be able to make sure that AI becomes an aide in human judgment (another crucial element in risk management and compliance) and not its substitute, thus making them accountable and enhancing trust among stakeholders. Innovations AI organizations of the modern corporate world are currently operating at the forefront levels and should simultaneously invest more in the creation of the organizational culture and infrastructure to ensure they overcome the potential hazards of using AI. Risk mismanagement and unhealthy organizational culture would place AI organizations on the track that could be

disastrous to both companies and society. Achieving data privacy and security breaches are some of the threats that may lead to increased scrutiny by policymakers, user adoption, and outside investment.

To circumnavigate this, AI firms should not undertake risky actions such as the ones that were not seen by Enron. In particular, they should take actions that encourage trust, transparency, and accountability, protect the internal critics, and ensure that unethical cultures do not entrench. The National Institute of Standards and Technology (NIST) offers a top-level framework on the ways organizations can initiate the process of recognizing and reducing the AI risks. Nonetheless, organizations have primary roles to perform by converting the NIST framework in their individual businesses and practices. The risks in the banking industry and AI are vastly different as compared to the risks that are represented by AI in building. Accordingly, the organizational practices based on their principles of AI should be adapted to the peculiarities of the risk in an industry and business. AI promises extraordinary changes in the ways corporate services are delivered, but successful adaptation to the latter necessitates an even-handed assessment of innovation versus possible risks. The compliance professionals lie at the center of such a process and help their organizations to realize the advantages of AI in a responsible and sustainable way.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict-of-interest to be disclosed.

References

[1] "Artificial Intelligence in Risk Management." 2021. KPMG. September 23, 2021. https://kpmg.com/ae/en/home/insights/2021/09/artificial-intelligence-in-risk-management.html.

[2] "The Future of AI: How AI Is Changing the World | Built In." 2022. Built In. 2022. https://builtin.com/artificial-intelligence/artificial-intelligence-future.

[3] Barron-Smith, Daniel. 2025. "From Reactive to Proactive: AI for Risk Mitigation and Safety." Fyld.ai. FYLD Limited. February 7, 2025. https://resources.fyld.ai/resources/from-reactive-to-proactive-ai-for-risk-mitigation-and-safety#:~:text=Predictive%20analytics%20uses%20historical%20safety,arise%20and%20recommend%20proactive%20measures.

[4] Becker, Helmut. 2025. "Using Artificial Intelligence (AI) to Minimize Errors in Business Enterprise Management." SpringerLink. https://doi.org/10.1007-978-3-658-47243-6.

[5] Boillet, Jeanne. 2018. "Why AI Is Both a Risk and a Way to Manage Risk." Ey.com. April 1, 2018. https://www.ey.com/en_gl/insights/assurance/why-ai-is-both-a-risk-and-a-way-to-manage-risk.

[6] Certa. 2024. "Challenges and Solutions in AI-Driven Compliance." Certa. June 11, 2024. https://www.certa.ai/blogs/challenges-and-solutions-in-ai-driven-compliance.

[7] Chicago, University of Illinois. 2025. "Online Master of Engineering." Uic.edu. March 21, 2025. https://meng.uic.edu/news-stories/ai-artificial-intelligence-what-is-the-definition-of-ai-and-how-does-ai-work/?utm_source=chatgpt.com.

[8] Crimes, Financial, and Young LLP|authorurl:https://www.ey.com/en_us/people/alex-treuber. 2025. "How AI Will Affect Compliance Organizations." Ey.com. 2025. https://www.ey.com/en_us/insights/financial-services/how-ai-will-affect-compliance-organizations.

[9] Dwillis, and Dwillis. 2024. "How Is AI Transforming Risk Management?" FinTech Global. August 6, 2024. https://fintech.global/2024/08/06/how-is-ai-transforming-risk-management/?utm_source=chatgpt.com.

[10] Fitzpatrick, Catherine Darling. 2025. "The Enron Collapse: Compliance Failures and Lessons." Planet Compliance. March 4, 2025. https://www.planetcompliance.com/regulatory-compliance/enron-compliance-failures/.

[11] Giudici, Paolo, Mattia Centurelli, and Stefano Turchetta. 2023. "Artificial Intelligence Risk Measurement." Expert Systems with Applications 235 (August): 121220–20. https://doi.org/10.1016/j.eswa.2023.121220.

[12] Ladurantie, Cyril Amblard. 2024. "How Artificial Intelligence Can Be Used in Compliance." MEGA. February 2, 2024. https://www.mega.com/blog/how-artificial-intelligence-can-be-used-compliance.

[13] Monreale, Anna. 2024. "An Introduction to Artificial Intelligence." Artificial Intelligence in Accounting and Auditing, 63–89. https://doi.org/10.1007/978-3-031-71371-2_3.

[14] National Institute of Standards and Technology. 2018. "Risk Management Framework for Information Systems and Organizations." Risk Management Framework for Information Systems and Organizations 2 (Revision 2). https://doi.org/10.6028/nist.sp.800-37r2.

[15] NIST, Gaithersburg MD. 2025. "NIST Privacy Framework 1.1." https://doi.org/10.6028/nist.cswp.40.ipd.

[16] NIST. 2023. "AI Risk Management Framework." Artificial Intelligence Risk Management Framework (AI RMF 1.0), January. https://doi.org/10.6028/nist.AI.100-1.

[17] Pimentel, Brandon. 2024. "How AI Can Help You Manage Risks." Thomson Reuters Law Blog. May 10, 2024. https://legal.thomsonreuters.com/blog/how-AI-can-help-you-manage-risks/.

[18] Stryker, Cole, and Eda Kavlakoglu. 2024. "What Is Artificial Intelligence (AI)?" IBM. August 9, 2024. https://www.ibm.com/think/topics/artificial-intelligence.

[19] Thomas, Mike . 2025. "The Future of AI: How AI Is Changing the World | Built In." Built In. January 28, 2025. https://builtin.com/artificial-intelligence/artificial-intelligence-future.

[20] Tookitaki. 2025. "AI in Compliance: How Artificial Intelligence Is Transforming Regulatory Adherence." Tookitaki.com. March 19, 2025. https://www.tookitaki.com/compliance-hub/AI-in-compliance-how-artificial-intelligence-is-transforming-regulatory-adherence.

[21] Winecoff, Amy. 2024. "What Today's AI Companies Can Learn from the Fall of Enron." Tech Policy Press. March 29, 2024. https://www.techpolicy.press/what-todays-AI-companies-can-learn-from-the-fall-of-enron/