MILLIMAN WHITE PAPER

Introduction to artificial intelligence

What are the key risks for insurers to consider over the short to medium term?

Joseph Sloan, FSAI
Nia Powis, AIA, CERA
Joanne Tan, FIA, CERA

Milliman

Introduction

Artificial intelligence (AI) has emerged as a transformative technology, reshaping the way we live, work, and interact. As defined by the European Union's AI Act, AI is a "*machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments."* In simple terms, it refers to the simulation of human intelligence processes by machines, particularly computer systems. These processes include learning, reasoning, problem solving, perception, and language understanding.

AI has a wide range of applications that span across a variety of industries. In healthcare, AI can be used for early disease detection, drug discovery, and personalized medicine. In the finance and insurance industries, it can help with fraud detection, risk assessment, and algorithmic trading. Despite the fact that AI has the potential to transform the insurance industry and has numerous benefits, the use of AI comes with potential risks and challenges, including ethical dilemmas, privacy concerns, and security threats.

Understanding these risks is crucial to harnessing the power of AI responsibly and effectively. In this briefing note, we will first explore the potential uses of AI in the insurance industry. We will then delve into the EU AI Act, its scope, and its implications for AI development and deployment. Finally, we will explore the various risks associated with AI, discuss their implications, and outline some strategies to effectively manage these risks. It is important to acknowledge that the capability and potential of AI models is developing very quickly—this note captures the risks associated with the use of advanced AI tools that exist today, such as machine learning techniques, large language models and generative AI (GenAI) tools such as ChatGPT, rather than the potential risks associated with artificial general intelligence (AGI) or further developments in GenAI.

Applications of AI in insurance

AI systems have the potential to reshape the insurance industry through optimising efficiency and decision making across the entire insurance value chain.

AI systems can enhance customer experience by streamlining processes and personalising interactions. AI's ability to analyse vast amounts of data has the potential to enhance the accuracy of risk ratings and accelerate underwriting processes. AI-powered chatbots and virtual assistants can provide immediate assistance, answering customer queries and guiding them through complex policies. In claims management, AI is being deployed to automate document processing and detect fraudulent claims promptly using machine learning algorithms, significantly expediting the process for the customer.

In addition to the applications above, AI is increasingly used in back-office functions such as finance, risk, and actuarial. AI-driven automation has the capacity to streamline back-office operations, reducing manual effort and improving efficiency. By automating routine tasks, (re)insurers may be able to reallocate resources to higher-value activities, ultimately reducing costs and boosting productivity. AI systems are a powerful tool for processing and analysing large volumes of data, leading to improved accuracy and efficiency in risk assessment and risk management. With appropriate use, AI also has the potential to empower management to make informed strategic decisions more effectively and efficiently.

The EU AI Act

The EU's Artificial Intelligence Act (AI Act or the Act hereafter) has significant implications for insurers using AI. In May 2024, the Act was formally adopted by the European Parliament and Council. The Act was published in the EU Official Journal on 12 July 2024 and the new law comes into force on 1 August 2024. However, most of the provisions will not take effect for a further two years after that date, giving insurers time to comply with the new regulations.

OBJECTIVES

The AI Act emphasises the ethical use of AI. AI should be used in a trustworthy and transparent way. The core objectives of the proposal include:

- Protecting the health, safety and fundamental rights of people
- Harmonisation of the regulations around AI usage across the EU
- To support innovation within the EU
- To ensure that AI uses data in a way that respects EU data protection rules
- Protect the fundamental rights of consumers

CLASSIFICATION

Under the AI Act, AI systems are classified according to their risk.

1. **Unacceptable risk:** These systems are prohibited—for example, social scoring and AI that manipulates human behavior or exploits people's vulnerabilities will also be forbidden.
2. **High risk:** These systems are regulated. They pose significant risks to health, safety, or fundamental rights and freedoms.
3. **Limited risk:** These systems are subject to lighter transparency requirements. Users should be aware that they are interacting with AI.
4. **Minimal risk:** AI systems not failing into the three categories above fall into the lowest level of risk described as minimal risk. These systems have minimal regulation. It is suggested to follow general principles such as ensuring that natural persons are informed that they are interacting with an AI system.

Insurance and financial services are specifically flagged in the AI Act as areas of concern for high-risk AI systems. The Act explicitly identifies AI systems used in health and life insurance for risk assessment and pricing as high risk, due to their potential significant impact on individuals' livelihoods. Poorly designed, developed, or utilized AI systems can violate fundamental rights and lead to serious consequences such as financial exclusion and discrimination, impacting people's lives and health. The Act distinguishes AI used for fraud detection and for the prudential purposes to calculate credit institutions' and (re)insurances undertakings' capital requirements—these are not considered as high risk under the regulation.

It will be important to ensure that the use of AI within a (re)insurance context does not inadvertently result in breaching the prohibitions set out in the Act, particularly where AI is used in an underwriting or pricing capacity for life and health insurance, but also for personal lines of non-life insurance.

The Act primarily imposes obligations on high-risk AI systems. Consequently, companies employing such systems will need to:

- Establish a risk management policy
- Conduct data governance
- Ensure sufficient technical documentation to demonstrate compliance
- Include functionality for record-keeping when designing high-risk AI systems
- Document instructions for downstream users
- Design systems to enable users to implement human oversight
- Ensure appropriate levels of accuracy, robustness, and cybersecurity when designing systems
- Establish a quality management system to ensure compliance
- Be listed with the authorities

TIMELINE

The timeline of adaptation is as follows:

- On 21 May 2024, the Act was formally adopted by the European Parliament and Council.
- On 12 July 2024, the Act was published in the EU Official Journal and comes into force 20 days later on 1 August 2024.
- Companies will have two years to comply—the AI Act is fully enforceable by August 2026 (noting that some provisions will apply sooner, e.g., bans on prohibited AI systems will apply six months after the Act enters into force, while requirements for General Purpose AI (GPAI) systems and models will apply 12 months after).

It is also worth noting that some countries have taken steps toward self-regulation of AI. For instance, in the Netherlands, an ethical framework for the application of AI in the insurance sector was introduced by the Dutch Association of Insurers. The framework is binding for all members of the association and is a requirement within the association's self-regulation. However, this paper does not delve into the details of similar ethical guidelines and codes of conduct within the EU.

WHAT DOES THIS MEAN FOR INSURERS?

The AI Act sets out a framework for the acceptable use of AI which will impact insurers using AI technology. The Act aims to ensure ethical and safe AI use and presents both challenges and opportunities for companies.

Insurers will need to ensure that their AI applications comply with these regulations, particularly for systems that meet the definition of high risk under the AI Act. Time and resources will be needed to develop a suitable risk management framework to support the use of high-risk AI in an insurance setting. It may become common practice to develop a risk management framework for the use of AI more generally, not just for high-risk systems. Some of these requirements under the AI Act are aligned to the normal risk management requirements under Solvency II, such as establishing a risk management policy, data governance, technical documentation, etc., and therefore actuarial and risk functions should be well positioned to help (re)insurers start to address some of the obligations under the Act.

The AI Act significantly impacts data protection. Insurers will need to ensure that their AI systems comply with data privacy regulations, increasing the complexity of data management and cyber risk exposure. European insurers are likely to be well versed in data protection requirements; however, they will need to ensure that AI systems comply with these requirements. There may also be consent issues to overcome.

The AI Act mandates increased transparency in AI systems, and insurers may need to rely on actuarial and risk management expertise to explain AI model outputs and decisions to stakeholders. This task can be challenging, especially for complex AI models that may operate as "black boxes," thereby introducing significant model risk. Actuaries may be uniquely positioned to ensure compliance in these areas, particularly given their knowledge of statistics and coding. Furthermore, actuaries are proficient at explaining model judgements and assumptions to boards and other stakeholders, and ensuring that proper governance is applied for key judgements. Robust model governance is a cornerstone of the actuarial profession, and therefore insurers should be able to utilise actuarial expertise to validate and explain AI models.

Stakeholders and customers will expect responsible use of AI, and any non-compliance could expose insurers to reputational risk. Moreover, failure to adhere to the regulations could incur severe penalties, potentially reaching €35 million or 7% of the global annual revenue, whichever amount is greater.

In the next section, we discuss the potential AI risks for insurers and explore approaches to mitigate them.

AI risk exposures and mitigations

In an insurance context, AI risk refers to the potential dangers and negative consequences associated with the development and deployment of AI systems within a (re)insurance company. These risks span the entire insurance value chain, from customer-facing business units such as sales, underwriting and claims, to back-office operations including finance, actuarial, risk management and IT. We have identified some key risks as:

- Model risk
- Data risk
- Data privacy and cyber security risks
- Ethical risk
- Regulatory risk
- Legal risk

However, this is not an exhaustive list and the actual risk exposure will depend on how specific (re)insurance companies employ AI throughout their own value chains.

MODEL RISK

Model risk in insurance refers to the potential financial loss or adverse impact that can arise from errors or inaccuracies in the models and methodologies used by insurers.

AI models, in particular, can be highly complex and difficult to interpret. Often operating as "black boxes," they can introduce significant model risk. The lack of interpretability can make it challenging for (re)insurers to understand how AI-driven decisions are made and to identify potential sources of error or bias. Ongoing research into post hoc explainability methods, such as SHAP (Shapley Additive Explanations), seeks to address these challenges and enhance transparency in such models.

These models rely heavily on data, and the quality and representativeness of this data can significantly impact model performance. Insufficient or biased data can lead to AI models making inaccurate predictions or decisions, which may result in financial losses or unfair treatment of policyholders.

Furthermore, excessive reliance on AI systems for decision making, coupled with difficulties in understanding and effectively communicating results to stakeholders, may lead to incorrect decision making. For instance, a policyholder could be unfairly denied cover or quoted an excessively high premium, or an AI model may make flawed trading decisions due to model inaccuracies, resulting in financial loss.

To mitigate these risks, establishing a strong model governance framework is essential. The introduction of the AI Act provides a structured approach for companies to follow. For instance, the AI Act requires a risk management policy to be in place for high-risk AI systems. This policy involves a continuous, iterative process that spans the entire lifecycle of such systems, requiring regular systematic review and updating. Companies can tailor and enhance existing model risk management policies and frameworks for AI systems, ensuring that they align with and comply with the AI Act regulations.

Rigorous testing and validation of AI models are integral to mitigating model risk. The Solvency II internal model framework (e.g., statistical quality test, use test, validation test, and documentation test) provides a good starting point for an AI model validation framework, as it aims to ensure that the model remains reliable, robust, and appropriate for the use within the company. This process also allows for the implementation of controls in the early stages of model development. Continuous monitoring is also essential to detect data drift, which can impact model performance and accuracy. Data drift occurs when the statistical properties of the input data that a model receives change over time.

Transparency is key in reducing model risk and fostering trust among stakeholders. Clear documentation of the data, assumptions, methodologies, and judgements used in AI models enhances understanding. It will be important to justify decisions with regard to the choice of modelling approaches in the underlying algorithms. Equally important is the ongoing training and education of staff involved in AI model development, validation, and deployment. Providing comprehensive training ensures that personnel possess the necessary skills to effectively manage and mitigate model risks.

DATA PRIVACY AND CYBER SECURITY RISKS

Data privacy and cyber security issues are always a key area of concern when it comes to new technologies.

AI systems, which rely on large datasets to generate outcomes and derive conclusions, will often involve handling personal data in an insurance context. Where models are trained using personal data, it will be important to ensure that the models are sufficiently locked down to mitigate the risk of unauthorised access and/or potential data breaches. Furthermore, improper use of AI, coupled with inadequate staff training on AI-related security risks, poses a significant risk. Employees might be unaware of the security vulnerabilities associated with GenAI platforms like ChatGPT and could inadvertently expose sensitive company and policyholder information by uploading it to these platforms.

To manage this, companies should consider ways to establish boundaries and restrictions for the use of AI systems, e.g., ensuring that the AI systems comply with the EU General Data Protection Regulation (GDPR), consumer protection codes, and sector-specific rules and regulations. Additionally, companies must align AI practices with their internal process and policies. For consumer-facing AI systems like chatbots, companies should further ensure that the information provided by the AI systems is compliant and consistent with the existing policies, processes, and models within the company. Controls need to be embedded into the process where AI systems are used, whether directly within the AI system or when using the results of AI models.

Regular security audits and penetration tests are crucial for identifying vulnerabilities within AI systems and strengthening their defences against potential cyber threats. Using AI-specific security tools, such as threat detection systems, can provide real-time monitoring and response to suspicious activities, thereby enhancing the overall security posture.

ETHICAL RISK

AI models used for underwriting or claims processing may reflect biases which may lead to discriminatory outcomes. Biased AI systems used to determine an individual's eligibility for an insurance policy could potentially result in an unfair and discriminatory outcome for the policyholder, leading to unjust pricing or claim decisions.

As a simple example, AI pricing models might not initially recognise regulations such as the EU Gender Directive (unless they are trained to do so) and therefore may inadvertently price policies differently for males and females based on the input data. This potential for bias not only leads to ethical concerns but also exposes insurers to significant compliance and regulatory risks.

Another ethical risk involves transparency. Some AI systems may prove difficult for stakeholders to understand how decisions are made. This lack of transparency can create challenges in ensuring that AI-driven processes are fair and justifiable. Customers may find it hard to contest decisions or understand the rationale behind premium adjustments or claim denials, leading to a lack of trust in the insurer.

The European Insurance and Occupational Pensions Authority (EIOPA) has recognised the ethical challenges associated with the use of AI in insurance. It has developed a set of governance principles aimed at addressing these challenges and mitigating risks stemming from AI applications.[1] These principles are designed to ensure responsible and ethical AI deployment within the insurance industry.

REGULATORY RISK

The introduction of additional regulations such as the AI Act has significantly heightened exposures to regulatory and compliance risk for insurers. Inevitably, the rise in AI usage across the insurance industry has resulted in additional regulations to ensure the safe application of the technology. The increased regulation and compliance risk will be most material where high-risk AI models are utilised by insurers.

There is also an increased liability risk, as more provisions may need to be set aside to account for anticipated regulatory fines due to non-compliance.

In order to mitigate regulatory and compliance risk, (re)insurers will need to develop appropriate frameworks to ensure that they are complying with the requirements of the AI Act.

1 EIOPA (June 2021). Artificial intelligence governance principles: towards ethical and trustworthy artificial intelligence in the European insurance sector. Retrieved from: https://www.eiopa.europa.eu/publications/artificial-intelligence-governance-principles-towards-ethical-and-trustworthy-artificial_en

OTHER AI RISKS

There are many other potential risks associated with the rise in AI that could impact the insurance industry. For example:

- The automation of systems via increased use of AI poses a significant societal risk. The potential impact of job displacement resulting from AI-driven automation of systems remains to be seen. Systematic use of AI across the insurance value chain may lead to an increased dependency on technology.
- AI can also introduce legal risk, particularly concerning liability for errors. What happens when AI makes a mistake? Determining responsibility and liability may be complex and potentially contentious.
- Improper use of AI may result in increased reputational risk, particularly where it is used to make decisions regarding policyholder claims, or if there are inadequate and ineffective security measures, resulting in a data breach.

There are many other potential risk exposures, and the list is also likely to increase, as the use of AI becomes more prevalent across the (re)insurance industry and as advances continue with regard to the technology itself.

Where to start?

Many (re)insurance companies will already be using AI to some extent through the insurance value chain, even if it is just via the use of GenAI systems such as ChatGPT or company specific versions. A good starting place is to conduct an inventory of all instances of the use of AI throughout the organisation, by business unit, focusing on a very broad definition of AI to start with.

Once the inventory is complete, a company will be able to classify the use of AI into various categories, as defined under the AI Act, and take appropriate action for high-risk uses to comply with the regulations.

An overarching AI policy or strategy can also be a useful tool to set the tone in terms of defining the company's ambition for AI and setting boundaries as appropriate. It will also be appropriate to develop a framework for new use cases for AI models, to ensure that they are consistent with the company's strategy and are classified appropriately under the AI Act.

Conclusion

AI presents great opportunities for insurers, offering efficiencies, automation, innovation, and improved customer experiences, amongst other things. However, these advancements also bring additional risks for insurers that should be carefully managed through their risk management framework.

As the use of AI becomes more prevalent, it will be crucial to manage these risks through the risk management control cycle, robust policies and guidelines, and strong data privacy and security measures, and by maintaining a balance between automation and human oversight to ensure responsible AI use. Companies should also be proactive in preparing for the impending AI Act. An AI policy or strategy can be a good starting point in defining the company's ambition in this area and in clarifying boundaries.

With appropriate measures put into place, AI systems can operate within a controlled environment defined by the company's risk management framework and allow insurers to capitalize on emerging opportunities within the market.

If you are interested in discussing any of the topics discussed in this paper in more detail, please reach out to the authors of this briefing note, or your usual Milliman consultant.

Milliman

Milliman is among the world's largest providers of actuarial, risk management, and technology solutions. Our consulting and advanced analytics capabilities encompass healthcare, property & casualty insurance, life insurance and financial services, and employee benefits. Founded in 1947, Milliman is an independent firm with offices in major cities around the globe.

milliman.com

CONTACT

Sinead Clarke
sinead.clarke@milliman.com

Joseph Sloan
joseph.sloan@milliman.com

Nia Powis
nia.powis@milliman.com

Joanne Tan
joanne.tan@milliman.com