

NAVIGATING AI AND THE CLOUD



PETRA HIELKEMA

Chairperson – European Insurance and Occupational Pensions Authority (EIOPA)

The future of cloud computing and AI in the EU insurance sector

The importance of data analytics in insurance makes cloud computing and artificial intelligence (AI) key strategic technologies for the sector. Integrated platforms from cloud computing service providers simplify and therefore accelerate the deployment of AI by insurance undertakings across the insurance value chain.

Most European insurance undertakings already use cloud computing, with the services commonly outsourced from large technology companies (commonly referred to as “BigTechs”). According to EIOPA’s 2024 report on the digitalisation of the European insurance sector (hereinafter EIOPA’s Report), 80% of respondents already outsource cloud computing storage services from BigTechs.

Cloud computing service providers often cross-sell different services

alongside data storage or basic compute capacity. As shown in EIOPA’s Report, Software as a Service (SaaS) is the most common service purchased from cloud providers by insurance undertakings. In addition to data storage services, SaaS packages typically include services such as IT security programs, marketing platforms, anti-money laundering (AML) screening tools, Customer Relationship Management (CRM) solutions and other data analytics services, including AI.

EIOPA’s Report shows that 50% of the respondents already use AI in non-life insurance and 24% in life insurance. An additional 30% and 39% of respondents expect to use AI in the next three years in non-life and life insurance, respectively. Furthermore, 66% of the reported AI use cases were developed in-house by insurance undertakings themselves, while the remaining 34% were outsourced from third-party service providers.

The expectation is that the use of both cloud computing and AI will considerably increase in the years to come in view of their significant benefits, including enabling the development of more efficient and automated processes or helping insurance undertakings to generate value for their customers.

But the adoption of modern technologies also entails risks, with cyber security and data privacy issues being the most material risks perceived by insurance undertakings that participated in EIOPA’s Report. The concentration of cloud computing within a reduced number of service providers can also raise relevant operational resilience issues.

The introduction of Large Language Models and Generative AI solutions, which are also typically developed by large technology firms and research institutions, introduces further complexities. These models bring new or amplified risks and opportunities and can make it more difficult for downstream users such as insurance undertakings and intermediaries to address these risks, while also requiring the up-skilling of staff and new governance approaches.

Insurers need to keep pace with these developments to remain competitive, yet the adoption of these technologies can pose organisational challenges. According to the insurers that participated in EIOPA’s Report, issues related to acquiring adequate talent and skills and the transition from old legacy

systems to new platforms represent the most relevant constraints.

Regulatory frameworks also play a key role in this process. They should facilitate innovative data ecosystems, for instance by enabling access to relevant datasets as it is done under the Data Act, the Data Governance Act, or the proposal for a Regulation on a Framework for Financial Data Access (FiDA). Regulatory sandboxes and other innovation facilitators, such as those promoted in the AI Act, and which already exist in the financial sector for several years in line with the principle of proportionality recognised in Solvency II, can also be seen as a positive development.

In addition, while insurance legislation such as Solvency II or the Insurance Distribution Directive already regulate operational risks as well as the use of AI by insurance undertakings, new regulations such as the Digital Operational Resilience Act (DORA) and the AI Act aim to update the legislative framework for the digital age: by ensuring robust operational resilience frameworks against cyber-attacks and promoting the responsible use of AI systems that deliver fair outcomes to consumers. For example, the AI Act recognises the shared responsibility of the different actors throughout the AI value chain (developers, deployers, importers etc.), while insurers remain ultimately responsible for the critical activities they outsource under Solvency II.

Cloud computing and AI in the European insurance sector present opportunities and challenges.

Navigating different regulations and their potential overlaps can be challenging. EIOPA is committed to supporting the consistent and proportionate implementation of existing and new provisions as the regulatory landscape evolves, including by training supervisors in modern technologies through initiatives such as the EU Digital Finance Supervisory Academy. The aim is to ensure that stakeholders harness the benefits of digitalisation while safeguarding customer protection and financial stability in the markets.



ANDREW VENNEKOTTER

Head of Security Regulatory
Engagement, Europe –
Amazon Web Services (AWS)

AI is already helping the financial sector create new value streams, securely

Amazon Web Services (AWS) has been working on artificial intelligence and machine learning (AI/ML) for more than 20 years, but we are now at an inflection point in technology driven by the availability through the cloud of secure, cost effective, scalable compute, and the concurrent rapid advancements in the areas of algorithms and mathematics. Consumers as well have grown more comfortable with using AI in their daily lives. As technology is advancing, we are also seeing an increasing sophistication on the part of end users, who now expect more intelligent, automated, and personalized experiences.

To understand where the industry is going with AI/ML, we need to differentiate between traditional statistics, AI/ML, and generative AI (GenAI). The financial industry has long been using traditional statistics and AI/ML to explore data, perform inference and classification tasks, find patterns, and learn from data in order to make more informed decisions. By contrast, GenAI can create new content and ideas, including conversations, stories, images, videos, and music. Like all AI, generative

AI is powered by ML models—very large models that are pre-trained on vast amounts of data and commonly referred to as foundation models (FMs). Recent advancements in ML (specifically the invention of the transformer-based neural network architecture) have led to the rise of models that contain billions of parameters or variables.

The opportunities for value creation in the financial sector when using AI are wide-ranging. Currently, customers are telling us about four key benefits. First, AI helps them fight financial fraud by identifying potential threats faster and streamlining regulatory compliance processes. Second, AI helps customers generate personalized marketing content, which allows them to meet brand guidelines consistently as well as accelerate new account acquisitions. Third, customers have registered an increase in productivity as the tools support accelerated analysis and decision making. Finally, financial sector customers report an improved customer service and call center experience.

Let me illustrate with a few use cases. Mastercard uses AWS's AI/ML services to improve fraud detection capabilities globally. This has enabled Mastercard to detect three times the number of fraudulent transactions and reduce false positives tenfold, leading to billions of dollars in merchant savings and providing a better experience for customers. In the United States, one hedge fund has built an AI-powered investment analyst assistant that can generate charts, compute financial indicators, and create summaries of the results. This flexible solution enables analysts to spend more time understanding markets and economies. In early April, we announced a partnership with AXA, a global commercial insurance and reinsurance company, to co-develop the AXA Digital Commercial Platform (DCP), a risk management solution. This new solution will integrate industry, business and environmental data with geospatial analytics and GenAI technologies to help clients monitor their assets and navigate complex and interconnected risks including supply chain disruption, natural disasters and cyber threats.

Financial services organizations are also using AI to improve their own security. For example, NatWest data scientists and engineers are leveraging the latest GenAI models in a secure and scalable platform to build new services to combat the next generation of threats from financial crime.

One of our leadership principles states: "Success and Scale Bring Broad Responsibility." So as customers grow in their adoption of AI/ML and GenAI, we

need to help them do so in the right way. We emphasize responsible AI dimensions like accuracy, fairness, security, and privacy in developing GenAI.

We also help customers on this journey with tools like Guardrails for Amazon Bedrock, which allow customers to block as much as 85% more harmful content, filter out over 75% hallucinated responses for retrieval augmented generation (RAG) and summarization workloads, and apply safety, privacy and truthfulness protections within a single solution. Builders can use SageMaker Clarify to bolster explainability and mitigate bias. In addition, AWS collaborates with industry and participates in AI governance initiatives for developing standards and best practices.

**The financial sector
is using AI to achieve
intelligent, automated,
and personalized
experiences.**

As VP for Generative AI Vasi Philomin said in July 2024, we are "committed to working with companies, governments, academia, and researchers alike to deliver groundbreaking generative AI innovation with trust at the forefront."

This is an area where regulators can play a constructive role. We encourage them to collaborate with the industry to develop and promote assurances and best practices that are consistent with existing risk-based legislation and aligned with international initiatives and standards. This would help ensure the financial services industry can innovate by leveraging AI responsibly while maintaining global competitiveness.



EMILY PRINCE

Group Head of Analytics –
London Stock Exchange
Group (LSEG)

‘Reframing financial services’ future with AI: making better and faster decision

Generative AI is creating new possibilities for the financial services industry, especially in the form of enhanced productivity and data discoverability. It brings a universe of opportunities for people to interact differently with vast amounts of data and to empower their decision-making.

While more data suggests more automation, decision-making and accountability will still lie with humans. However, the focus of human input is shifting to controlling where data comes from, how it is managed and treated, and ensuring that outputs are accurate, auditable and unbiased.

As part of this, risk and data management literacy will continue to grow as a fundamental requirement for financial services professionals across various roles. Regulations such as the GDPR, the EU AI Act, and the Digital Operational Resilience Act (DORA) are already bringing this to the forefront through new requirements and clear accountability.

Flexibility and Interoperability are Key When Innovating with AI

To gather and analyse the volumes of data now available to them, financial services organisations need a modern and resilient data architecture. Companies are strategically augmenting their existing tech stacks to create a flexible, yet unified data architecture capable of supporting AI projects at scale.

At the same time, companies integrating third-party data or technology for AI purposes face increased scrutiny from policymakers regarding supplier concentration, data privacy, or audit risks. However, with the right controls in place, flexibility, and human oversight, a safe and effective environment for AI innovation can be achieved.

At LSEG, our ability to successfully deliver critical operations and timely data, regardless of circumstances, is key to our business as a financial market infrastructure and data provider. Developing an AI framework for finance is more than just using technology. It’s about building trust, ensuring robust governance, and instilling a culture of ethical AI usage.

Importance of Guardrails and a Responsible Approach

The financial services industry relies on pinpoint accuracy, and for most of the existing AI use cases, risks tend to be centred around data. Generative AI is only as good as the quality of the data it is trained on, making it particularly important to actively mitigate risks associated with AI hallucinations, data bias, and privacy.

Governance frameworks should be ‘responsible by design’. This includes setting policies, standards, and procedures and integrating risk management into all stages of the AI development lifecycle. Responsibility also lies in how companies decide to embed AI within their existing processes. This means choosing the right AI tools that best solve specific tasks and deploying them in the most appropriate use cases, maximising benefits while reducing and effectively mitigating risks.

Looking Ahead on Policy

The private sector has a key role to play by clearly implementing and demonstrating a responsible usage of AI. Doing so will enable businesses to scale their governance and work closely with policymakers on developing practical AI regulations that ensure the safety and privacy of users and consumers. Many businesses are proactively seeking to integrate AI governance into their

operations, but this process requires time and legal certainty when investing in resources for AI implementation.

The EU AI Act stands as an important marker in AI governance, reshaping the way companies approach AI deployment and development. As financial regulators take stock of existing use cases and examine the implications of AI in financial services, guidance is beneficial. However, such guidance should be principle-based and focused on risks rather than specific technologies or types of AI models.

Developing an AI framework for finance is more than just using technology. It’s about building trust.

Finally, facilitating multistakeholder collaboration and international consensus will help to clear the path towards a global approach to responsible AI and mitigate the risk of policy fragmentation. The work of policymakers and new AI agencies such as the EU AI Office should now focus on helping firms subject to the EU AI Act to implement these requirements, including via guidance and industry engagement.

In addition, supporting international efforts will ensure the interoperability of different AI governance frameworks. As AI technology develops and other initiatives emerge, policymakers should ensure that the existing legislative framework is flexible enough to be implemented alongside other jurisdictions’ frameworks and remain relevant for upcoming AI use cases.



MATTHIAS PETER

Partner, Financial
Services – KPMG

AI in the financial services - Managing risk and fostering innovation

Information gathering and processing are fundamental to financial services. This is evident from historical innovations: Lloyd's of London, initially a coffee house in the 17th and 18th centuries, served as an information exchange for sailors and ship owners. Moreover, the 'ticker' from the ticker tape machine, a late 19th-century innovation, enabled real-time stock price updates. The internet and cloud computing, recent innovations, have enabled fast banking apps that are transforming customer interactions with banks globally.

Banks have long worked on automated information processing, as shown by the prevalence of legacy IT systems built inhouse. These systems predate current AI methods, which are now crucial for banks in knowledge derivation, decision support, and automation to reduce costs, to optimize processes, or to even improve customer experience. Like this, AI addresses broader industry challenges like skilled worker shortages and cost pressure from intense competition in banking markets.

The initial introduction of AI, particularly machine learning, saw a

mutated response in risk management due to existing robust frameworks. Established regression models like probit and logit for credit default predictions meant that many in industry and regulation, saw no need for significant changes in model risk management, affirming that existing regulations sufficiently cover AI models.

The release of ChatGPT in late 2022 marked a shift. Unlike traditional machine learning, GenAI applications like ChatGPT allow user interaction without coding knowledge, producing outputs like text, images, and videos in user-friendly formats. This easy accessibility offers both opportunities and risks.

GenAI models pose specific challenges.

The EU AI Act is the first comprehensive legislation in the EU to address AI-related challenges through a risk-based approach. It categorizes applications into banned, low-risk, and high-risk categories, with stringent requirements for high-risk scenarios on transparency and fairness.

The EU AI Act identifies credit scoring and life and health insurance pricing as high-risk. Due to its broad AI definition, the act affects existing models. At the same time, the Act's risk-based approach struggles with GenAI's versatility, as one model can serve numerous use cases, imposing extensive requirements, especially on third-party providers. Outputs from GenAI models must be meticulously scrutinized to manage risks effectively.

AI Risk Management is key to leverage the benefits of the new technologies.

GenAI presents unique challenges in bias identification and mitigation, as direct data access is often unavailable. Evaluation methods for these models include:

- **Automated Evaluation:** Uses statistical models to assess and compare responses.
- **Model-Based Evaluation:** Another trained model evaluates the model.
- **Human Evaluation:** A human assesses and validates GenAI outputs.

Additional challenges and regulatory intricacies include but are not limited to data protection and the necessity for cloud-based data hosting of GenAI solutions.

AI Model Risk Management is key to leverage the benefits of new technologies.

Initially, the financial services industry increased awareness of GenAI risks by blocking direct access to OpenAI's ChatGPT and advising against using GenAI chatbots with bank data on personal devices. This was a reactive measure. Now, the industry is proactively identifying GenAI use cases, defining AI governance and strategies, and providing employees with secure GenAI solutions and training to enhance their output.

In the long run, banks need to evolve their model risk management frameworks to include AI models. Traditional ML methods like supervised learning can be integrated into existing frameworks with relative ease. Integrating GenAI models is harder. For instance, a sharpened focus on model use is required, considering the broad capabilities of GenAI and the use-case-based nature of AI regulation. Also, adhering to industry and regulatory standards (e.g., NIST standards) ensures the necessity that validation processes go beyond statistical accuracy.

Traditional ML methods typically run on-premise, giving banks full control over data and models. In contrast, banks lack the data to train their own GenAI. To leverage managed open-source and proprietary models hosted by external providers a cloud application strategy for GenAI is required.

Banks' Model Risk Management frameworks are a good base for managing AI model risk.

GenAI represents a significant innovation in financial markets. To replicate the success of past innovations, the industry must grasp GenAI's benefits and manage its risks effectively.

Fortunately, there is no need to reinvent the wheel. Existing bank model risk management frameworks provide a strong base. It is crucial to enhance these frameworks to fully leverage GenAI while controlling its risks. Augmenting these frameworks by accounting for AI regulatory guidelines and implementing industry standards will be the next steps to be taken.