



DAMIAN JAWORSKI

Executive Director – European Insurance and Occupational Pensions Authority (EIOPA)

Scaling AI in finance: systemic risks, resilience and European sovereignty

Artificial Intelligence (AI) is moving from experimentation towards established use across financial services in general, including in the insurance sector. EIOPA's 2025 Generative AI market survey, covering 347 insurers in 25 EEA countries, found that 65% were already using generative AI and another 23% planned to do so.

As AI is deployed across the insurance value chain, it creates both opportunities and new financial stability challenges. AI technologies are increasingly used in fraud detection, customer service, claims management and data analysis.

These technologies may improve efficiency and support innovation; however, they also amplify cyber and operational risks, increase reliance on external technology providers and may contribute to market concentration and interconnectedness.

Advanced AI systems may also increase the sophistication of cyberattacks, automated fraud and social engineering techniques, making cyber risk more

dynamic and potentially more difficult to model using traditional actuarial approaches.

Against this background, EIOPA, alongside the other two European Supervisory Authorities, has raised awareness about the ICT risks posed by the widespread adoption of advanced AI models and engaged with EU competent authorities to ensure that financial entities take appropriate mitigation measures. In their first annual report on major ICT-related incidents under DORA, the ESAs encouraged financial entities to strengthen cybersecurity measures to maintain their resilience amid the rapid evolution of highly capable AI-driven tools.

The ESAs also concur with the ESRB's recent warning on the systemic cyber risks stemming from frontier AI models, whose ability to identify and exploit high-severity vulnerabilities within very short timeframes has advanced significantly. Financial entities are encouraged to make appropriate arrangements to adapt their cybersecurity capabilities, and competent authorities to reflect these developments in their supervisory activities. They can also strengthen defence through faster detection and response.

These developments underline the importance of strong governance frameworks, effective risk management practices and robust supervisory oversight. They also expose Europe's dependence on non-European providers for critical IT infrastructure and AI technologies.

The safe scaling of AI requires effective supervision alongside a diversified European AI ecosystem.

A strong framework, with implementation as the priority

The EU already has a strong regulatory framework. DORA addresses ICT risk management, testing, incident reporting, contractual safeguards, concentration risk and exit strategies, and establishes oversight of critical ICT third-party providers. The AI Act complements it through requirements for AI systems and GPAI model providers, including additional obligations for models presenting systemic risks. In EIOPA's survey, 59% of respondents considered the AI Act's generative AI provisions

useful or very useful for improving provider reliability.

These instruments do not specifically identify correlated model behaviour, common dependencies across models and integrators, or simultaneous AI-driven market reactions, but they enable it. Therefore, effective implementation and coordinated supervision are more effective than another legislative layer. Financial entities and supervisors should map material dependencies, test provider or model failures, verify that exit plans work, and improve information-sharing. Financial entities should retain human expertise, fallback capacity and sufficient provider diversity.

CADA and the supply side

The Cloud and AI Development Act (CADA), the AI Continent agenda and the European Technological Sovereignty Package can complement these efforts by addressing the supply side. CADA aims to triple the EU's data-centre capacity within five to seven years, accelerate infrastructure deployment and establish an EU-wide framework for assessing cloud and AI sovereignty. Together with AI Factories, AI Gigafactories, investment support, skills initiatives and the EU Open-Source Strategy, these initiatives could broaden access to European computing infrastructure and AI models while fostering a more diverse and competitive ecosystem.

However, while sovereignty enhances resilience, the two are not synonymous. Reducing dependence on a handful of non-EU providers only to create dependence on a handful of EU providers would leave the underlying concentration risk largely unchanged. Sustained efforts to promote competition, interoperability and portability therefore remain essential to building long-term resilience.

To conclude, AI scaling is beneficial and should be enabled, but its dependencies must be visible and manageable. At this stage, the EU does not need another broad layer of AI regulation for finance. The priority is rigorous implementation of DORA and the AI Act, coordinated monitoring and targeted supervisory action wherever concrete gaps emerge.