

ARTIFICIAL INTELLIGENCE AND DIGITAL OPERATIONAL RESILIENCE IN THE EUROPEAN INSURANCE SECTOR

17/19/2026
Assal Conference

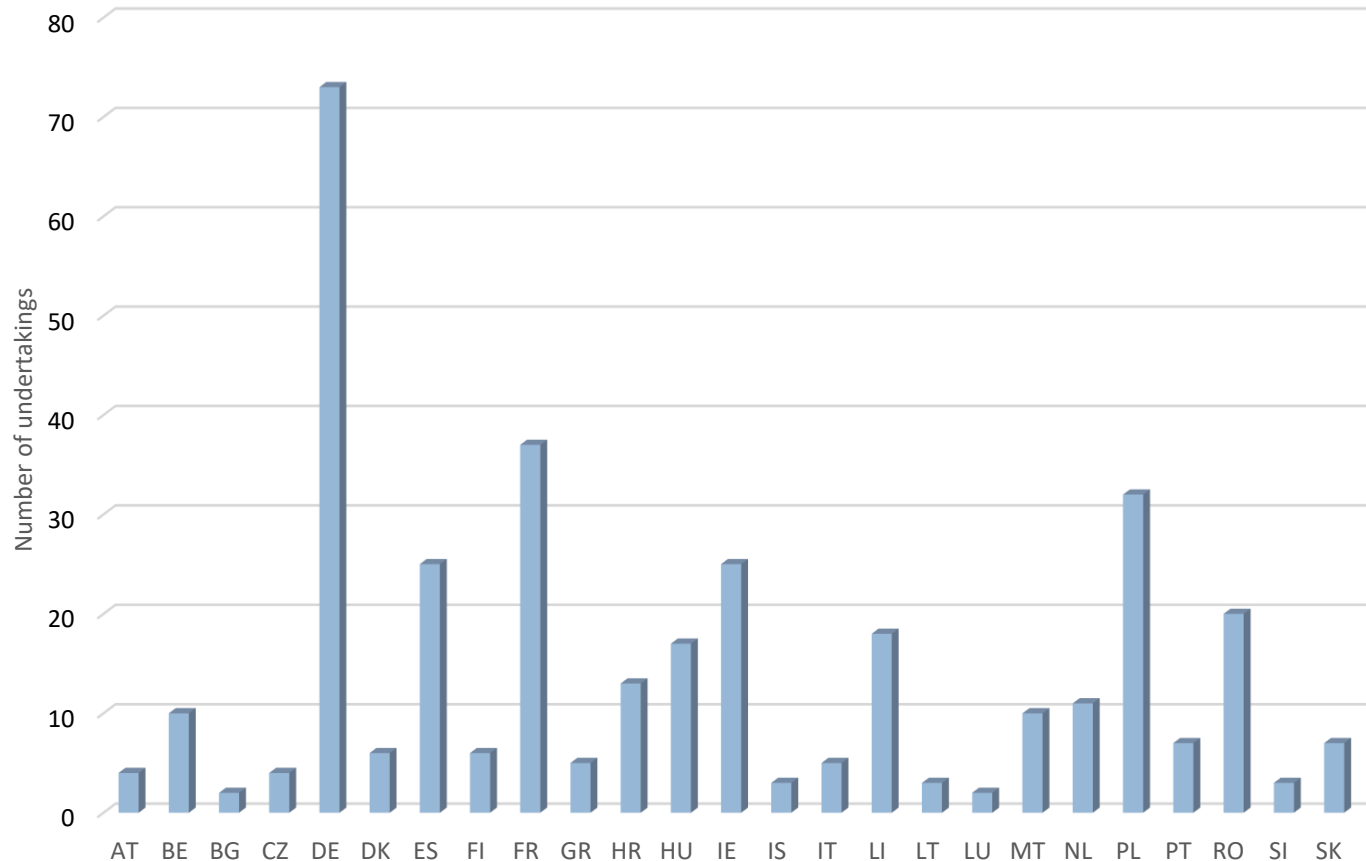
GENERATIVE AI MARKET SURVEY: OUTLOOK, USE CASES AND RISK MANAGEMENT

GENERATIVE AI SURVEY

- INTRODUCTION

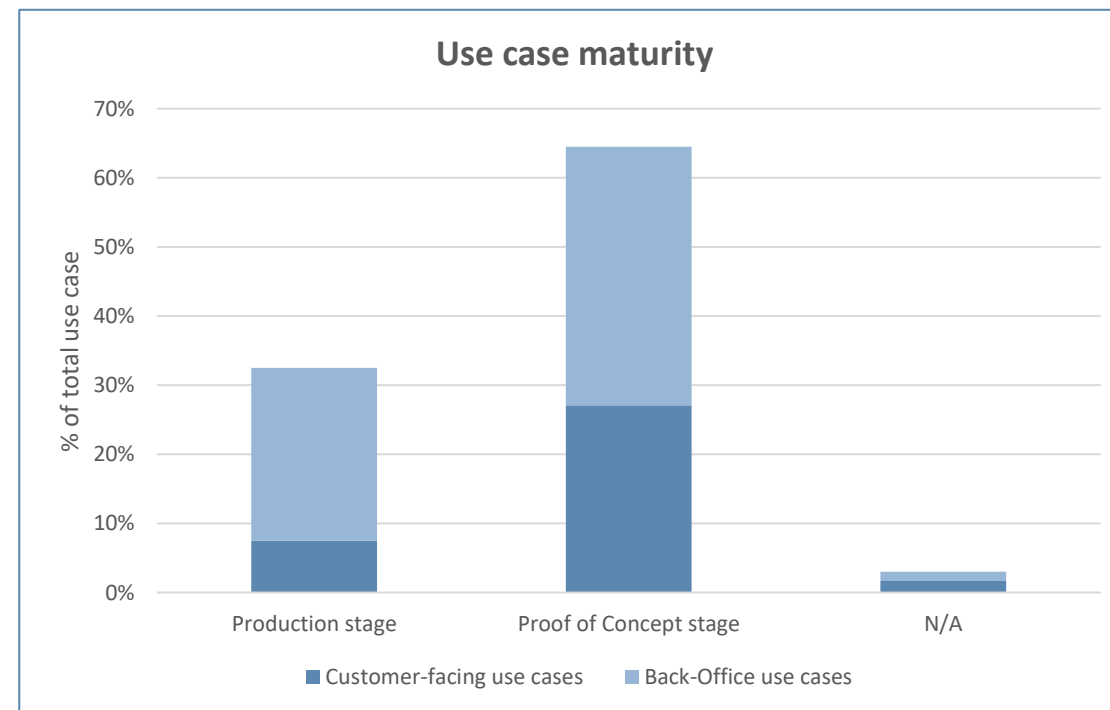
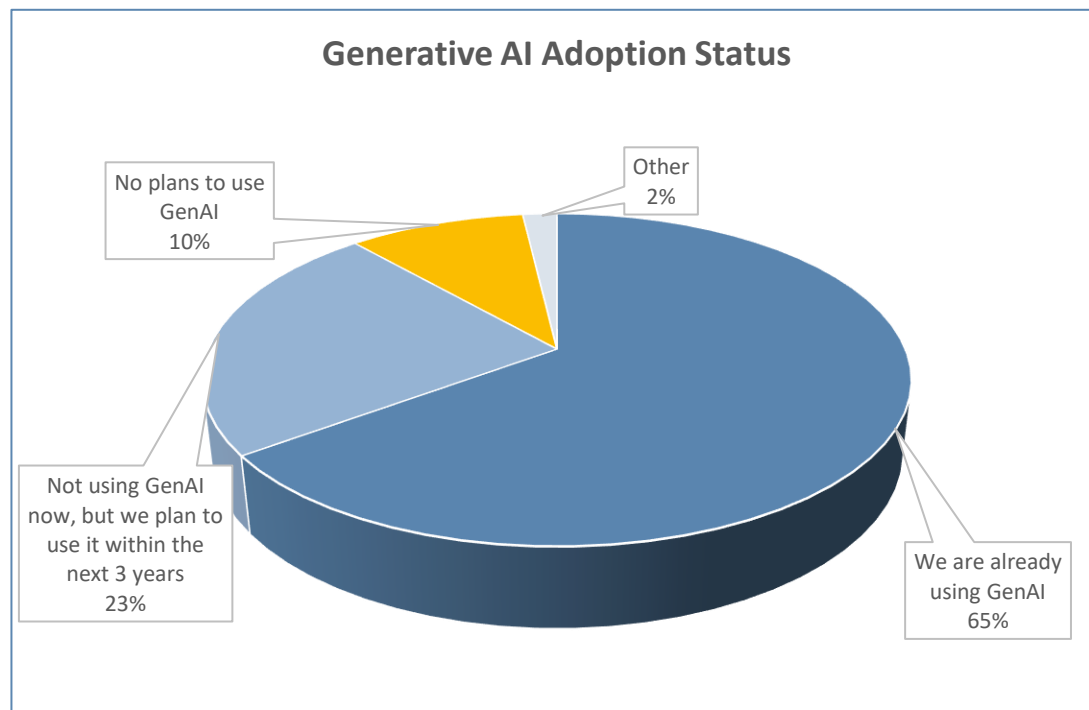
Overview

- **Objective:** monitor Gen AI adoption, including applications, market developments, regulation, risks and barriers to Gen AI innovation
- **Methodology:** market survey conducted between May and July 2025, complemented with Eurobarometer survey
- **Scope:** Generative AI adoption, Implementation & data, Applications and Use Cases, Governance & risk management, Challenges, AI Act, Agentic AI and Carbon footprint
- **Geographical distribution:** the analysis includes responses from 347 insurance undertakings across 25 EU (and EEA) countries.
- **Targeted market coverage:** $\geq 60\%$ of Gross Written Premiums per national market.



GENERATIVE AI SURVEY

- GENERATIVE AI ADOPTION

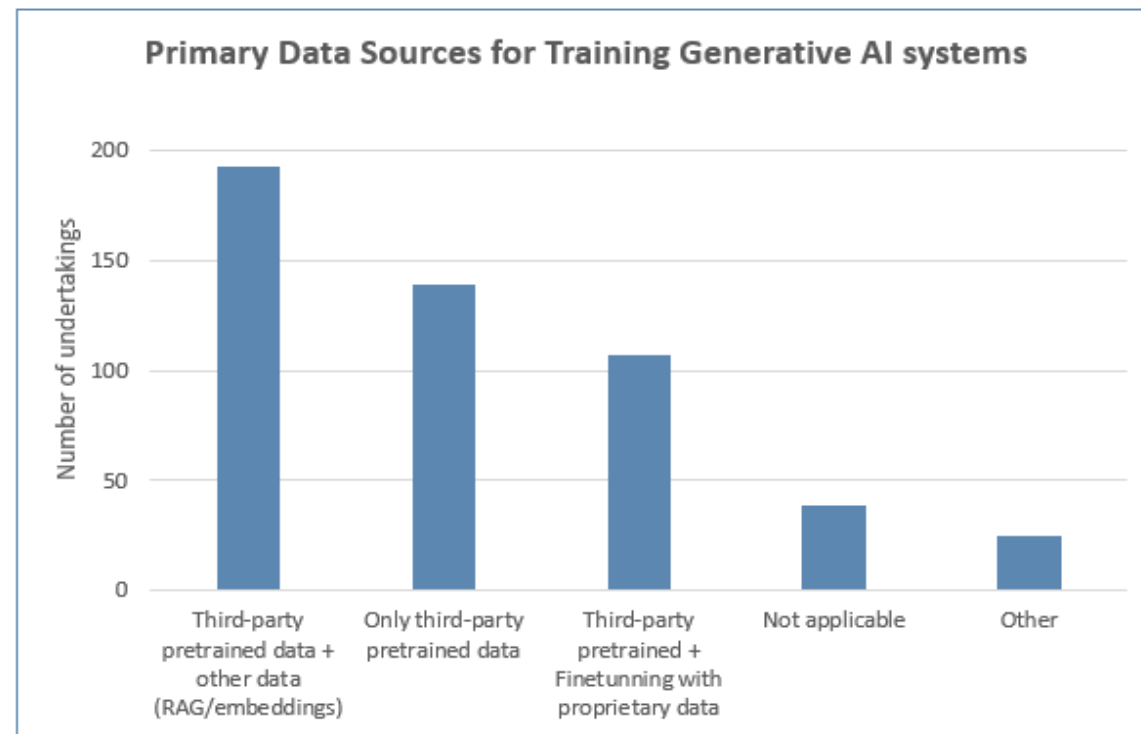
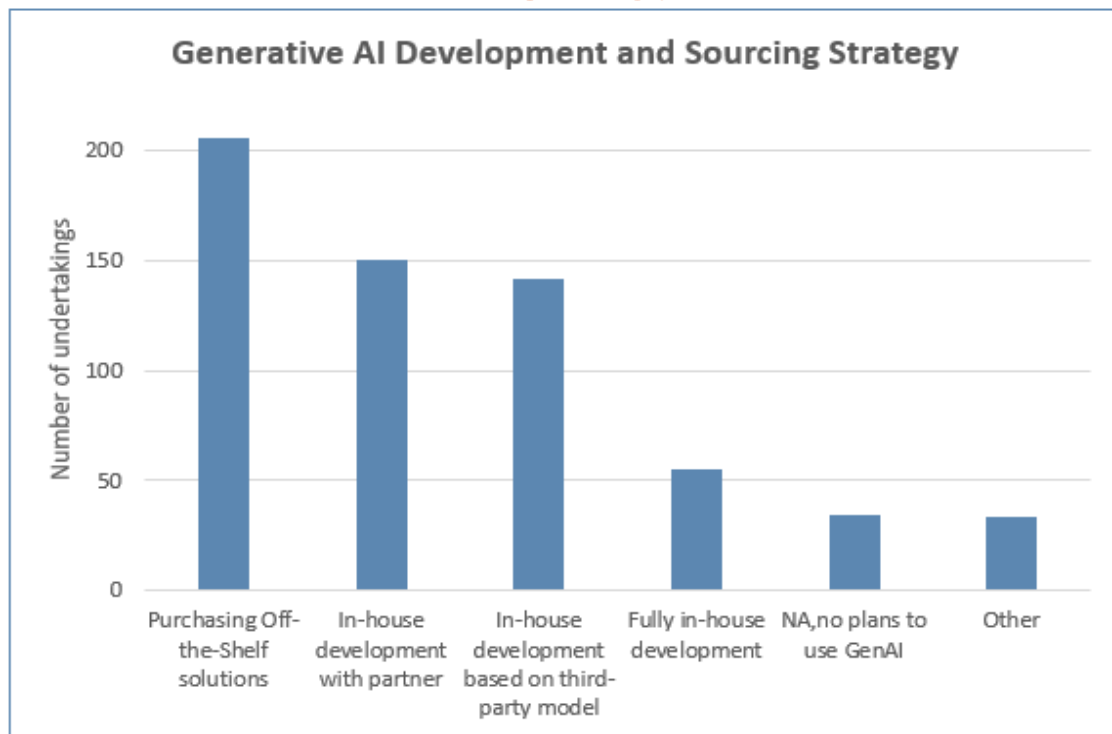


Key takeaways:

- **Survey data indicates that 65% of undertakings** are already actively using Generative AI (excluding self-usage by staff), and a further 23% are planning to implement it within the next three years.
- **High growth potential**; the majority of use cases are at a proof-of-concept stage, especially concerning customer-facing applications.
- **Controlled scaling of Gen AI** : Most of the use cases focus on back-office applications with Human Oversight

GENERATIVE AI SURVEY

- IMPLEMENTATION & DATA

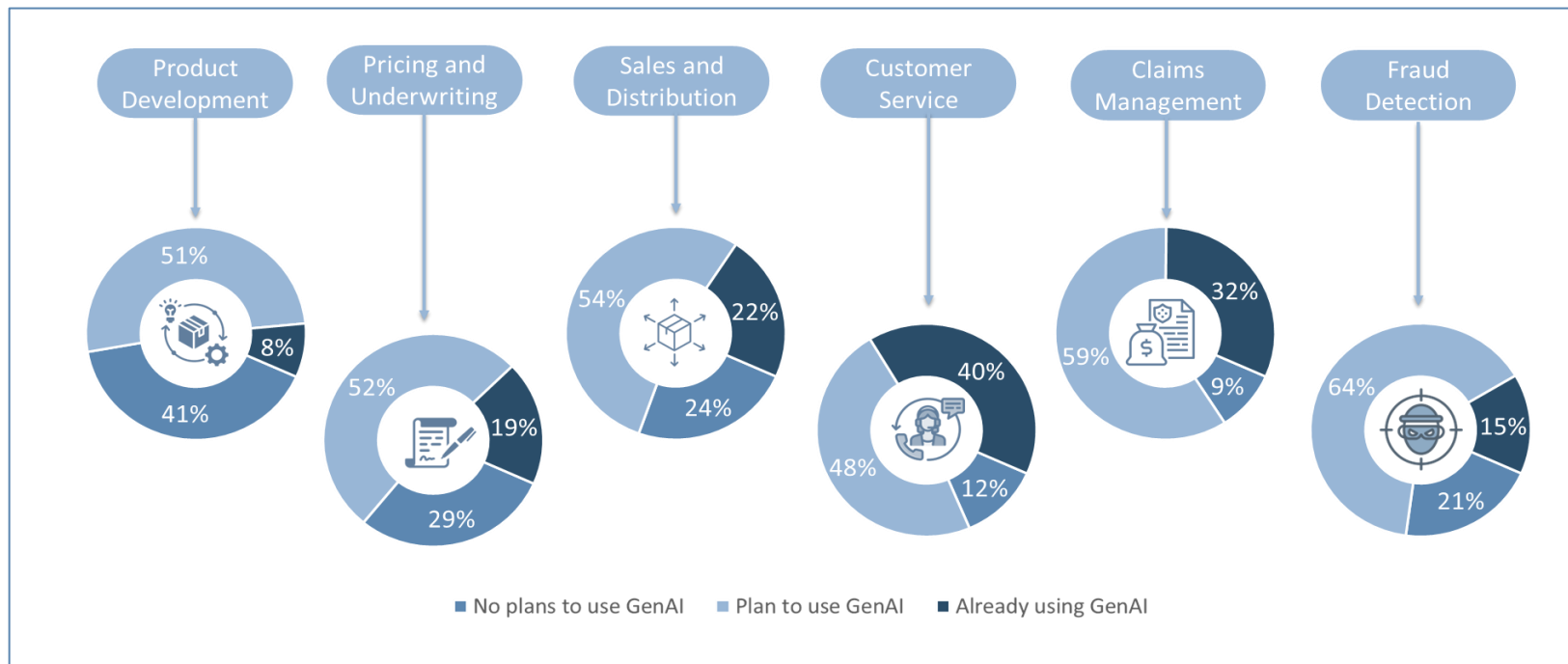


Key takeaways:

- Insurers will normally choose a **“mix” of solutions** based on their organisational needs, such as the specific use case where Gen AI will be implemented, time-to-market constraints or costs considerations.
- **Reliance on third-party service providers:** The preferred approach for insurers is now to purchase off-the-shelf solutions from third-party service providers, marking a significant shift away from the previous preference for in-house development, as indicated in earlier AI surveys.
- **Gen AI systems are pre-trained by third-party service providers on external data sources**, and subsequently insurers can enhance them with alternative data sources and techniques such as Retrieval-Augmented Generation (RAG) and embeddings or finetuning with proprietary data.

GENERATIVE AI SURVEY

- USE CASES ACROSS THE INSURANCE VALUE CHAIN



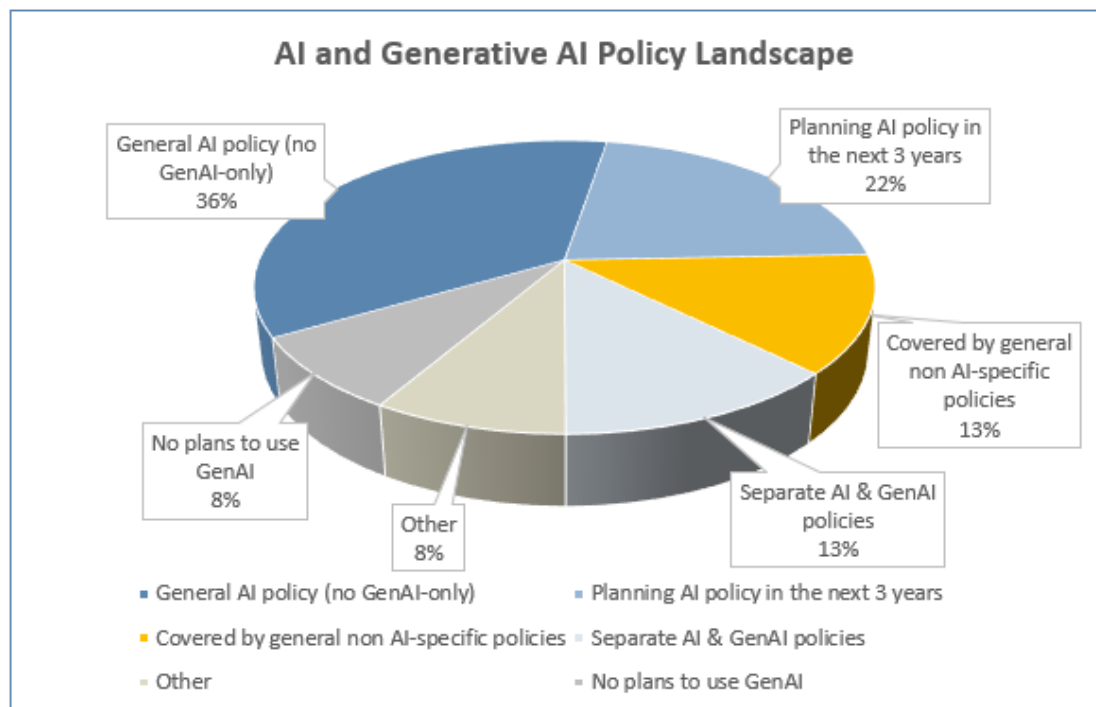
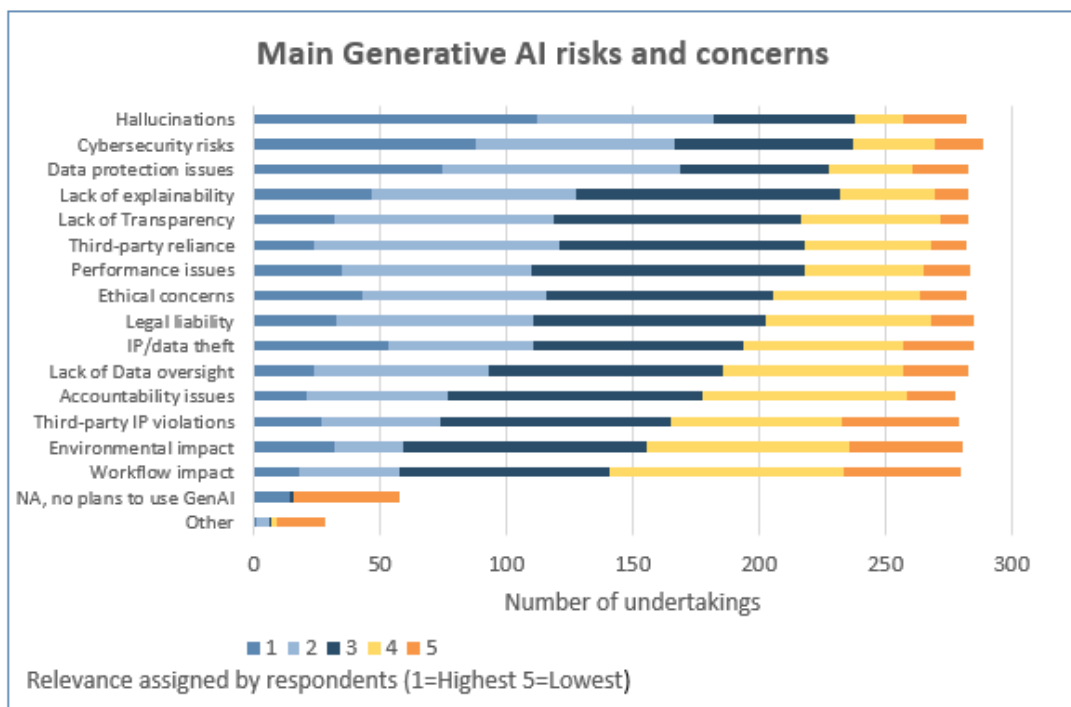
Key takeaways:

- Current Gen AI uses cases are focused on **Customer Service** and **Claims Management**, while top future interest is in areas like **Fraud Detection**.
- Without counting back-office applications, current GenAI adoption is most matured in **Non-life insurance**; in contrast, **Life insurance** shows higher future interest
- Use cases with **Human Oversight** dominate (>83%), but **Agentic AI** adoption is expected to grow considerably; majority expects it to be transformative over the next 3–5 yrs.

Identified Use Cases	Examples
Conversational AI	Customer Q&A,, contract updates.
Writing & Content Generation	Draft emails, marketing content.
Data Extraction	Invoices, reports, voice insights.
Text Summarization	Medical reports, contracts.
Knowledge Management (RAG)	Employee search tools, underwriting LLMs.
Code Assistants	Coding help, test scripts.
Process Automation	Invoice processing, email routing.
Translation	Policies, FAQs.
Scenario Modelling	Risk and pricing analysis.

GENERATIVE AI SURVEY

- GENERATIVE AI RISKS AND GOVERNANCE



Key takeaways:

- **Hallucinations (i.e. accuracy)** is the foremost relevant risks identified with Generative AI.
- **Insurance undertakings are adapting their governance and risk management frameworks**; 49% of undertakings have developed a dedicated AI policy (a twofold increase from 2023).
- **Compared to traditional AI systems (e.g. supervised machine learning algorithms), Gen AI systems require greater focus on the model inference stage and closer collaboration with third-party service providers**



ARTIFICIAL INTELLIGENCE ACT

AI ACT'S RISK-BASED FRAMEWORK

Risk based approach

Unacceptable risk 2 Feb 2025

Prohibited as contravening Union values

High-risk 2 August 2026

Comprehensive set of obligations

Transparency risk 2 August 2026

Limited transparency risk: transparency obligations

Minimal to no risk

Voluntary codes of conduct

General Purpose AI models 2 August 2025

Protection of fundamental rights, health and safety

Primarily apply to high-risk use cases (Annex III)

→ Risk assessment and pricing for life and health insurance

Governance requirements for high-risk AI systems

→ Responsibilities distributed to different actors in the AI value chain (providers, deployers, etc.)

Application: 2 Aug 2025

→ Digital Omnibus –requirements for high-risk AI systems postponed until Dec 2027

HIGH-RISK AI SYSTEMS

□ Governance and risk-management requirements for high-risk AI systems

Establish and implement risk management systems

Use high-quality **training, validation and testing data** (relevant, representative etc.)

Establish **documentation** and **record-keeping** logging features (traceability & auditability)

Ensure appropriate certain degree of **transparency** and provide users with **information** (on how to use the system)

Ensure **human oversight** (measures built into the system and/or to be implemented by users)

Ensure **robustness, accuracy** and **cybersecurity**

□ Providers

- Ensure that AI systems comply with the obligations outlined above.
- Registration in the EU database, quality management system (including post-market monitoring), maintaining documentation, and ensuring that systems undergo a conformity assessment and affix the CE marking.

□ Deployers

- Use high-risk AI systems in accordance with the instructions
- Assign human oversight and inform the provider or distributor
- Ensure that input data is relevant in view of the intended purpose
- Prior to the first use conduct a fundamental rights impact assessment

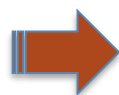
GENERAL PURPOSE AI MODELS (GPAI)

- **GPAI model:** AI model that displays significant generality and is capable to competently perform a wide range of distinct tasks and that can be integrated into a variety of downstream systems or applications
- The **AI Office** is responsible for application of rules on GPAI models
- **Obligations for providers of GPAI and GPAI models with systemic risk**
 - Transparency obligations, including drawing up technical documentation
 - Closely cooperate with the providers of the high-risk AI systems that integrate the GPAI model
 - Make publicly available information of the content used for training the GPAI model
 - Cooperate with the Commission and NCAs
 - Codes of Practice to demonstrate compliance with the obligations
 - Additional requirements for GPAI with systemic risk
 - Some exceptions apply for GPAI models under free open license

COM GLs scope of obligations for providers of general-purpose AI (GPAI) models

INTERPLAY BETWEEN THE AI ACT AND INSURANCE LEGISLATION

	AI ACT	INSURANCE LEGISLATION
OBJECTIVES	► protection of fundamental rights, health, and safety	► consumer protection, solvency, and financial stability
GOVERNANCE	► The AI Act introduces a comprehensive governance and risk management framework for providers of high-risk AI systems. Insurance undertakings as providers or deployers of high-risk AI systems already have to comply with a comprehensive system of governance requirements. ► To address potential overlaps the AI Act introduces limited derogations applicable to undertakings subject to Solvency II, e.g. risk management system, post-market monitoring system.	
SCOPE	► AI systems, providers and users ► requirements primarily focused on high-risk use cases	► activities of direct insurance and reinsurance ► activities of insurance and reinsurance distribution
OUTSOURCING	► Using third-party AI systems could be considered outsourcing under Solvency II. The AI Act establishes different obligations and responsibilities for the different actors of the AI value chain (e.g. providers, deployers, importers etc.). However, insurance undertakings remain fully responsible for all their obligations under Solvency II when they outsource functions or any insurance activities.	



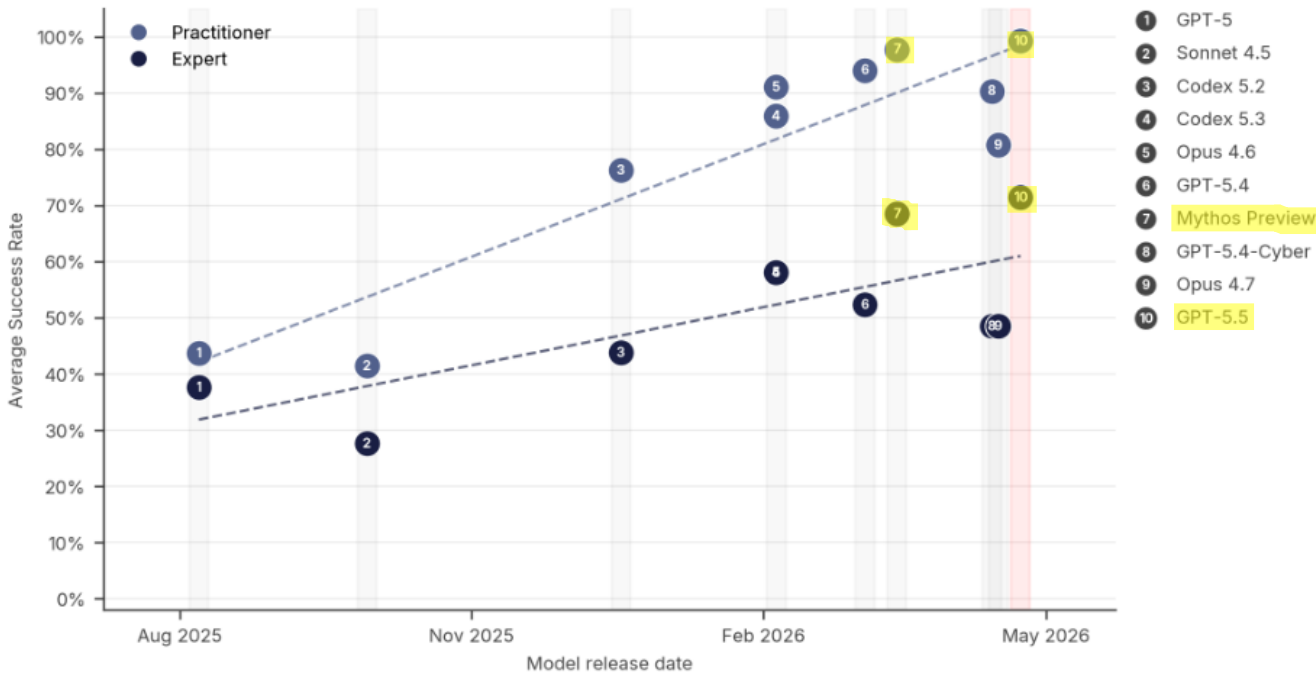
EIOPA's Opinion on AI governance and risk management clarifies how insurance sector legislation applies in the context of AI ([link](#))

FRONTIER AI MODELS - DIGITAL OPERATIONAL RESILIENCE

EVIDENCE: STRONGER PERFORMANCE ON CYBER EVALUATIONS

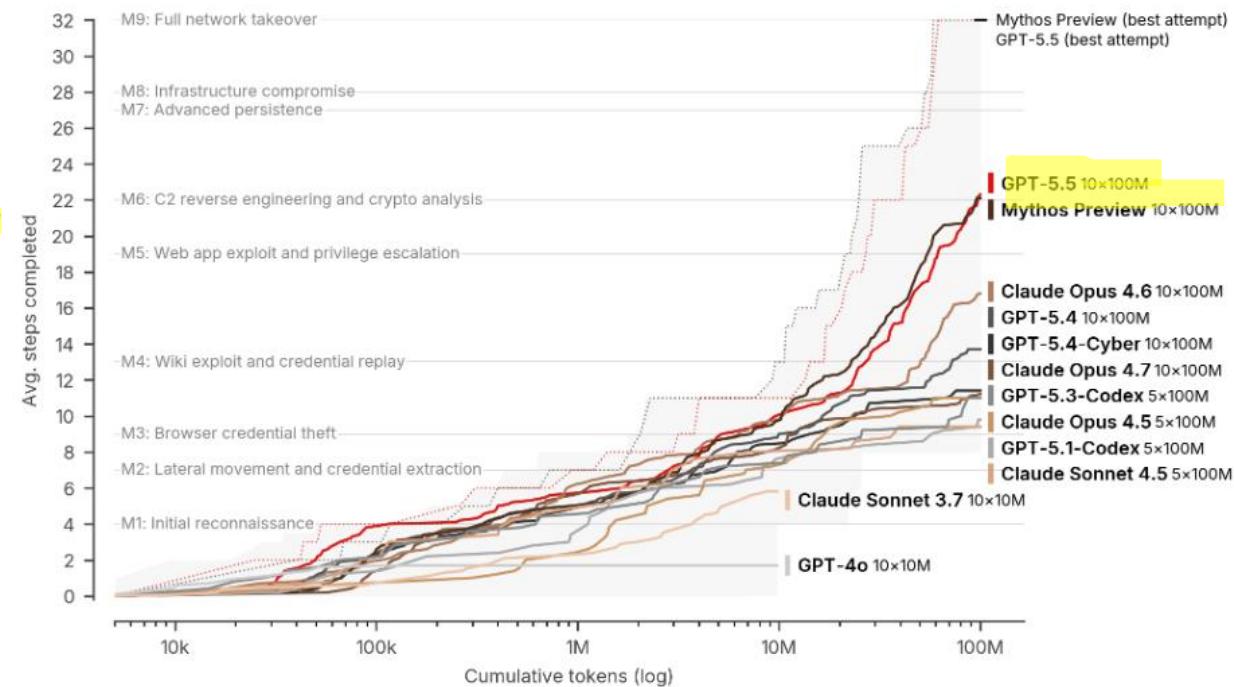
UK AI Security Institute evaluated frontier models on cyber tasks designed to test vulnerability research, exploitation and multi-step operational capability.

Advanced CTF Performance by Model (50M token budget)



On narrow cyber capture-the-flag tasks, both models reached expert-level performance.

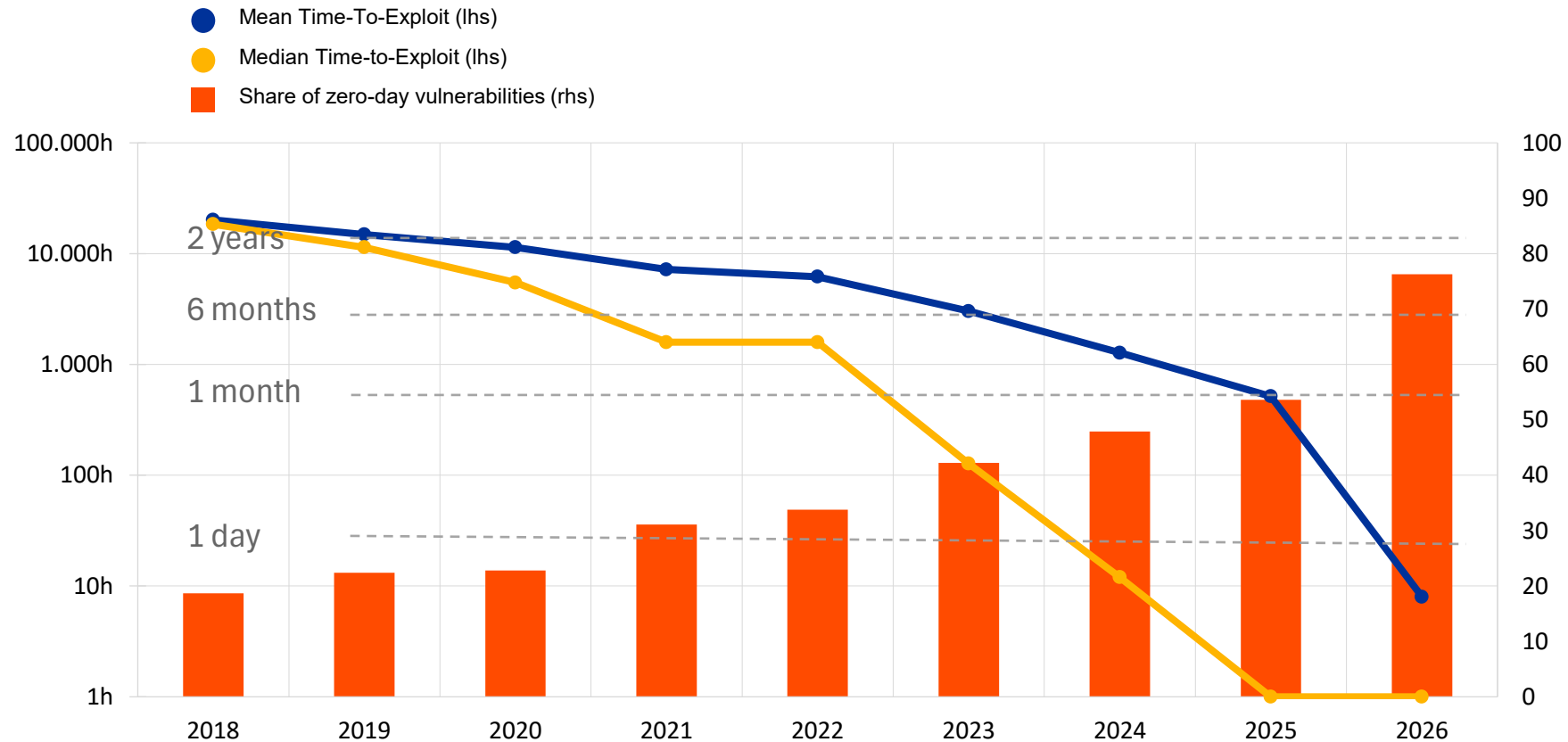
Completed steps on "The Last Ones" per spent tokens



In "The Last Ones", a 32-step corporate-network attack simulation across multiple subnets and hosts, both models completed the full chain in some attempts

COLLAPSE OF DEFENSIVE TIME BUFFERS

The time between identification of a system vulnerability and its exploitation has fallen rapidly
(lhs: hours (log scale); rhs: percentage)



Source: Zero Day Clock

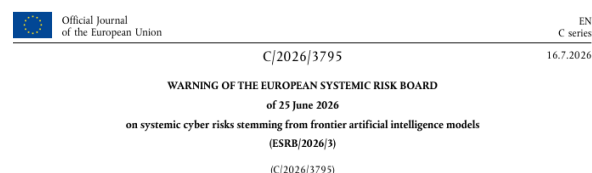
Notes: TTE (Time-To-Exploit) measures the gap between cyber threat public disclosure and first confirmed in-the-wild exploitation (zero = same-day). Percentage of zero day, shows the share of exploited vulnerabilities, where exploitation occurred before or on the day of disclosure (TTE $\leq$ 0).

IMPLICATIONS FOR INSURANCE AND FINANCIAL SECTOR

- **Accelerated vulnerability discovery:** by using AI vulnerabilities can be identified and exploited significantly faster and at lower cost than under current conditions.
- **Collapse of defensive time buffers:** the traditional window between vulnerability discovery and public disclosure—allowing vendors to patch systems—may be materially reduced, increasing the likelihood of disruption to critical functions.
- **Pressure on firms' vulnerability management:** institutions using such models may face operational strain due to the volume and speed of required patching activities. Legacy systems and size of firms matter.
- **Third party and concentration risk:** a vulnerability in a third-party provider could affect multiple financial entities at the same time
- **Cyber insurance:** implication of models on cyber insurance books, underwriting strategies and protection gaps is an area that EIOPA may need to monitor closely.
- **Holistic perspective:** Board and senior management must be literate on the issue to understand the potential implications for ICT risk appetite, remediation capacity, outsourcing dependencies, business continuity and cyber insurance exposure.

FRONTIER AI MODELS – SUPERVISORY RESPONSE

Warning of the European Systemic Risk Board



THE GENERAL BOARD OF THE EUROPEAN SYSTEMIC RISK BOARD,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to the Agreement on the European Economic Area ⁽¹⁾, and in particular Annex IX thereto,

Having regard to Regulation (EU) No 1092/2010 of the European Parliament and of the Council of 24 November 2010 on European Union macroprudential oversight of the financial system and establishing a European Systemic Risk Board ⁽²⁾, and in particular Article 3(2), point (c), and Articles 16 and 18 thereof,

Having regard to Decision ESRB/2011/1 of the European Systemic Risk Board of 20 January 2011 adopting the Rules of Procedure of the European Systemic Risk Board ⁽³⁾, and in particular Articles 18 and 19 thereof,

Whereas:

- (1) Leading artificial intelligence (AI) providers have developed Frontier AI Models (FAIMs), which are highly capable in the cybersecurity domain and able to carry out fully automated cyber-attacks on complex systems, including through vulnerability discovery and the development and weaponisation of exploits, thereby fundamentally changing the cyber-threat landscape.
- (2) FAIMs are significantly better than earlier AI models in finding ways to carry out cyberattacks, outperforming earlier models in cost, speed and accuracy, now rivaling leading human experts.
- (3) FAIMs have the capability to threaten the systems underpinning the information and communications technology (ICT) environments on which financial infrastructure relies, increasing the probability and severity of cyber incidents with systemic impact.
- (4) FAIMs have demonstrated the capability to discover vulnerabilities and craft novel exploits, thereby exposing major operating systems and software used across almost all organisations' ICT environments to the risk of cyber-attacks.
- (5) Historically, the discovery of such vulnerabilities has been rare and often made by security researchers, allowing for targeted remediation. In those cases, software providers are often given a standardised timeframe – usually 90 days – to patch the vulnerability before its public disclosure. However, FAIMs are likely to increase the volume of vulnerabilities found.

Statement of the European Supervisory Authorities



ESA Statement

Toward a consistent and risk-based approach for ICT risks from frontier AI models

1. The advanced capabilities of recent frontier AI models significantly accelerate cyber risks, underscoring the urgent need for robust cybersecurity measures and rapid incident response capabilities. AI-enabled cyber tools could generate systemic risks due to their ability to: i) rapidly discover and exploit vulnerabilities; ii) target vulnerabilities in shared infrastructure; and iii) leverage single points of failure across entities¹. While these models can help deliver substantial defensive improvements, they can also provide an advantage to malicious actors, which could leverage these capabilities, while defenders need to implement their responses following quality assured protocols.
2. On 7 July, the European Commission published its Action Plan on Cybersecurity and Artificial Intelligence to reinforce the EU's cybersecurity and resilience². In this context, the ESRB stressed in its issues note and in its warning³ that the misuse of highly capable AI models could have a substantial impact in the financial system. If such disruptions persist for several days or affect multiple institutions simultaneously, the consequences could extend beyond individual entities to the broader financial system and the real economy. Likewise, ENISA published an initial set of recommendations to develop the operational capabilities of the various stakeholders to face these risks⁴.
3. Therefore, the supervisory dialogue with the financial entities pays particular attention to these risks and to the measures financial entities have in place to safeguard operational resilience. In particular, the ECB has emphasised to the CEOs of the significant institutions⁵ the importance of addressing, without delay, open supervisory findings and measures related to the ICT areas in focus and security risks that have been identified in previous supervisory activities such as on-site inspections, targeted reviews and the 2024 cyber-resilience stress test. Given the accelerating threat landscape, existing weaknesses that remain unresolved may become increasingly material and pose significant risks to operational resilience. Likewise, other competent authorities may set their supervisory expectations accordingly.

DIGITAL OPERATIONAL RESILIENCE ACT

DORA

ICT risk management

- Principles and requirements on ICT risk management framework

ICT 3rd party risk management

- Monitoring third-party risk providers
- Key contractual provisions

Digital operational resilience testing

- Basic testing
- Advanced testing

ICT-related incidents

- General requirements
- Reporting of major ICT-related incidents to competent authorities

Information Sharing

- Exchange of information and intelligence on cyber threats

CTPP oversight

- Oversight framework for critical ICT TPPs

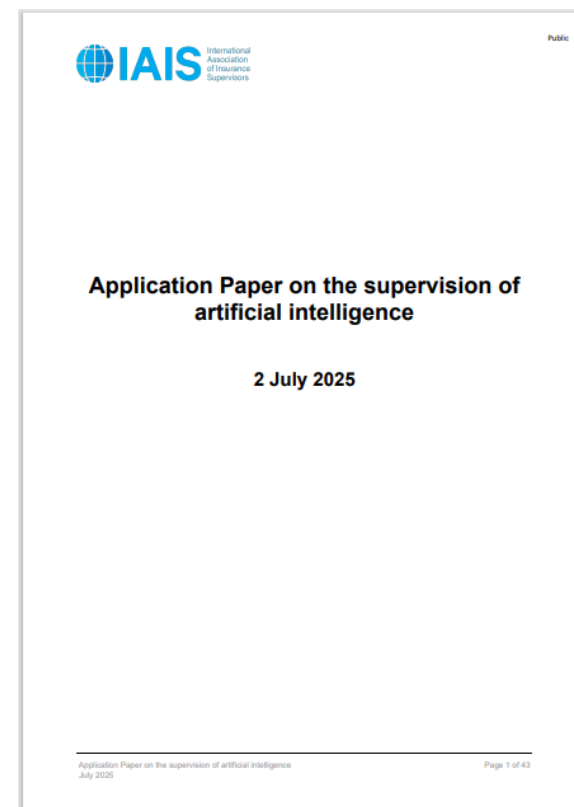
OTHER ACTIVITIES

TRAININGS AND INTERNATIONAL WORK

Training of supervisors

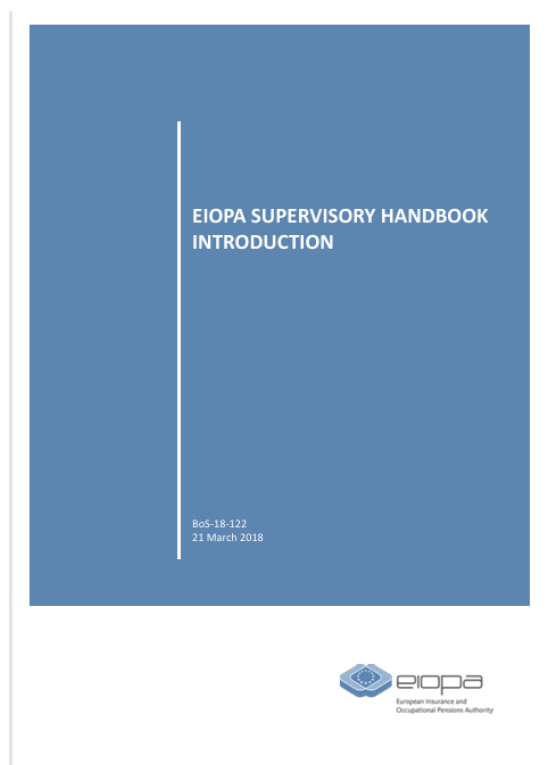


International cooperation and convergence



SUPERVISORY HANDBOOK AND COLLEGES OF SUPERVISORS

AI Supervision Chapter in the Supervisory Handbook



AI discussions in the Colleges of Supervisors



SUPTECH

Suptech





THANK YOU!

For more information visit:
<https://www.eiopa.europa.eu>