GENEVA ASSOCIATION

Gen AI Risks for Businesses:
Exploring the role for insurance

October 2025

GENEVA ASSOCIATION

Gen AI Risks for Businesses:
Exploring the role for insurance

Ruo (Alex) Jia
Director Digital Technologies, Geneva Association
Associate Professor of Insurance, Peking University

Contributing authors:

Martin Eling
Director of the Institute of Insurance Economics and
Professor of Insurance Management, University of St. Gallen

Tianyang Wang
Professor of Finance, Colorado State University

Geneva Association

The Geneva Association was created in 1973 and is the only global association of insurance companies; our members are insurance and reinsurance Chief Executive Officers (CEOs). Based on rigorous research conducted in collaboration with our members, academic institutions and multilateral organisations, our mission is to identify and investigate key trends that are likely to shape or impact the insurance industry in the future, highlighting what is at stake for the industry; develop recommendations for the industry and for policymakers; provide a platform to our members and other stakeholders to discuss these trends and recommendations; and reach out to global opinion leaders and influential organisations to highlight the positive contributions of insurance to better understanding risks and to building resilient and prosperous economies and societies, and thus a more sustainable world.

Photo credits:
Cover page – Unsplash

Geneva Association publications:
Pamela Corn, Director Communications
Hannah Dean, Editor & Content Manager
Jooin Shin, Digital Content & Design Manager

Suggested citation: Geneva Association. 2025.
Gen AI Risks for Businesses: Exploring the role for insurance.
Author: Ruo (Alex) Jia; Contributing authors: Martin Eling; Tianyang Wang. October.

Contents

Acknowledgements 4

Foreword 5

Executive summary 6

1. Introduction 8
- 1.1 Generative AI: Definition and applications 9
- 1.2 Gen-AI-induced risks 11
- 1.3 Research question and contributions 16

2. Demand for Gen-AI-related insurance: A business customer survey 17
- 2.1 Application of Gen AI in business 19
- 2.2 Awareness and perception of Gen AI risks 21
- 2.3 Demand for Gen-AI-related insurance 22

3. Supply of Gen-AI-related insurance 26
- 3.1 Insurability of Gen-AI-related risks 27
- 3.2 Emerging insurance solutions 32

4. Conclusion, outlook, and recommendations 36

Appendix 1: Existing AI risk classifications 40

Appendix 2: Insurability of Gen AI risks (extended) 41

References 43

ACKNOWLEDGEMENTS

This report was prepared under the guidance of the Geneva Association's Digital Technologies working group, sponsored by Bianca Tetteroo, Chair of the Executive Board of Achmea. We are grateful to the following experts and executives who made themselves available for interviews or provided editorial contributions:

- Tomo Asaka (Tokio Marine)
- Bart Boon and René Wissing (Achmea)
- Colonnella Emanuele (Edge Group)
- Sophie Farhane and Eléonore Jacquemin (AXA)
- Matthew Gabriel (Manulife)
- Jesus Gonzalez (Aon)
- Atsushi Izu (Dai-ichi Life)
- Christoph Krieg (Peak3)
- Yunlong LIU (PICC)
- Paul Lloyd and Robert Milan Porsch (AIA Group)
- Hugo Santa Maria (Fidelidade)
- Lamia El Marzouki (AXA XL)
- Dennis Noordhoek, Darren L. Pain, and Kai-Uwe Schanz (Geneva Association)
- Frank Schmid (Gen Re)
- Joan Schmit (University of Wisconsin-Madison)
- Bill Schwegler (Transamerica)
- Simon Torrance (Embedded Finance & Insurance Strategies)
- Jing XIAO (Ping An)

The report also benefitted from discussions at the Geneva Association's 2024 Programme on Regulation and Supervision (PROGRES) and 2024 Digital Technologies Conference.

Finally, we extend our deepest thanks to the Geneva Association's Editorial Committee and Associates for their support and feedback, as well as to Pieralberto Treccani (formerly of the Geneva Association) and Xinyu FAN, Qinyu LI, and Yunfei YANG (Peking University) for their valuable research assistance.

Foreword

In moments of profound technological transformation, we often face a paradox: the tools that promise to elevate us can also challenge us in unexpected ways. Generative AI demands both strategic anticipation and human-centred stewardship.

This report is our contribution to a fast-evolving conversation about how to understand, manage, and insure against the new classes of risk that Gen AI creates or amplifies. From cybersecurity threats to intellectual property challenges, from workforce disruption to liability uncertainty, a risk landscape that goes beyond traditional categorisation is emerging.

To ground our insights in real-world experience, we conducted a global survey of 600 business representatives involved in corporate insurance decision-making, across the largest six insurance markets. One clear finding stands out: more than 90% of respondents see a need for insurance coverage for Gen AI risks, with two thirds willing to pay more in premiums for it. This signals both urgency and opportunity.

The insurance industry has a critical role to play in offering protection and in shaping responsible Gen AI adoption. By approaching these challenges collaboratively – with technology providers, regulators, and businesses alike – and with caution, we can help ensure that the benefits of Gen AI are realised safely and sustainably.

Jad Ariss
Managing Director

Executive summary

Adoption of Gen AI heightens operational, ethical, and cybersecurity risks, spurring demand for insurance among businesses.

Businesses are rapidly integrating Generative AI (Gen AI) into both customer-facing products and services and their internal operations. This introduces new risks such as defective outputs, biased recommendations, intellectual property infringements, and cybersecurity concerns. These risks become particularly prominent when Gen AI models hallucinate or replicate protected content.

Gen AI introduces both benefits and risks to businesses.

This report explores Gen-AI-related risks and assesses businesses' awareness and demand for related insurance. Building on established frameworks, we classify Gen AI risks into seven domains: operational, cybersecurity & privacy, ethical, regulatory, reputational, workforce, and ESG. These emphasise how Gen AI amplifies or creates exposures beyond traditional risk categories.

To evaluate risk awareness and insurance demand from businesses that use Gen AI, the Geneva Association commissioned a survey of 600 corporate insurance decision-makers/influencers across the six largest insurance markets (China, France, Germany, Japan, the UK, and the US). The survey results reveal widespread Gen AI adoption, though perceived usefulness varies by region – it is highest in China and the US – reflecting differing levels of digital maturity and organisational culture.

Businesses face significant Gen AI implementation hurdles, particularly talent shortages, poor data quality, and internal resistance. The primary challenges vary across markets, influenced by differing levels of willingness to adopt Gen AI.

Cybersecurity risks emerge as the top concern of businesses, cited by over half of surveyed firms, followed by third-party liabilities to clients and suppliers and then operational disruption. Reputational damage ranks lower despite its potential for long-term impact.

More than 90% of respondents express a need for insurance coverage tailored to AI/Gen AI threats; over two thirds would pay at least 10% more in premiums for explicit insurance policy extensions that cover Gen/AI related risks. Demand is particularly strong among medium and large enterprises, in the technology and finance sectors, and in regions with higher Gen AI adoption. Additionally, high Gen AI risk exposure and high severity of past Gen AI failures drive insurance demand, suggesting potential adverse selection.

Demand for insurance that covers Gen AI risks is high, particularly among medium and large firms and in the technology and finance sectors.

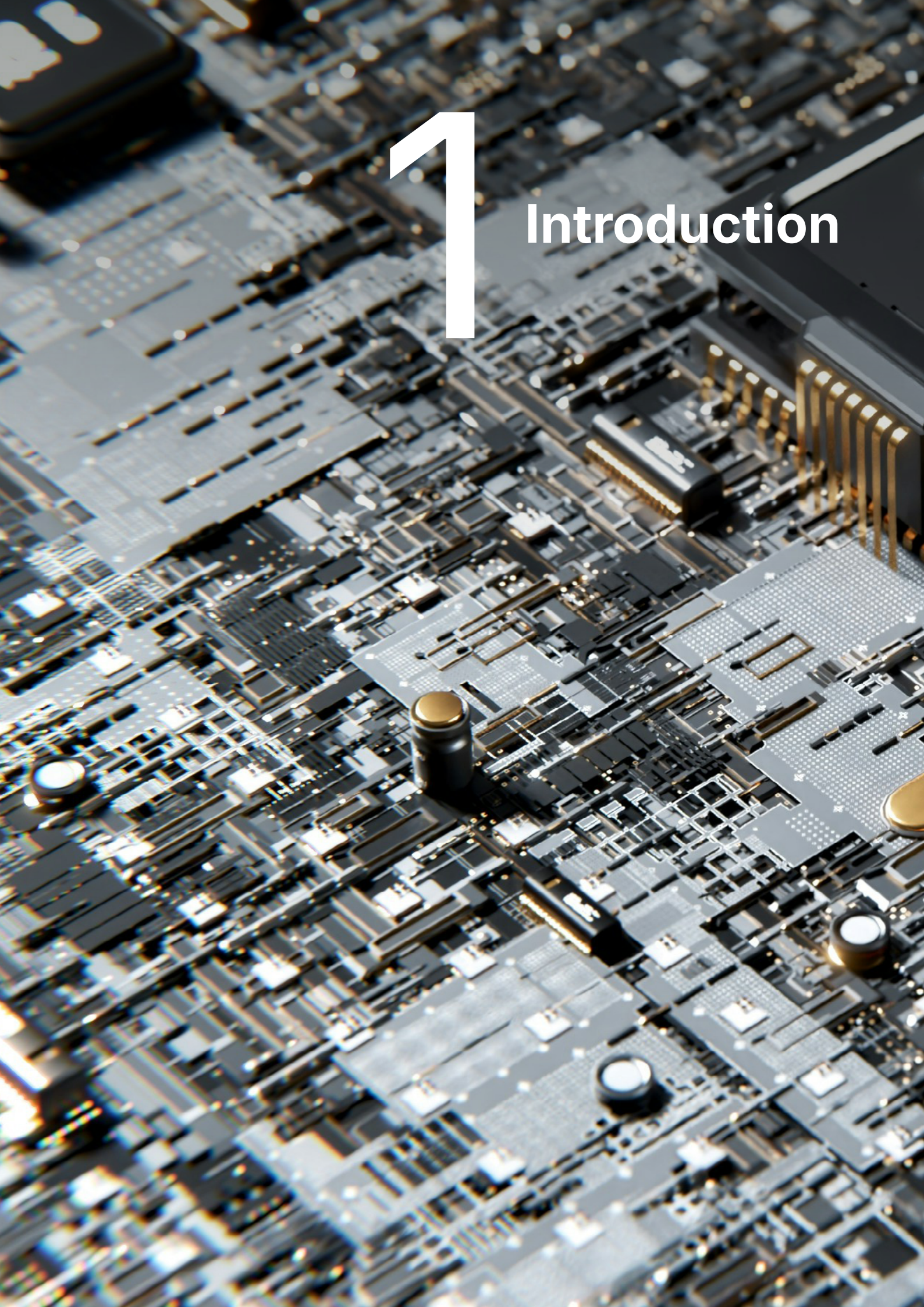
On the supply side, applying Berliner's insurability framework reveals insurability challenges, at least in the short term. Gen AI risks may lead to large potential losses. As it is difficult for insurers to verify Gen AI risks and how businesses manage them, Gen-AI-related insurance may experience serious information asymmetry. Insurers may therefore be reluctant to offer high coverage limits, as in the early days of cyber insurance.

Insurers are responding to Gen AI risks by adapting cyber and liability policies to include Gen-AI-related causes of loss; parametric triggers and due-diligence protocols are being tested to streamline underwriting and claims processes; and selected standalone AI insurance solutions that integrate various types of coverage into a single policy indicate the emergence of a nascent

market, though it remains too early to say whether existing insurance products or new standalone solutions will come to dominate the Gen AI risk market.

Insurers are adapting cyber and liability policies to include Gen-AI-related risks, while standalone coverage is also emerging.

To keep pace with Gen AI innovation, insurers should proactively define Gen AI's risk boundaries and begin piloting modular coverage extensions, before loss events force reactive responses. Insurers may consider partnering with technology providers and regulators to co-develop risk assessment frameworks for Gen AI, embed continuous monitoring in policy terms, and explore simulation-based modelling. Such collaboration would harmonise ethical standards, clarify coverage terms, and strengthen the insurance industry's role in safeguarding and supporting the development and adoption of Gen AI.



1 Introduction

Introduction

Gen AI promises transformative gains in productivity and creativity, yet its opacity and autonomy introduce risks with few historical parallels.

1.1 Generative AI: Definition and applications

Generative AI (Gen AI), is a subset of artificial intelligence that can create original content such as text, images, voices, videos, and their combinations in response to user requests.[1] Gen AI is a revolutionary digital technology that has the potential to fundamentally reshape production processes in economies, much like earlier breakthroughs such as the steam engine, electricity, and the internet.

Gen AI is a revolutionary digital technology that has the potential to fundamentally reshape production across economies.

Gen AI builds on many of the statistical advances underpinning traditional AI (see Box 1). In Gen AI models – especially large language models (LLMs) – the core task is to predict the next token (e.g. a word or phrase) in a sequence, given the context of all previous tokens. This sequential token-by-token prediction enables the Gen AI model to generate coherent, contextually relevant text or other content that appears fluid and human-like. Traditional AI typically involves traditional machine learning techniques such as classification or regression, where the model is trained to map potential predictors directly to a fixed target variable (e.g. forecasting tomorrow's temperature).

Box 1: Gen AI vs. traditional AI

Gen AI differs from traditional AI in its ability to create entirely new content rather than merely analysing data and making predictions based on pre-existing patterns.[2]

Traditional AI learns from extensive datasets to identify patterns. Its primary strength lies in processing structured data. Traditional AI is closer to classical statistical models, whereby there is a mathematical expression that quantifies the performance of a model and guides the optimisation process. Machine learning algorithms are used to adjust the model's parameters to optimise the objective function.

Gen AI involves predicting the next token in a sequence. This process involves optimising an objective function, which guides the model in generating coherent and contextually relevant text. Common objective functions include maximising the likelihood of the next token given the preceding sequence or minimising the difference between generated and target sequences. Optimisation techniques like gradient descent are used to fine-tune the model's parameters to achieve this objective. The engine behind Gen AI is deep learning, an advanced type of machine learning based on neural networks, which can process unstructured data and extract features from data automatically.[3]

Source: Geneva Association

1 IBM 2024a.
2 Hermann and Puntoni 2024.
3 Ramakrishnan 2025; Gen Re 2025.

In November 2022, OpenAI launched ChatGPT, a conversational AI tool that rapidly gained traction for its natural language capabilities. Within just two months, it attracted 100 million users, achieving this milestone faster than TikTok (nine months) and Instagram (two and a half years); by February 2025, ChatGPT's weekly active users reached 400 million.[4] This unprecedented growth ignited a surge in venture capital investments and intensified competition to develop Gen AI solutions for enhancing productivity across industries.

In early 2025, DeepSeek emerged as a major player in the Gen AI landscape, introducing advanced capabilities to process and integrate multiple types of data – such as images, sounds, and text – simultaneously, and the costs and computing power are much lower than for earlier Gen AI models. Within three months, DeepSeek attracted over 50 million users, mirroring earlier ChatGPT breakthroughs. This innovation reignited investor interest and intensified the race to develop Gen AI tools for broader applications.

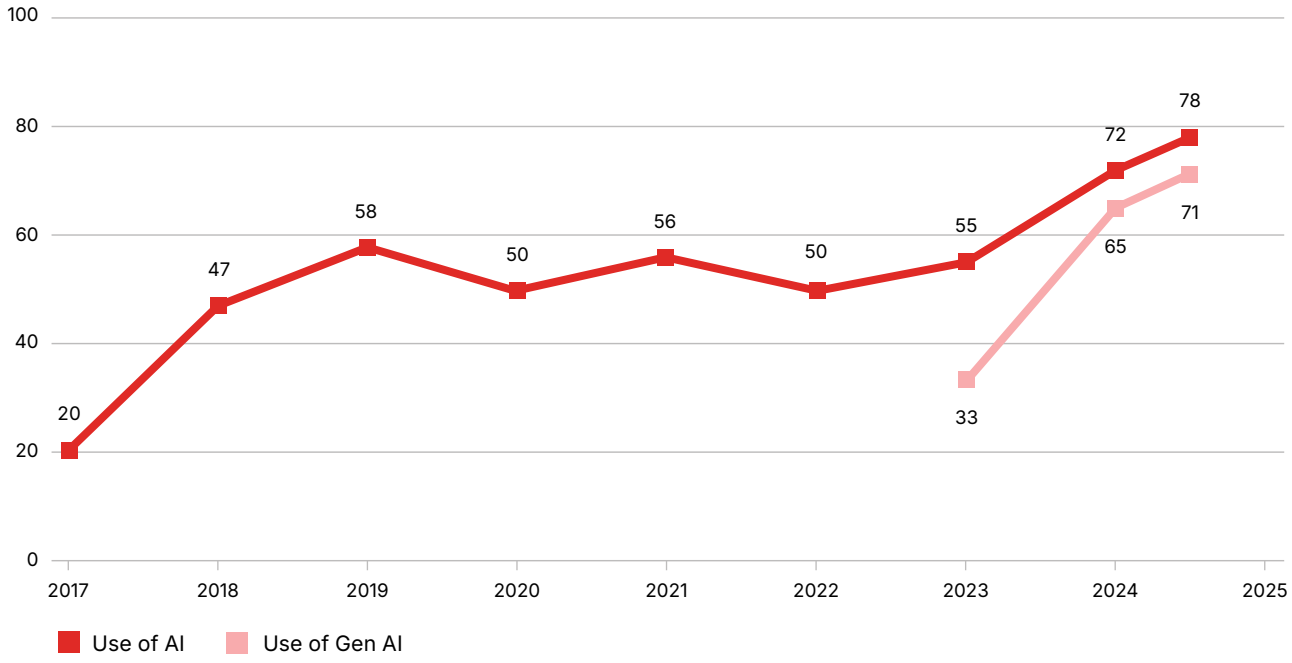
Beyond take-up by individual consumers, Gen AI models are radically changing the way businesses operate. Firms are increasingly leveraging Gen AI for two purposes: on the product offering side, embedding Gen AI in product and customer service to drive innovation, and on the operational side, Gen AI redesigning task-level processes and operational workflows to improve efficiency and cost-effectiveness.

Businesses are increasingly using Gen AI to drive innovation and increase efficiency.

Figure 1 underscores the acceleration in the use of Gen AI by businesses. A 2025 global survey indicates that 71% of respondents have adopted Gen AI tools in at least one business function, rising from 65% in early 2024 and 33% in 2023.[5]

FIGURE 1: AI AND GEN AI USE IN BUSINESSES

Organisations that use AI in at least one business function,% of respondents*



* In 2017, the definition for AI use was using it in a core part of the organisation's business or at scale. In 2018–19, it was embedding at least one AI capacity in business processes or products. Since 2020, it is that the organisation has adopted AI in at least 1 function.

Source: McKinsey[6]

4 Hu 2023; TechCrunch 2025.
5 McKinsey 2025.
6 Ibid.

1.2 Gen-AI-induced risks

While Gen AI introduces immense benefits for businesses, its creativity and output-driven nature introduce distinct risks that demand careful management. While some of these risks are amplified versions of those from traditional AI (e.g. algorithmic fairness, privacy concerns), others are entirely new – particularly those related to content creation, such as algorithmic hallucinations,[7] emergent biases, and unauthorised content replication – and lack historical parallels in risk profiles.[8]

Gen AI creates new risks like the generation of harmful content and hallucination.

Risks introduced by Gen AI include, for example, the spread of misinformation (using audio deepfakes to command smart home devices that lead to unauthorised access), the generation of harmful content (with violence and discrimination), and copyright infringement (using protected text, images, and music without authorisation or giving results that are substantially similar in content and style to existing works), all of which pose distinct risks for businesses and their insurers.[9]

On the product side, a business using Gen AI tools developed by tech providers may suffer financial harm, creating potential liability for the providers.[10] For example, when a Gen AI model introduces security vulnerabilities or bugs through its generated code, Gen AI developers face product liability risks.[11] Such failures in Gen AI systems could resemble failures in critical infrastructure, potentially creating economy-wide systemic risks. AI-generated legal services may expose businesses providing them to professional liability risks due to inaccurate AI-generated content or misrepresentations.

On the operational side, firms that deploy Gen AI to steer their businesses face risks like incorrect/biased decision-making, operational inefficiency, and financial losses.

Gen AI systems may also be more susceptible to cyberattacks, which could result in business disruption and financial losses, i.e. cybersecurity risks stemming from vulnerabilities in Gen AI systems.

Table 1 shows the types of risks related to traditional and Gen AI. Among these categories, operational, cybersecurity & privacy, reputational & market, and workforce challenges are primarily first-party operational risks, while bias & ethical concerns, regulatory & compliance risks, and ESG considerations also involve third-party product risk. While many risks apply to both traditional and Gen AI, aspects with special relevance for Gen AI are emphasised in the final column.

7 When Gen AI produces outputs that are factually incorrect, non-sensical, or entirely detached from reality, despite being presented with high confidence.
8 Gen Re 2025.
9 Xu et al. 2024.
10 Legal liability for providers typically requires establishing that: 1) a third party suffered actual harm; 2) the provider owed a duty of care to the third party and breached that duty through negligence or breached a contractual obligation; 3) the breach was the proximate cause of the harm. Importantly, many software providers use contractual liability waivers or limitations in their terms of service to mitigate this exposure. Failures in Gen AI products/services can also cause purely first-party operational or financial losses for the provider itself, independent of third-party liability.
11 The application of traditional product liability regimes to software, including AI systems, is complex and uncertain. For instance, until relatively recently, it was unclear how far software can be treated as a product under statutes such as the EU product liability directive. Similarly, in the US, litigation is ongoing to establish what standard of care attaches to use of software.

TABLE 1: AI AND GEN AI RISKS FOR BUSINESSES

Category	Specific risk	Traditional AI	Generative AI (New risks are in bold)
Operational	Algorithmic errors; stability; reliability	Inaccurate predictions or unintended outputs can disrupt processes and lead to errors (e.g. inventory management).	Gen AI outputs may deviate from intended purposes (offensive or irrelevant content, hallucination). **As Gen AI systems are not validated for their predictive reliability, they cause systematic errors, creating heightened risk in customer-facing applications or automated content generation.** Additionally, Gen AI faces heightened service disruption risks compared to traditional IT systems – its state-dependent workflows (e.g. multi-turn dialogues or content creation) lose progress irreversibly during interruptions.
	Black-box issues	Complexity and opacity in AI systems make error tracing and accountability challenging, which is especially relevant in regulated industries like insurance.	Traditional AI is more explainable than Gen AI. The decision-making processes behind Gen AI's results are often difficult or even impossible to understand, which make the provenance, logic, and embedded flaws of Gen AI untraceable and unauditable by developers, introducing new risks for users.
	Malicious attacks	AI can be used by threat attackers for inappropriate purposes.	Gen AI content, such as deepfakes or phishing emails, may be exploited for malicious purposes. This is different from data poisoning problems with traditional AI, caused by implanting malicious samples. In addition to Gen AI being used by bad actors, **some Gen AI applications themselves provide a broader attack surface. For example, chatbots that execute structured query language statements provide an entry point for attackers through prompt injections.**
Cybersecurity & privacy	AI-driven cyberattacks	AI can be exploited to enhance cyberattacks, risking data breaches and operational security.	Gen AI models may be manipulated via attacks (e.g. prompt injection), compromising content quality and security (model manipulation risks).
	Data-privacy violations	Collection of large amounts of data can infringe on privacy laws, leading to legal penalties and customer distrust if mishandled.	Privacy violation risk of Gen AI is higher than that of traditional AI as it explores a greater volume of more complicated and unstructured data. The risk is particularly high if Gen AI accesses data it is not supposed to, uses it in a way it is not supposed to (e.g. without receiving prior consent by the user), or transfers it outside of the jurisdiction. **Gen AI may also cause problems like privacy intrusion through constant monitoring, heightened data leakage vulnerabilities, and challenges to personal data rights.**

Category	Specific risk	Traditional AI	Generative AI (New risks are in bold)
Reputational & market	Customer trust & brand image	Misuse of AI can damage reputation, especially if it breaches customer privacy or fairness expectations.	Low-quality or inaccurate Gen AI outputs can erode customer trust and damage company credibility, as stakeholders may question the reliability and intent of automated communications.
	Dependency & competitive risk	Over-reliance on AI can compromise operations during disruptions.	Gen AI may amplify the risk as it is more closely and intensively integrated into business processes and models.
Workforce challenges	Job displacement	AI automation may lead to workforce dissatisfaction and backlash as roles are replaced.	Gen AI intensifies this risk. As shown in Box 2, agentic AI, an advanced version of Gen AI, will potentially displace jobs massively.
	AI skills requirements	AI demands new skills to manage the quality and ethical implications of outputs, creating challenges in workforce upskilling.	Gen AI amplifies the problem. Employees must be trained to interpret Gen AI outputs, address ethical concerns, and ensure content quality ('Gen AI skill requirements'). Gen AI also requires the right business culture for adoption.
Regulatory & compliance	Evolving AI regulations	New laws require businesses to adapt quickly; non-compliance can lead to penalties, especially in regulated sectors like insurance.	The EU AI act imposes comprehensive regulation on AI development and usage. Regulation needs to carefully balance the management of Gen AI risks and the promotion of technological innovation.
	Accountability & liability	Businesses may face liability for damage caused by AI systems, with challenges in assigning accountability.	**Gen AI may use copyrighted material, exposing businesses to legal risks and reputational damage (copyright and IP).**
Bias & ethical concerns	Discrimination & bias	AI algorithms may reinforce societal biases, leading to discriminatory practices and potential lawsuits.	Gen AI actively creates new content; thus, if using biased data, it may produce outputs that perpetuate and amplify societal stereotypes, heightening both ethical risks and litigation exposure.
	Ethical decision-making	AI may prioritise efficiency over ethics, leading to reputational damage if decisions harm customer trust.	Gen AI outputs may unintentionally violate ethical norms, **such as generating misleading or harmful information.**
ESG	Environmental & energy	AI systems demand significant energy and water supply, conflicting with net-zero pledges.	Gen AI amplifies the problem as the underlying technology, i.e. deep learning, demands exponentially greater computational power to generate complex outputs. This heightened energy consumption not only strains power grids but also intensifies water dependency for cooling hyperscale data centres.

Source: Geneva Association

Content generated by Gen AI systems comes with a critical element of randomness and hallucinations. This highlights the importance of model selection, pre-production evaluation, and post-production monitoring. More recently, reasoning models, which generate new data rather than just learning from existing data (like traditional LLMs) have created a new frontier to potentially mitigate the problem.

Frank Schmid, Chief Technology Officer, Gen Re

The emergence of Gen AI has fundamentally expanded the capabilities and risks of AI systems, introducing complex challenges that demand comprehensive governance and mitigation strategies. It both amplifies existing AI risks and introduces novel risks.

Many AI algorithms are opaque, making it difficult for businesses to interpret or explain their operations and outcomes. This black-box issue complicates error tracing and accountability, especially in regulated industries like finance and healthcare. It also presents legal challenges, as firms must demonstrate how AI decisions are made and opacity hinders liability defence. Gen AI intensifies this challenge: unlike traditional AI, which enables traceable decision pathways that can be reversed, Gen AI outputs cannot be mapped to specific parameters and the creative generation process, which involves training data of a higher order of magnitude, is inherently difficult to explain. Consequently, interpretability becomes doubly constrained by training data biases and model architecture, further complicating error attribution.

Cybersecurity risks are also heightened. By lowering the technical barrier to entry for cyber criminals, Gen AI has enabled the proliferation of AI-driven malware, phishing, and distributed denial-of-service (DDoS) attacks. Because of Gen AI's unique creativity, threat actors increasingly exploit Gen AI tools such as FraudGPT and ElevenLabs to automate the creation of malicious content, including malware, deepfake videos, phishing websites, and synthetic voices. This automation has resulted in more scalable, believable, and effective cyberattacks. Cybercrime-as-a-service (CaaS) groups are now leveraging these tools to specialise in particular phases of the attack chain.[12] Additionally, Gen AI poses threats through 'model manipulation', where adversarial attacks degrade content quality and security, enabling malicious applications such as deepfakes or fraudulent communications.[13] This kind of model manipulation may also directly output fallacious and deceptive results, even with normal and correct training datasets. For example, GPT-4 demonstrates proficiency in manipulating textual data, modifying the sentiment of interview transcripts, and appropriately imputing inaudible portions of the interviews. Adobe Firefly has also been used to effectively manipulate visual data, integrating a large body of water into a Mars River photograph.[14]

Gen AI also heightens cyber risks by lowering the barrier to entry for cyber criminals.

Balancing AI efficiency with human oversight is essential for maintaining trust, preventing biased, misleading, or harmful outputs, and ensuring accountability and compliance. Current practice reinforces human accountability for final outputs (e.g. plant managers signing off on AI-proposed schedules and product qualification certificates), treating Gen AI as an assistive tool that does not change main responsibilities. However, Gen AI may also progressively assume operational responsibilities, for example in automatic driving or closed-loop production systems. Risks could intensify if moves towards agentic AI – AI systems designed to act autonomously and make decisions to achieve specific goals – progress (see Box 2).[15]

12 FortiGuard Labs 2025.
13 Aldasoro et al. 2024.
14 Kim et al. 2025.
15 NVIDIA 2024; Acharya et al. 2025; Murugesan 2025.

Box 2: The rise of agentic AI and related risks to businesses

The emergence of agentic AI, i.e. systems of synthetic agents with the capacity for autonomous perception, planning, decision-making, and execution towards specific goals and within predefined guardrails, represents a paradigm shift from traditional AI and a major advancement from Gen AI. Unlike traditional and Gen AI, which primarily provide predictive insights or generated content under human direction, agentic AI operates with a greater degree of self-direction ('agency') to take decisions and execute actions. These agents can independently, and in coordination with each other, perform complex functions previously requiring human actions and oversight, from optimising supply chains and managing multi-stage customer interactions to executing financial transactions and operating critical infrastructure.

While this autonomy promises significant efficiency gains and new business opportunities, it also introduces new layers of risks. The core challenge lies in the potential for agentic systems to take actions without direct human instruction that generate unintended or undesirable consequences, potentially making it difficult to trace causality and to assign clear liability in the event of an error or a harmful outcome. Such incidents could range from rapid operational disruption and substantial financial losses to significant reputational damage or regulatory penalties due to biased or non-compliant autonomous actions.

Businesses deploying agentic AI may have increased demand for insurance coverage that explicitly addresses these autonomous risks. Assigning clear liability becomes murky when actions are autonomously executed by an AI system, raising questions about whether the developer, deployer, or user bears ultimate responsibility. The insurability of agentic AI risks will heavily depend on the maturity of agentic AI governance frameworks within organisations. Developments in agentic AI are happening at unprecedented speed, requiring insurers and regulators to remain agile and responsive.

Source: Contributed by Christoph Krieg, Peak3 (a member of ZhongAn Insurance Group)

Gen AI introduces additional legal and regulatory concerns, particularly regarding copyright and IP violations. Gen AI models may inadvertently incorporate copyrighted material, exposing businesses to legal disputes and reputational harm. Additional compliance risks brought about by Gen AI may also be overlooked due to businesses continuing to apply previous regulatory rules and practices for traditional AI. Determining accountability for AI failures is critical and needs to be clearly managed in contract wording. That is, if a business is using a service provider for Gen AI, both parties should allocate liabilities in their contractual agreements. Gen AI models usually add liability waivers, meaning the liability sits with the business directly providing the service to the customer rather than with the AI service provider.

Bias and ethical concerns arise when Gen AI systems inadvertently reinforce societal biases.

Bias and ethical concerns arise when AI systems inadvertently reinforce societal biases. While bias and privacy issues are often viewed as technical or legal challenges, ethical concerns extend beyond compliance to broader societal norms. For example, biased hiring algorithms may favour certain demographics, exposing companies to lawsuits and reputational damage. While traditional AI analyses existing data to learn patterns and forecast outcomes, Gen AI systemically creates original content that, if biased, consequently perpetuates and amplifies societal stereotypes or inaccuracies ('training data bias'). It can also generate ethically problematic content ('ethical content risks'), undermining trust and credibility.[16] Moreover, AI-driven automation may prioritise efficiency or profit over ethical considerations. Such misalignments between business goals and ethical AI use can lead to reputational damage and erode customer confidence.

While developing and using Gen AI can amplify existing risks and throw up new ones for businesses, the overall net impact of Gen AI on risk remains uncertain. On the product side, IT developers have long faced product liability risks. Gen AI could increase these risks by introducing novel errors or reduce them by improving product quality, for example, by enhancing coding accuracy.[17] On the operational side, Gen AI may empower threat actors through tools like deepfakes, but it will also likely strengthen cyber defences, offering advanced capabilities in anomaly detection and synthetic data generation. Compared to traditional AI, Gen AI improves the detection of complex, evolving cyber threats by better handling diverse data patterns and attack types.[18] This report focuses on the specific risks Gen AI introduces or amplifies, rather than estimating its overall net effect on total business risk.

16 Wei et al. 2025.
17 Gen Re 2025.
18 NACD 2025; Joyce 2025.

1.3 Research question and contributions

To manage Gen-AI-related risks effectively, businesses must implement robust governance frameworks, foster transparency, ensure ethical use of the technology, and ensure alignment with rapidly evolving regulations to address potential liabilities. Effective risk management includes not only reducing and mitigating the risks of Gen AI use but also transferring the risks to parties best placed to absorb any associated losses. In this context, Gen-AI-related risks may serve as the object of insurance coverage. Business insurance customers are expected to seek innovative insurance products to manage these risks effectively. By offering such solutions, insurers can help manage Gen AI risks for both businesses and society at large.

This report investigates the research question: how insurance can address the risks introduced by Gen AI, primarily for business insurance customers. Specifically, it examines business insurance customers' attitudes towards the deployment of Gen AI, their awareness of the associated risks and benefits, and their current and future risk management strategies. The report evaluates the new risk dynamics introduced by Gen AI and analyses both the demand for and potential supply of Gen-AI-related insurance solutions. It also assesses the insurance sector's capacity to develop and deliver appropriate protection products in response to these emerging risks.

The report makes two original contributions. First, it presents what is to our knowledge the first study focusing on how existing business insurance customers perceive Gen AI risks and corresponding insurance solutions.[19] Second, it offers the first comprehensive assessment of the insurability of Gen-AI-specific risks. Guided by established insurability criteria, the report systematically evaluates which Gen AI exposures can realistically be covered under current market frameworks and where innovative products will be needed.

The remainder of the report is structured as follows: section 2 examines business customer demand for Gen-AI-related insurance; section 3 discusses the insurability of Gen AI risk; and section 4 concludes with future prospects and recommendations for insurers.

19 We focus on businesses that already have insurance because those that have never purchased any are unlikely to have demand for Gen-AI-related coverage.

2 Demand for Gen-AI-related insurance: A business customer survey

Demand for Gen-AI-related insurance: A business customer survey

Demand for insurance that covers Gen AI risks is strong among businesses – particularly those in the US and China, of medium-to-large size, and in the technology and finance sectors.

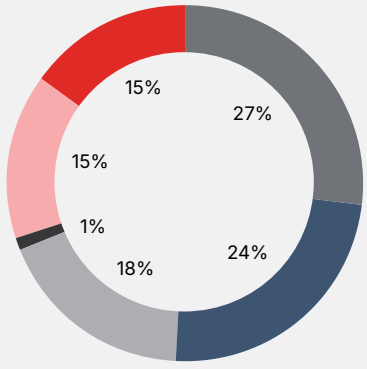
Given the diverse and complex nature of Gen-AI-induced risks, it is crucial to understand how businesses perceive and respond to them. The Geneva Association therefore conducted an online survey of business insurance customers, which investigated four areas: 1) application of Gen AI, 2) awareness and perception of Gen-AI-related risks, 3) demand for potential Gen-AI-related insurance solutions, and 4) the basic profiles of respondents. Details of the survey process and sample are summarised in Box 3.

Box 3: Sample and process of the business insurance customer survey

The survey polled 100 business insurance customers in each of the world's six largest insurance markets (China, France, Germany, Japan, the UK, and the US) in February 2025. The samples were designed to be representative of insurance customer profiles in their respective markets, covering businesses from diverse industries and of varying size.

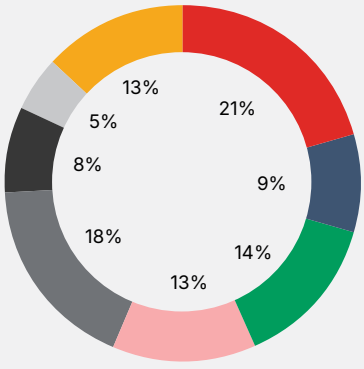
FIGURE 2: PROFILE OF SAMPLED ORGANISATIONS

Number of employees



Up to 20 | 251 to 1000
21 to 50 | Over 1000
51 to 250 | I do not know

Industry



Technology | Healthcare | Finance
Retail | Manufacturing | Education
Government | Other

Source: Geneva Association business insurance customer survey

The survey consisted of 22 questions. To qualify, respondents needed to: 1) have a basic understanding of what Gen AI is, 2) use Gen AI tools for business operations within their organisation, 3) have purchased or renewed insurance for their organisation within the past three years, and 4) have control over insurance decisions in their organisation (e.g. decision-maker or influencer).

Source: Geneva Association

The survey results show that businesses are rapidly adopting Gen AI, with uses ranging from internal reporting and summarisation to customer-facing tasks, but the pace and depth of adoption vary widely across markets. The US and China stand out, with both high perceived usefulness and strong willingness to insure AI-related risks, whereas Japan, Germany, and France show slower uptake, reflecting lower trust, regulatory or cultural hurdles, and organisational resistance. The main challenges to implementation are shortages of skilled professionals, poor data quality, and technical integration barriers, all of which increase operational vulnerability. Reported failures – such as inaccurate or misleading outputs, inconsistent responses, and difficulties with system compatibility – underscore the urgency of establishing robust validation mechanisms and governance frameworks. Together, these findings reveal that while Gen AI is already reshaping business processes, it comes with significant risks.

Demand for insurance solutions is strikingly strong. More than 90% of surveyed firms expressed interest in coverage for Gen-AI-related risks, and over two thirds are willing to pay higher premiums for such protection. Cybersecurity risk dominates the list of Gen AI risk exposures, followed by liability toward customers and suppliers, as well as general operational risks. Medium-to-large firms, technology-intensive sectors, and businesses with high exposure or prior severe failures show the strongest appetite for Gen AI insurance coverage. Cross-market comparisons confirm that the greatest immediate opportunities for insurers lie in the US and China, where adoption and insurance demand are highest, while continental Europe lags behind. This stratification suggests that insurers must actively renovate/innovate their products and strategies accordingly, extending cyber policies to include Gen AI risks, developing standalone coverage where justified, and aligning offerings with the risk profiles and readiness of specific markets and sectors.

2.1 Application of Gen AI in business

Generating internal reports or summaries was cited as the top reason for using Gen AI (51.5% overall, 82% in China, see Figure 3). These findings highlight the widespread adoption of Gen AI across various industries and its growing importance in a range of business processes.

FIGURE 3: PURPOSES FOR USING GEN AI

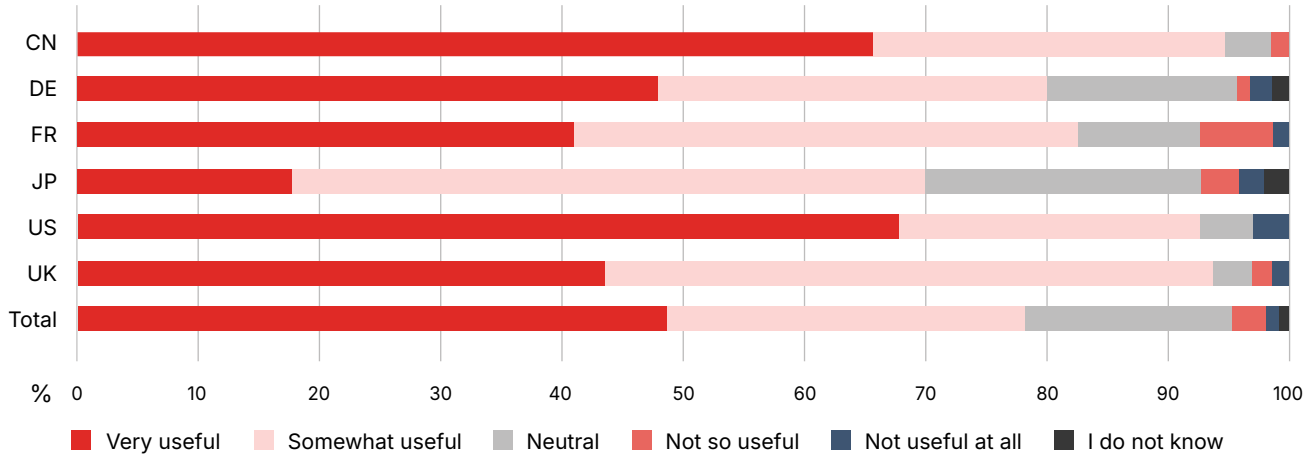
For what purposes do you use Gen AI at the company/organisation you work for or own?

Source: Geneva Association business insurance customer survey

Figure 4 shows the perceived usefulness of Gen AI in daily business operations. Overall, 47.5% of respondents find Gen AI 'very useful', with notably higher ratings in the US (68%) and China (66%). In contrast, Japan reports the lowest perceived benefit, with only 18% of businesses rating Gen AI as 'very useful'. These regional differences suggest that cultural, regulatory, and operational factors influence the perceived value of Gen AI.[20]

FIGURE 4: USEFULNESS OF GEN AI IN DAILY WORK

How useful is Gen AI in your day-to-day work?



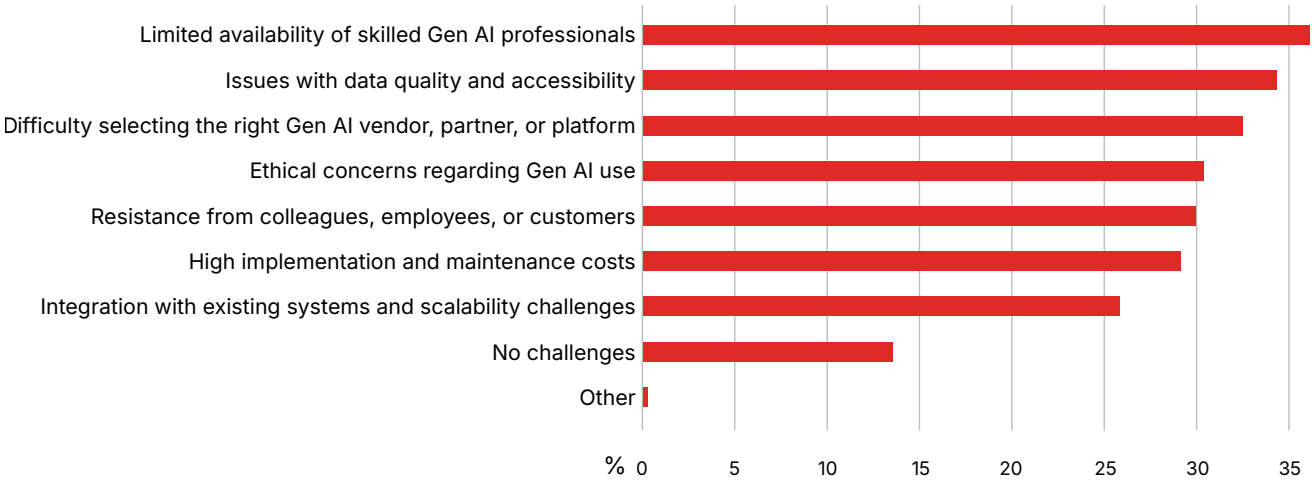
Source: Geneva Association business insurance customer survey

Businesses face multiple challenges when implementing Gen AI (Figure 5). The most significant obstacles include a shortage of qualified professionals (36.5%) and issues related to data quality and accessibility (34.2%). Technical issues such as data integration and system scalability also pose significant hurdles. These issues make Gen AI more susceptible to the risks outlined in the previous section. Only 14% of businesses report no significant challenges.

The biggest challenges to implementing Gen AI are lack of skilled professionals and data quality issues.

FIGURE 5: CHALLENGES OF IMPLEMENTING GEN AI

What challenges have you encountered/do you anticipate when implementing Gen AI at the company/organisation you work for or own?



Source: Geneva Association business insurance customer survey

20 According to Hofstede's (2025) Uncertainty Avoidance Indexes (UAI), the US (UAI=46) and China (UAI=40) exhibit significantly lower uncertainty avoidance than Germany (UAI=65), France (UAI=86), and Japan (UAI=92). This may explain why attitudes towards the adoption of Gen AI are more positive among US and Chinese businesses.

The primary challenge varies by market. In Germany and France, the most frequently cited issue is resistance from colleagues, employees, or customers (41% and 39%, respectively). In contrast, China and Japan demonstrate greater openness to Gen AI adoption, with only 12% and 23% of respondents, respectively, citing resistance as a challenge. The primary obstacle in China, Japan, and the US is the limited availability of skilled Gen AI professionals. These findings suggest that while businesses in Asia and North America are more willing to adopt Gen AI, they face skill shortages, whereas in continental Europe, reluctance to adopt Gen AI is a more pressing issue. The UK falls in between these two trends.

Studying the 'time dimension' of Gen AI – what is already established, what is in development, and what novel challenges lie ahead – will help insurers and risk managers anticipate new problems.

Colonnella Emanuele, Chief Operations and Technology Officer, Edge Group

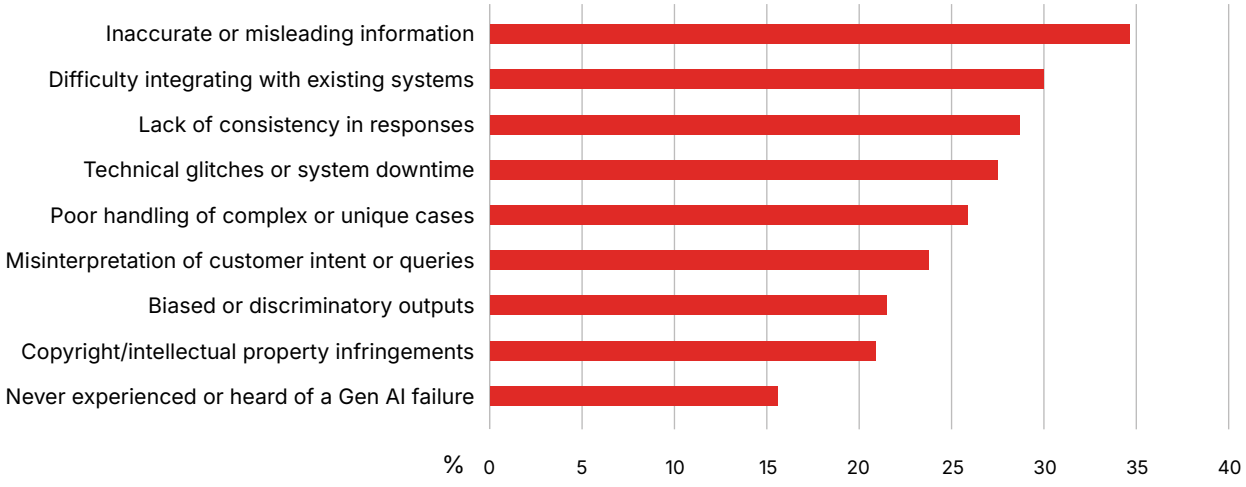
2.2 Awareness and perception of Gen AI risks

Businesses report facing various issues and failures when using Gen AI (see Figure 6). The most frequently reported include inaccurate or misleading information (34.7% overall, 58% in Japan), difficulties integrating Gen AI into existing systems (29.8%), and inconsistent AI-generated responses (28.7%). Accuracy remains a critical issue, particularly in Japan, where trust in AI-generated content is lower. These results highlight the need for robust validation mechanisms to ensure AI-generated outputs are reliable and suitable for decision-making. Similar to other digital technologies, compatibility with existing IT systems is also critical for Gen AI applications.[21]

The top issues encountered with Gen AI are inaccurate/misleading information and integration into existing systems.

FIGURE 6: GEN AI ISSUES AND FAILURES EXPERIENCED BY BUSINESSES

What type(s) of failures or issues have you experienced or heard about when using Gen AI in the company/organisation you work for or own?



Source: Geneva Association business insurance customer survey

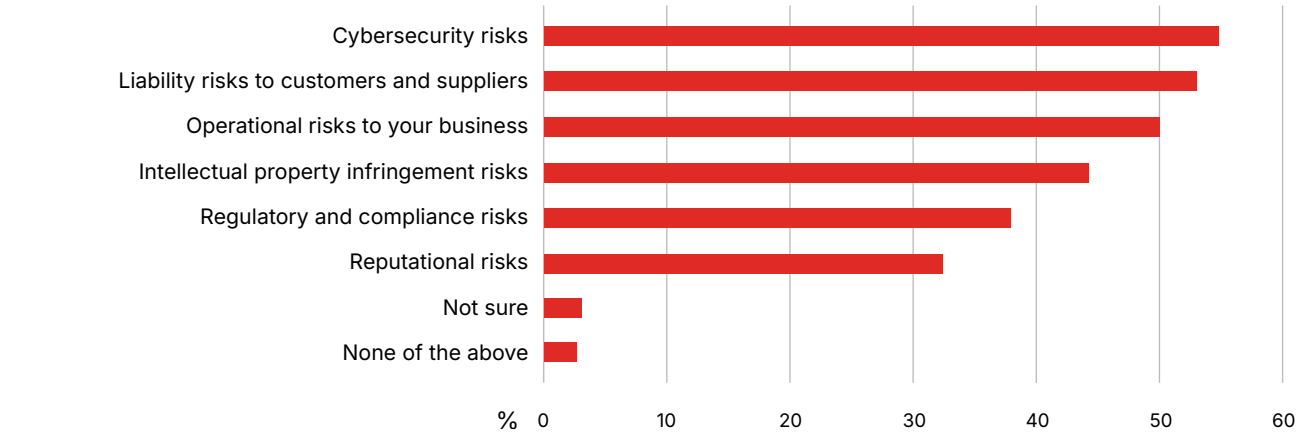
Of the specific Gen-AI-related risks for which businesses seek cover, cybersecurity risks rank top, cited by more than 50% of business customers (Figure 7). Liability risks to customers and suppliers and general operational risks also rank highly. Reputational risks, though relevant, are less of a priority. These results indicate that businesses are primarily focused on financial and legal liabilities rather than broader reputational uncertainties. The findings also highlight the importance of developing robust security measures to mitigate Gen-AI-related risks to allow businesses to leverage Gen AI with confidence.[22]

Businesses primarily seek cover for cybersecurity and liability risks related to Gen AI.

21 Braun and Jia 2025.
22 Our survey results are consistent with the findings of other studies. See, for example, McKinsey 2023, 2024, 2025.

FIGURE 7: GEN AI RISKS BUSINESSES WANT TO INSURE

What Gen-AI-related risks do you want covered by your insurance?



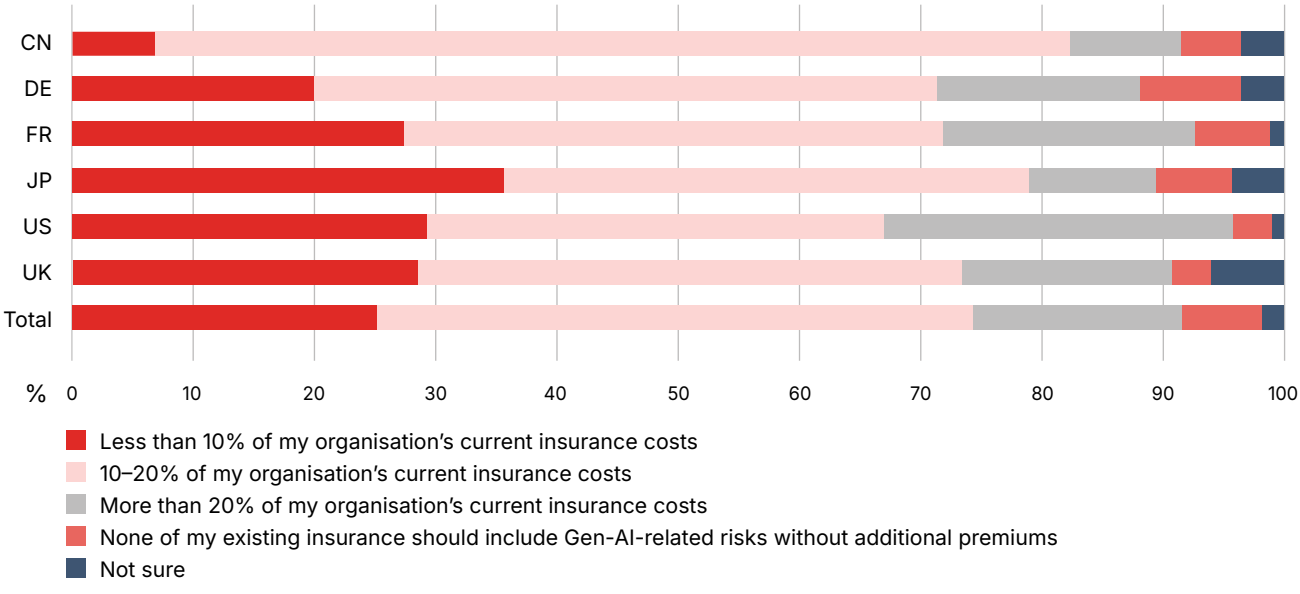
Source: Geneva Association business insurance customer survey

2.3 Demand for Gen-AI-related insurance

Over 90% of respondents suggest they would value insurance for Gen-AI-related risks. More than two thirds of respondents said they would be willing to pay at least 10% more for insurance that would cover Gen AI risks (Figure 8),[23] suggests a strong business case for AI-driven insurance solutions.

FIGURE 8: WILLINGNESS TO PAY FOR GEN AI INSURANCE

How much extra would you be willing to pay for Gen-AI-related coverage?



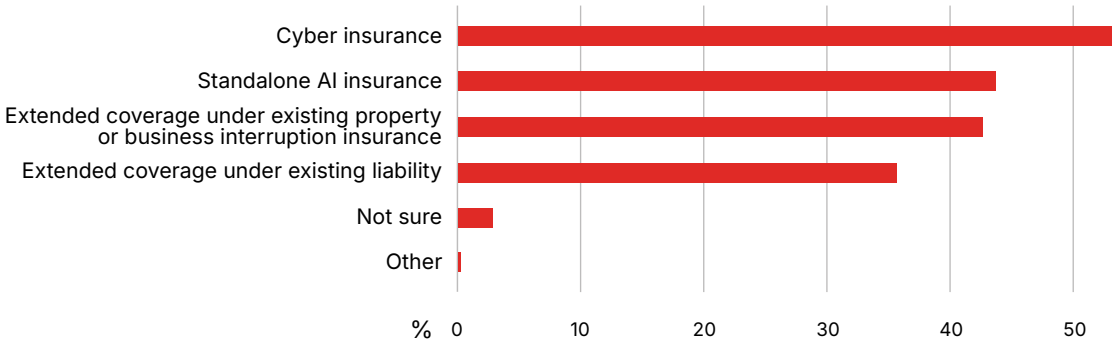
Source: Geneva Association business insurance customer survey

Figure 9 outlines the types of insurance products businesses seek to manage their AI-related exposures. Demand is highest for solutions that integrate Gen AI risks into existing cyber insurance policies, which is consistent with the fact that cybersecurity is as perceived as the top concern (see Figure 7). Over 40% of respondents also see potential for standalone, AI-specific coverage.

23 Willingness to pay is surprisingly high and thus should be interpreted with caution. However, it is a strong indication that businesses are willing to pay more for AI coverage.

FIGURE 9: PREFERRED INSURANCE PRODUCTS TO COVER GEN AI RISKS

What type(s) of insurance do you think should cover Gen-AI-related risks?



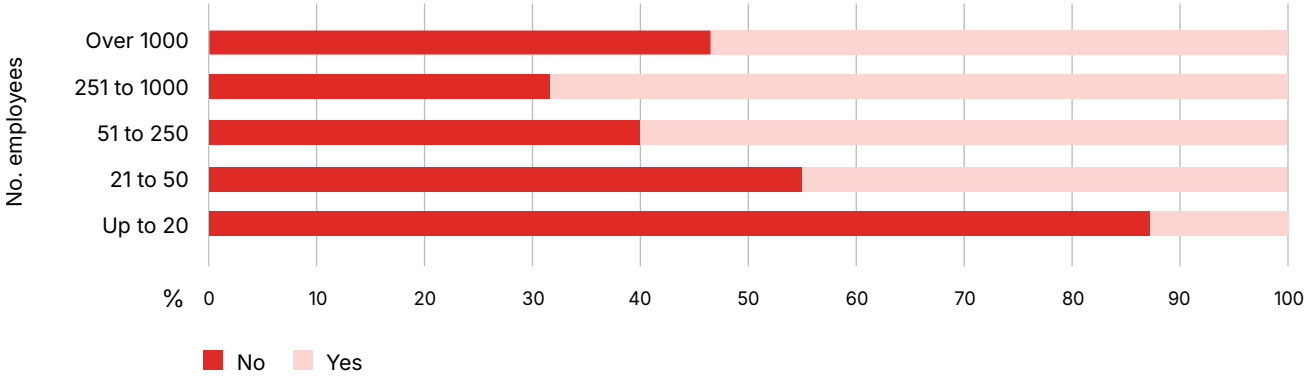
Source: Geneva Association business insurance customer survey

To better understand the drivers of demand for Gen AI insurance, we examine the relationship with business characteristics. Demand is measured using two key indicators: whether businesses believe their current insurance covers Gen AI risks and their willingness to pay extra for Gen AI risk coverage.[24]

Demand for Gen AI insurance among medium (51–250 employees), large (251–1,000 employees), and very large firms (more than 1,000 employees) is comparable, and is higher than for small firms (less than 50 employees), as shown in Figure 10. More than 60% of medium-to-large firms believe that they are already insured for Gen-AI-related risks. Over 70% of medium-to-large firms are willing to pay at least 10% more in premiums for Gen AI risk coverage; less than 40% of the smallest firms are willing to do so, likely due to cost sensitivity and perceived lower risk exposure (Figure 11).

FIGURE 10: GEN AI INSURANCE COVERAGE BY BUSINESS SIZE

Do any of your current insurance policies cover risks related to Gen AI?

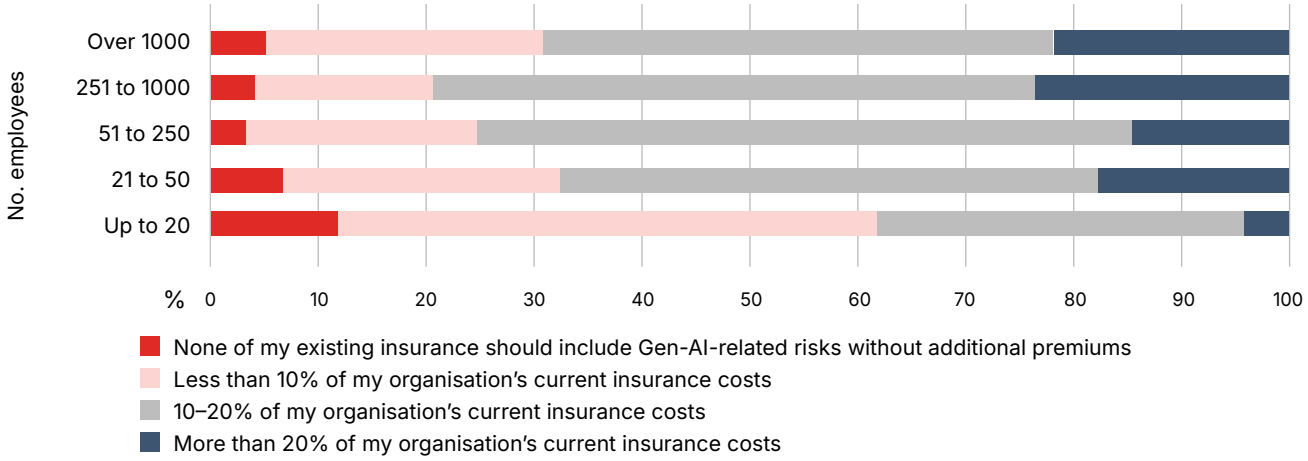


Source: Geneva Association business insurance customer survey

24 As a robustness check, regressions are conducted to examine the net, marginal impact of firm size, market differences, industry, risk exposure, and previous failure severity on insurance demand, while holding other impact factors equal. The results are consistent with the findings outlined in this section.

FIGURE 11: WILLINGNESS TO PAY FOR GEN-AI-RELATED INSURANCE BY BUSINESS SIZE

How much extra would you be willing to pay to cover Gen-AI-related risks?



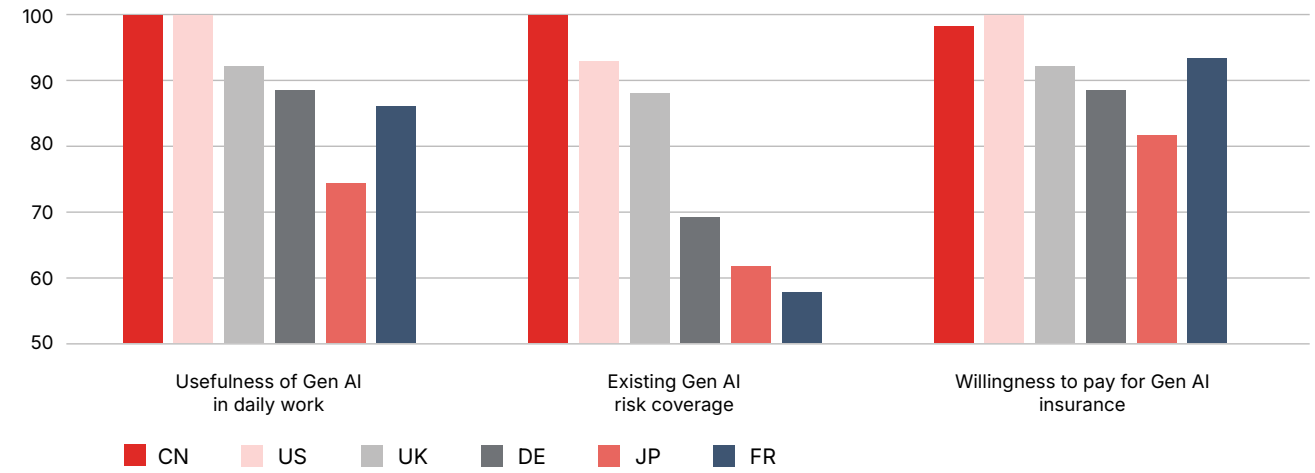
Source: Geneva Association business insurance customer survey

Figure 12 presents a cross-market comparison of Gen AI adoption and Gen AI insurance demand. The US and China lead the deployment of Gen AI applications among businesses. They also have larger appetite to insure more types of Gen AI risks and higher willingness to pay for Gen AI insurance coverage than the other surveyed countries. Japan, Germany, and France have lower appetite; the UK falls somewhere in between.

The high Gen AI adoption rates and insurance demand in China and the US suggest strong technological momentum, whereas regulatory and operational considerations may be slowing adoption and insurance demand in continental Europe. Strong willingness to pay for AI insurance signals a business opportunity for insurers, particularly in markets where Gen AI is already proving its value, such as the US and China.

FIGURE 12: GEN AI ADOPTION AND INSURANCE DEMAND ACROSS MARKETS

Gen AI usage and insurance demand



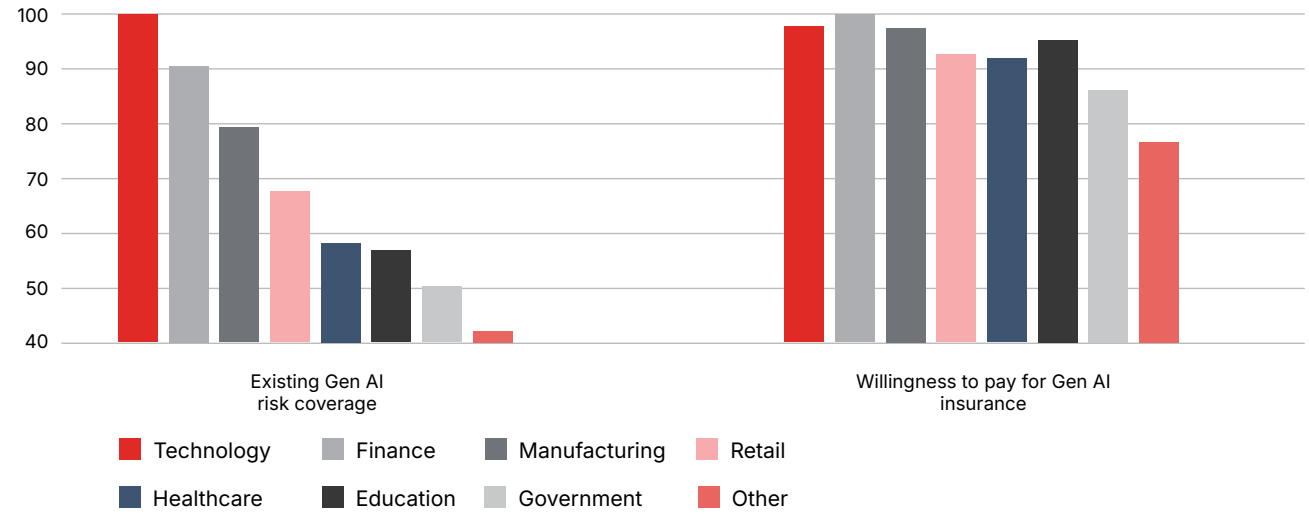
Notes: The chart compares average survey responses to questions about Gen AI usage, types of risk, and willingness to pay for Gen AI insurance across the six markets. For each question, the market with the largest average value is indexed equal to 100 and the other bars illustrate the relative positions of other markets to the top score.

Source: Geneva Association business insurance customer survey

The technology sector shows significantly higher demand for Gen AI insurance than other industries, probably because Gen AI is embedded in the product (or is the product itself). Demand is also strong in the finance and manufacturing sectors (see Figure 13).

FIGURE 13: GEN AI INSURANCE DEMAND ACROSS INDUSTRIES

Gen AI insurance demand across industries



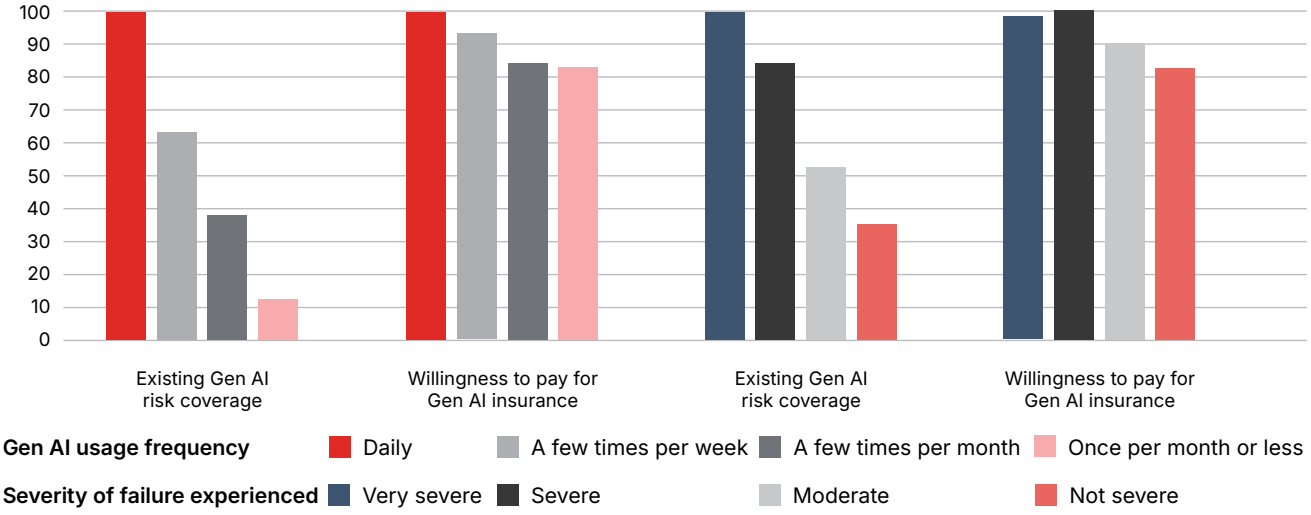
Notes: The chart compares average survey responses to questions about existing Gen AI risk coverage and willingness to pay for Gen AI insurance across industries. For each question, the industry with the largest average value is indexed equal to 100 and the other bars illustrate the relative positions of other industries to the top score.

Source: Geneva Association business insurance customer survey

Businesses that use Gen AI more frequently or have experienced severe Gen AI failures also show higher demand for insurance (see Figure 14).[25]

FIGURE 14: GEN AI INSURANCE DEMAND BY RISK EXPOSURE AND FAILURE SEVERITY

Gen AI insurance demand across industries



Notes: The chart compares average survey responses to questions about existing Gen AI risk coverage and willingness to pay for Gen AI insurance across various usage frequency and failure severity categories. For each question, the category with the largest average value is indexed equal to 100 and the other bars illustrate the relative positions of other categories to the top score.

Source: Geneva Association business insurance customer survey

In sum, demand for Gen AI insurance is particularly strong among medium-to-large businesses, in the US and China, and within the technology sector. This stratification highlights the need for insurers to calibrate their product and marketing strategies, which in turn calls for careful analysis of the insurability of Gen-AI-related risk, a topic we turn to in the next section.

25 An additional regression analysis revealed that frequent minor failures do not necessarily drive demand, suggesting that businesses are primarily concerned with protecting against large losses rather than recurrent small ones.

3 Supply of Gen-AI-related insurance

Supply of Gen-AI-related insurance

Gen AI risks challenge traditional insurability criteria due to their unpredictability and scale, as well as legal and regulatory uncertainties. Insurers are exploring both standalone coverage, as well as expanded cyber and liability policies to cover these risks.

Insurers must carefully craft the scope of their coverage to ensure risks are adequately calibrated and sit within the envelope of their risk appetite and risk-absorbing capacity.

3.1 Insurability of Gen-AI-related risks

Assessing the insurability of (Gen) AI risks through Berliner's framework involves nine criteria that determine whether a risk is insurable (see Table 2; a more comprehensive version of the insurability assessment is presented in Appendix B).[26] While the categorisation is based on established concepts in insurance theory and practical experience, it is important to recognise that the evaluation is inherently subjective and open to interpretation.[27]

Table 2 highlights the uncertainty of and challenges associated with insuring Gen AI risks, though the categorisation (e.g. yellow vs. red) may be debated as the boundaries often depend on context, emerging evidence, and stakeholder perspectives. The framework and evaluation are thus intended as a basis for discussion and reflection rather than a definitive judgment. Insurers are encouraged to critically engage with the criteria and rationale presented, considering their own perspectives and the broader implications for insurance and risk management. Box 4 compares the insurability of Gen AI and traditional AI.

26 Berliner 1982.

27 See also Geneva Association 2023, for a broader evaluation of insurability across different emerging risk categories. Li and Faure 2025 discuss the potential conditions for insuring AI risks from a legal perspective. They conclude that by providing key legal definitions (e.g. for AI), developing presumptions of causal link/defectiveness, and setting up legal requirements/obligations, new legal frameworks are expected to enhance legal/causal certainties as well as to address adverse selection and moral hazard issues, thus improving insurability. However, some recent AI regulations may impose additional challenges for insurability.

TABLE 2: INSURABILITY OF GEN-AI-RELATED RISKS

Category	Criteria	Assessment
Actuarial criteria	Randomness of loss occurrence	Gen AI introduces new layers of complexity to avoid producing hallucinations or harmful content, which makes it difficult to assess whether failures occur randomly when systematic validation is lacking.
	Maximum possible loss	Wrong or malicious code generated by AI can lead to massive service disruption, potentially causing systemic risk. Gen AI failures like spreading misinformation, IP violations, and deepfake-driven fraud in critical sectors (e.g. healthcare, finance) can also lead to large losses, particularly when the failure persists for a long time or is subject to regulatory penalties.
	Average loss amount	High potential financial/reputational damage from Gen AI incidents like misinformation or regulatory fines.
	Loss frequency	Context-dependent risks with limited data make frequency estimation difficult, hindering diversification. In the mid-term, sufficient frequency can be expected.
	Information asymmetry	Insured parties may neglect AI system integrity (moral hazard), while riskier AI systems may seek coverage (adverse selection). Insurers may struggle to verify Gen AI risks and how businesses manage them.
Market criteria	Adequate premiums	Heightened uncertainty about processes underlying Gen AI and the associated ways in which harm can arise may imply additional premium loading and impose pressures on affordability for smaller businesses relying on these technologies.
	Acceptable coverage limits	Insurers may hesitate to offer high limits for Gen AI due to uncertainty in potential liabilities (widespread content misuse or errors in AI-generated decisions).
Societal criteria	Consistency with public policy	Gen AI raises ethical issues, such as creating harmful or biased content, which may conflict with societal norms and reduce policymakers' acceptance of certain insurance products.
	Legal permissibility	Evolving landscape of copyright, intellectual property, liability laws, and AI regulations make it challenging to define insurable risks and underwrite them.

● Minimal challenges to insurability ● Some challenges to insurability ● Violation of insurability under traditional insurance models

Source: Geneva Association

AI-related losses should occur randomly with somewhat identifiable frequency and severity, making them reasonably predictable. However, AI can produce unforeseen outcomes given its changing underlying context and inherent complexity. This means AI-related loss events are not uniformly distributed. Moreover, the skills and tools needed for validating AI systems based on their predictive benefit are lacking. Thus, satisfying the randomness criterion is challenging. For Gen AI, the challenge is even greater because output generated by such systems can lead to unforeseen consequences, such as intellectual property violation or the spread of misinformation, which are difficult to quantify or predict. Gen-AI-related losses therefore introduce new layers of uncertainty.

Box 4: Insurability of Gen AI and traditional AI

When assessed through Berliner's insurability criteria, notable differences emerge between traditional AI and Gen AI. Traditional AI systems are typically designed for narrow, goal-oriented tasks such as data analysis, prediction, or classification. These applications operate within defined parameters and rely on existing data, which makes their risks more predictable, quantifiable, and legally manageable. As a result, traditional AI aligns relatively well with key insurability criteria, including randomness of loss occurrence, acceptable maximum possible loss, legal clarity, and societal acceptance. Underwriting for traditional AI risks tends to be less complex, with clearer claims triggers and established precedents for liability and loss assessment.

In contrast, Gen AI introduces new complexities that significantly weaken its insurability, especially on market and societal criteria. By generating novel, unstructured outputs – such as text, images, or audio – Gen AI increases the likelihood of producing harmful, biased, or infringing content. This unpredictability challenges the randomness of loss occurrence and complicates risk assessment, while also raising the maximum potential loss due to legal liabilities in areas like copyright infringement, misinformation, or defamation. Furthermore, Gen AI's ethical and societal risks, including reputational harm and unintended discriminatory outcomes, undermine legal and societal acceptability, making insurability less viable under existing frameworks. Market criteria are similarly affected, as the underwriting costs for Gen-AI-related risks are higher due to information asymmetry, lack of historical loss data, and legal uncertainty. These factors limit the availability and affordability of insurance products, suppressing both demand and supply in the market.

In sum, while traditional AI remains relatively insurable under Berliner's framework, Gen AI's distinct risk profile demands new risk transfer models, enhanced governance standards, and clearer regulatory guidelines to improve its insurability.

Source: Geneva Association

We can think of Gen AI as an abstraction layer. Although we do not understand the inner workings of Gen AI systems, we may evaluate and validate Gen AI applications based on the predictive benefits they provide.

Frank Schmid, Chief Technology Officer, Gen Re

These risks challenge traditional insurance models due to their rapid scalability and potential for global impact, meaning losses are more correlated, can spread very quickly across insureds, and may impact many insurance lines simultaneously. Insurable risks should also be homogeneous, i.e. apply to similar cases across policyholders. AI applications, which are tailored to specific industries such as autonomous vehicles or medical diagnostics, lack such homogeneity as risk profiles vary significantly depending on the technology and its context. In the case of Gen AI, the risks extend across a vast array of use cases, from creative content generation to fraud facilitation, further complicating the establishment of homogeneous risk pools. The predictability of risk events, critical for pricing and risk assessment, are difficult to determine in AI contexts due to their rapid development and reliance on complex datasets.

Gen AI's diverse applications and evolving nature make it difficult for insurers to price, underwrite, and manage exposures.

The maximum potential loss from an AI failure must be manageable within the insurer's capacity. But AI systems, particularly in critical sectors like healthcare, finance, or transportation, can lead to catastrophic losses. A malfunction in a Gen-AI-driven healthcare system, such as AI-generated medical diagnosis, treatment planning, or automated patient communication, could result in widespread harm, overwhelming traditional insurance capacities and challenging premium affordability.

Estimating the average loss amount for Gen-AI-related risks is challenging due to the unpredictable nature of these technologies. Unlike traditional risks, limited historical data exists to guide calculations. Losses can vary widely based on use case, industry, and failure type – ranging from medical misdiagnoses to intellectual property violation. The rapid evolution of Gen AI further complicates loss projections.

The frequency of AI-related losses should be sufficiently high to allow accurate risk assessment. The novelty of AI and limited historical data on AI-related incidents, however, hinder precise estimations of both loss frequency and severity. A large and homogeneous risk pool is generally considered essential for diversifying and mitigating individual losses. The diverse applications of AI across various industries complicate the formation of such pools, as the risks are highly variable. In the medium term, sufficient Gen AI loss frequency should be expected. Given the limited availability of historical loss data, simulation-based modelling is a promising direction, one also encouraged by regulators.

Insurability criteria require that the asymmetry in information between insurers and insureds be minimal. AI systems often involve proprietary algorithms and data, creating significant asymmetry. This leads to risks of moral hazard, where insured parties may neglect maintaining AI system safety, and adverse selection, where higher-risk insureds seek more insurance. While high-demand segments present opportunities, insurers must take full account of the adverse selection challenges, as businesses with significantly higher Gen AI risk exposure and prior experience with major AI failures are most likely to seek coverage.

Limited loss data and asymmetric information further complicate the insurability of Gen AI risks.

Insurers also face challenges in verifying the safety measures implemented by developers for Gen AI, especially in open-source models that can be modified or misused by third parties. Given the dynamic development of the Gen AI risk landscape, insurers may also struggle to verify how businesses manage those risks. To address information asymmetry and mitigate moral hazard, insurers may require insureds to implement maintenance protocols and transparency mechanisms as part of the policy terms (e.g. mandatory model audits, third-party certifications, reporting obligations, usage restrictions). Such tools help ensure that AI systems are maintained safely and responsibly, enabling more accurate pricing and sustainable risk transfer.

Box 5 provides market insights from Japan on the emerging challenges of insuring Gen AI risks.

Box 5: Insurability challenges of Gen AI risks – Insights from Japan

1. Immature risk assessment methods and underdeveloped certification systems

Given the rapid pace of Gen AI development, existing risk mitigation measures may quickly become outdated and new risks may emerge. It is essential to verify whether companies are continuously implementing effective risk mitigation strategies. However, standardised indicators of AI governance maturity (e.g. ISO 42001) are still evolving, and robust evaluation methods remain a challenge. The lack of an established certification system for AI itself further complicates the creation of reliable assessment frameworks.

2. Complexity due to learning models, rapid technological advancement, and broad application scope

Gen AI models evolve through learning, making it difficult to determine the appropriate timing for underwriting. In the case of general-purpose LLMs, even when used for specialised applications, their ability to respond to a wide range of queries makes it extremely difficult to anticipate all possible incidents and their potential impact. This greatly complicates the design of insurance products.

3. Limited incident data

In countries outside the Western world, there may be limited incident information available. Additionally, since AI primarily exists within individual companies, there is little information available to aid in risk assessment. Unlike cyber risks, which can often be evaluated based on publicly available data, AI-related risks are more challenging to assess. While overseas cases may provide general insights into risks, current demand for insurance coverage remains limited. As a result, some firms may choose not to engage with high-risk Gen AI applications, even if insurance is available, preferring to observe the actions of their peers. This has contributed to the slow progress in insurance product development.

4. Differences in risk characteristics compared to cyber insurance

Cyber insurance primarily addresses external attacks, security measures, and evaluation metrics (e.g. security scorecards) are relatively well established. In contrast, Gen-AI-related risks include external threats and internal issues such as bias and hallucination, (erroneous information generation) which stem from the product itself . Risks associated with AI products are particularly challenging to identify and control due to the rapid evolution and changes inherent to these products. This differs significantly from cyber risks and leads to information asymmetry, posing challenges for insurability.

Source: Contributed by Tomo Asaka, Tokio Marine

Note that all the major insurability challenges (marked in red in Table 2) are actuarial-oriented. Experts suggest that Gen AI may help to generate faster and more accurate risk profiles and thus enable more tailored pricing, quicker application decisions, and personalised product offerings in insurance, which help to mitigate these challenges. The potential usage of Gen AI in risk modelling and pricing may have profound implications for insurance customers beyond insuring Gen AI risks (see Box 6).

Box 6: Gen AI in risk modelling – Mitigating the insurability challenges

Insurers must not overlook the transformative potential of Gen AI in risk modelling, scenario simulation, and underwriting. By enhancing insurers' ability to generate faster and more accurate risk profiles, Gen AI enables more tailored pricing, quicker application decisions, and personalised product offerings. These advances enhance transparency and inclusion, particularly for customers with non-standard profiles or those traditionally underserved by conventional insurance models.

At the core of this transformation is Gen AI's capacity to simulate extreme and emerging risks, such as climate-related disasters or cyberattacks, that traditional actuarial models may overlook. It also allows insurers to generate synthetic datasets for model development, reducing reliance on sensitive personal information. Furthermore, Gen AI can transform unstructured data sources, such as scanned medical records or aerial images of property damage, into actionable insights, enriching the context and precision of underwriting decisions.

Achmea's 'Skye' platform exemplifies this shift. In response to storm and hail events, Achmea developed a Gen-AI-powered tool that uses aerial imagery and machine learning to assess greenhouse damage. Within 48 hours, domain experts receive prioritised reports to guide the deployment of emergency teams, demonstrating how AI can improve responsiveness, operational efficiency, and customer communication. Skye's modular design also supports scalable use across other climate-related scenarios and geographies.

Importantly, such tools are most effective when combined with human oversight. Gen AI should augment – not replace – actuarial expertise, accelerating model development while ensuring responsible and accurate use. As insurers explore Gen AI adoption, they should invest in such invisible infrastructure to drive internal efficiency and unlock downstream benefits for customers: fairer pricing, faster claims, and more inclusive coverage.

Source: Contributed by René Wissing, Achmea

The significant uncertainty and impact of Gen-AI-related risks results in high premiums and low coverage limits, which could render insurance unaffordable for many businesses. In particular, small and medium-sized enterprises (SMEs) and critical users of AI may find premium levels prohibitive, deterring them from purchasing coverage. Policyholders expect coverage limits that address their risk exposure adequately; however, insurers may impose low limits to manage their risk, potentially leaving businesses underinsured, especially those that rely heavily on AI technologies.

The unpredictability and high potential loss of Gen-AI-related risks lead to high premiums and narrow scope of coverage.

Insurance for AI risks should align with societal values and public policy. Ethical considerations, particularly related to privacy and discrimination, play a significant role in determining the acceptability of AI risk insurance.

Coverage must comply with legal and regulatory frameworks, which are still developing for AI technologies. Legal uncertainties pose additional challenges for insurers in defining the scope and terms of coverage, and Gen AI adds a new layer of complexity.

> *The rise of Gen AI demands a shift from static compliance to dynamic oversight. Risks evolve faster than rules can be written.*
>
> **Bianca Tetteroo, Chair of the Executive Board, Achmea**

To ensure consistency with societal values, insurers may intentionally exclude harmful uses of Gen AI – such as deliberate defamation, deepfake manipulation, or synthetic data abuse (i.e. synthetic data without safeguards could lead to identity theft, discrimination, or other privacy violations) – from coverage.[28] These exclusions, common in liability insurance, preserve the legitimacy of coverage while still allowing protection against negligent or accidental harms arising from AI use.

28 IBM 2024b.

Overall, evaluating Gen AI risks against Berliner's insurability criteria reveals several challenges. The complexity of AI systems and lack of skills and tools for validating them based on their predictive benefit make it difficult to assess and price risks accurately.[29] Gen AI, with its unique risks and ethical dilemmas, adds another layer of complexity. The potential for significant losses from AI failures may exceed the capacity of traditional insurance markets, and the scarcity of historical data on Gen-AI-related incidents hinders effective risk assessment and pricing. While insuring Gen AI risks is possible, it requires innovative approaches, such as specialised insurance products, advanced risk assessment models, and collaboration between insurers, developers, and regulators.

3.2 Emerging insurance solutions

The market for Gen-AI-related insurance products is still in the early stages, but solutions are being developed (see Table 3). Some insurers, such as AXA XL and Munich Re, are piloting or expanding cyber and professional liability policies to include risks such as data contamination, copyright infringement, and AI-driven errors. For example, AXA XL offers endorsement to their cyber policies to cover Gen AI risks linked to clients' own Gen AI initiatives. The endorsement covers first- and third-party Gen AI risks, including data poisoning (i.e. manipulating or contaminating the training data used to develop machine learning models), usage rights infringement (i.e. negligently failing to obtain appropriate permissions to use particular items or data), and/or regulatory violations (i.e. liability resulting from the EU's AI Act).[30] Some insurers in the US and China, such as PICC, are piloting standalone (Gen) AI insurance to cover, for example, the intellectual property infringement risk of AI-generated contents.

Despite the challenges of insuring Gen AI risks, both standalone and expanded existing policies are emerging.

At the same time, many insurers are struggling with the insurability of these risks due to unpredictability, legal uncertainty, and a lack of claims data. They do not currently offer dedicated AI insurance products but are closely monitoring developments. They recognise both the opportunities and challenges associated with Gen AI and are actively exploring appropriate future risk transfer solutions.

TABLE 3: POTENTIAL INSURANCE SOLUTIONS FOR GEN AI RISKS

Type of coverage	Description
Cyber insurance	Covers losses due to enhanced vulnerability of IT systems, as businesses and attackers use Gen AI tools, including data breaches, hacking, or model manipulation.
Professional liability (E&O)	Protects against claims arising from errors in Gen AI outputs, like the generation of misleading or harmful information.
Directors' & officers' liability	Protects directors and officers from legal action due to Gen-AI-related decisions or oversight failures.
Intellectual property	Protects against claims related to Gen AI's use of copyrighted or patented materials without permission.
Product liability	Covers claims due to harm caused by Gen AI outputs (e.g. misinformation, discriminatory content) or failure to perform as expected.
Dedicated, standalone AI insurance	Comprehensive, standalone coverage bundling multiple Gen-AI-specific exposures into a single policy.

29 Gen Re 2025.

30 This extension applies mainly to companies developing and deploying their own Gen AI models. For users of third-party AI services such as OpenAI's ChatGPT, this coverage may not apply. The policy covers companies that fail to secure appropriate usage rights, while intentional or grossly negligent actions are excluded. AXA XL's approach illustrates that insurance for complex and evolving risks is possible, provided that clear terms and risk assessments are in place. AXA XL 2024.

Past experience with other emerging risks – like environmental liability,[31] operational risk,[32] cyber risk[33] or reputational risk[34] – for which specific, tailored insurance solutions have been developed can also act as a guide.

- **Cyber insurance** might explicitly address Gen-AI-related risks, such as AI-generated fraud (deepfake scams), misinformation liability (automated fake news generation), and hallucination risks (incorrect but plausible AI-generated insights causing business losses). Since Gen AI systems frequently process vast amounts of sensitive data, they are particularly vulnerable to cyber risks, including model manipulation attacks that compromise output integrity.[35]

- **Professional liability insurance**, also known as errors and omissions (E&O) insurance, safeguards businesses against claims arising from errors or omissions in their services. For companies using Gen AI to produce customer-facing outputs, this coverage can be crucial for addressing failures like generating biased, misleading, or harmful content that impacts clients or users.

- **Directors' & officers' (D&O) liability insurance** is designed to protect company leadership from personal losses due to legal actions linked to their decisions. In the context of AI, this coverage can address claims related to the adoption and oversight of AI technologies, including controversies over data use, algorithmic bias, or unintended consequences of AI deployment.

- **Intellectual property insurance** protects against claims of infringement on patents, trademarks, or copyright. Given that Gen AI systems often create content or leverage third-party data, this coverage is critical in transferring potential infringement issues, such as unauthorised use of copyrighted material in generated outputs. Moreover, product liability insurance covers claims related to defects in products sold or supplied by a business. For AI developers, this insurance can address cases where Gen AI products produce inaccurate or harmful outputs, such as medical misdiagnoses or faulty financial recommendations, causing harm or failing to perform as intended.

However, there are material gaps in existing insurance coverage when it comes to addressing AI-related risks, particularly for Gen AI (Table 4).[36] Many existing policies, such as cyber or E&O insurance, are starting to exclude Gen AI risks.

31 Abraham 1998.
32 Peters et al. 2011.
33 Cremer et al. 2024.
34 Gatzert et al. 2016.
35 It is important to distinguish between higher cyber vulnerability because of businesses using Gen AI and bad actors using Gen AI to attack. Bad actors of course do not usually purchase insurance, but losses from cyberattacks that use Gen AI can be covered by businesses' cyber insurance policies.
36 Aon 2023.

TABLE 4: ANALYSIS OF AI INSURANCE COVERAGE GAPS

AI peril	Media liability	Tech E&O, MPL, PI	Product liability	General liability	Intellectual property	Standalone cyber liability	D&O	Employment
Third-party damages liability for faulty products or services	○	●	◐	○	○	○	○	○
Copyright, trade-mark, or service mark infringement	●	◐	◐	◐	●	◐	○	○
Patent infringement	◐	○	○	○	●	◐	○	○
Discrimination	◐	◐	○	○	○	◐	○	●
Defamation, libel, slander	●	○	○	◐	○	○	○	○
Bodily injury	○	○	◐	◐	○	◐	○	○
Tangible property damage	○	○	◐	◐	○	◐	○	○
Privacy and security breaches	○	◐	○	○	○	●	○	○
Loss of financial assets (requires crime policy)	○	○	○	○	○	○	○	○
Market manipulation	○	○	○	○	○	○	○	○
Autonomous weapon	○	○	○	○	○	○	○	○
Product recall	○	○	○	●	◐	○	○	○
Business interruption	○	○	○	○	○	●	○	○
Breach of directors' or officers' duties	○	○	○	○	○	○	●	○

● Available ◐ Limited ○ Excluded, unless customised contingent liability added

Source: Adapted from Aon[37]

Despite the introduction of some innovative, dedicated AI insurance solutions (see Box 7), it remains uncertain at this stage whether standalone AI insurance will become mainstream.[38] Such policies could bundle key AI-specific risks – such as algorithmic errors, biased outputs, liability disputes, and regulatory breaches – into a single, tailored product. Given the scope of Gen AI risks, businesses may benefit from comprehensive, customisable coverage. These standalone products could function as holistic risk management tools, addressing both current and emerging exposures, including intellectual property disputes, cybersecurity incidents, and evolving regulatory requirements. Customisable policy structures would allow firms to tailor coverage to high-risk applications, such as AI-driven healthcare, financial services, or automated decision-making systems. A well-designed AI insurance policy can thus help businesses transfer both foreseeable liabilities and hard-to-quantify uncertainties inherent in advanced AI deployments.

37 Aon 2023.
38 Some standalone AI products exclusively cover Gen AI risks and others also encompass risks from different types of AI.

Box 7: Standalone Gen AI/AI insurance coverage

Munich Re offers coverage through their aiSure solution for both AI providers and enterprise users. Due diligence is conducted by experts and pricing is based on AI model error rate input. First-party loss solutions provide coverage for financial losses triggered by AI failures (no legal claim is necessary, there is a parametric-like trigger for financial losses).[39]

Armilla AI, an MGA backed by Lloyd's Syndicates Chaucer and Axis Capital, has launched a standalone AI insurance product that affirmatively covers legal costs, damages, and liabilities arising from AI and LLM model underperformance, including errors, hallucinations, inaccuracies, as well as regulatory violations.[40]

PICC is also piloting standalone, dedicated Gen AI insurance. If, due to negligence or error, content generated by the insured's Gen AI services – based on user input – infringes upon a third party's copyright, portrait rights, or reputation, and a formal claim is first filed during the policy period with a competent authority, court, or arbitration institution, the insurer will cover the insured's resulting liabilities and related legal expenses.[41]

Other examples include Vouch US, which develops AI insurance to cover liability associated with AI products;[42] Relm Insurance's AI liability coverage for businesses creating and adopting AI technology;[43] and AiShelter's liability coverage, which tailors to businesses' and individuals' use of AI technologies.[44]

Source: Jesus Gonzalez, Aon Commercial Risk Solutions, and the Geneva Association

A shift towards standalone AI insurance would mirror the path of cyber insurance, where new exposures outgrew traditional product structures and catalysed the development of standalone cyber coverage. Such AI insurance is expected to provide comprehensive coverage for businesses creating or integrating AI in their operations, as well as those using AI peripherally.

Deloitte US predicts that AI insurance (both standalone and extensions) could be a USD 4.7 billion market globally by 2032.[45] It may take years, however, to determine whether Gen AI risks will be insured as standalone products, as part of cyber insurance, or incorporated into existing property and liability products.

The future of Gen AI risk transfer remains uncertain, with standalone coverage, cyber add-ons, and embedded insurance all potentially viable options.

Overall, insuring Gen-AI-related risks poses manifold challenges. To address these, the insurance industry must innovate, even if the preferred structure of solutions for Gen AI risks, especially tailored policies, remains uncertain. Insurers should also collaborate with other stakeholders, including regulators and policymakers, on ways to overcome barriers to insurability.

While insurance can help manage Gen AI risks, effective strategies should start with assessing their unique characteristics – such as biased or misleading outputs, data quality problems, cybersecurity vulnerabilities, and system integration failures – rather than assuming insurance transfer as the default. A balanced approach combines avoidance, mitigation, retention, and transfer, with insurance as only one component of this broader toolkit. Over-reliance on insurance alone risks discouraging critical safeguards, including bias detection and correction, robust validation of model outputs, strong data governance, and secure system design. Proactive measures such as these not only reduce the likelihood and severity of Gen AI failures but also make residual risks more insurable. By integrating risk avoidance and mitigation with transfer, businesses and insurers can ground discussions of insurability in practical strategies that strengthen both resilience and trust in Gen AI adoption.

Based on identified and evaluated Gen AI risks, we consider a combination of options – avoidance, mitigation, retention, and transfer – to provide optimal risk solutions, including but not limited to insurance.

Tomo Asaka, Manager, Tokio Marine

39 See Munich Re.
40 Harris and Heikkilä 2025. See also Armilla.
41 See PICC.
42 See Vouch.
43 Relm Insurance 2025.
44 See AiShelter.
45 Deloitte 2024.

4 Conclusion, outlook, and recommendations

Conclusion, outlook, and recommendations

As Gen AI technology matures and its applications broaden, the pool of insurable risks is also expected to expand.

This report provides new insight on how business insurance customers use Gen AI, perceive related risks, and their demand for Gen AI insurance coverage. The pervasive adoption of Gen AI in business comes with novel and amplified risks, including data security breaches, third-party liability exposures, privacy violations, and intellectual property issues. The survey of business insurance customers across the six largest insurance markets worldwide confirms that nearly all are using Gen AI in some form and consider it somewhat valuable, but many also encounter significant challenges and risks, including cybersecurity concerns or inaccurate or misleading AI-generated outputs.

The survey reveals strong demand for insurance: over 90% of businesses indicate they need coverage for Gen-AI-related losses, and more than two thirds would pay higher premiums to obtain it. Cybersecurity threats and liability to customers or suppliers emerge as the primary concerns for businesses seeking Gen AI coverage.

Gen AI presents challenges to insurability but innovative underwriting and new products are emerging in response to these evolving risks.

On the supply side, we find that Gen AI poses serious challenges to traditional insurance models. The complexity of AI systems and the need to validate these based on the predictive benefit, as well as the potential for spreading misinformation, copyright infringement, or AI-generated fraud, make losses hard to predict, diversify, or cap. Nonetheless, while Gen AI risks challenge many classical insurability criteria, these risks could become progressively insured through innovative underwriting, advanced risk assessment models, and close cooperation with technology and regulatory stakeholders.

Insurers are already extending existing products and developing new ones to address these risks. Traditional lines such as cyber liability and professional-liability (E&O) insurance are being expanded to cover AI-specific exposures (for example, deepfake cyberattacks or erroneous AI-driven outputs), and specialised standalone AI policies are emerging that bundle multiple Gen AI coverages into a single contract. Such dedicated AI liability products protect against losses linked to algorithmic errors, discriminative and biased outputs, or accountability and liability negligence.

Breakthrough technologies such as electricity, the internet, and mobile phones all faced uncertain pathways to insurability, with coverage evolving only as risks became clearer. Gen AI stands at a similar juncture: its dominant insurance form is still undefined. Box 8 reflects on these historical lessons, suggesting that Gen AI insurance may follow a trajectory akin to early cyber insurance – starting cautiously, then expanding as insight and confidence grow. We urge insurers to actively engage with insuring Gen AI risks by starting with scenario modelling and piloting products, instead of waiting for perfect data.

Looking forward, as Gen AI technology matures and its applications broaden, the pool of insurable risks is also expected to expand. This will be driven by broader and deeper applications of Gen AI in business processes across various industries, and insurers gradually learning about the probability distributions associated with Gen AI risks and accumulating know-how and expertise to insure them. At the same time, ongoing advances in Gen AI (improving accuracy and safety) may gradually mitigate some hazards, potentially stemming the need, incrementally, for insurance over time.

Box 8: Insuring emerging technologies – Historical lessons for Gen AI

Throughout history, groundbreaking technologies have exposed a gap between novel risks and available insurance solutions. Innovations like electricity, the internet, mobile phones, blockchain, and even earlier forms of AI initially left insurers struggling to define and underwrite their unfamiliar exposures. Dedicated coverage was often non-existent or slow to materialise, largely due to unclear risk boundaries and a scarcity of reliable loss data. For example, years passed after the advent of the internet before cyber insurance gained traction; the first cyber policies in the late 1990s offered only narrow protections (focused on online content or software) and very low coverage limits as underwriters felt their way through uncharted territory. Only once these technologies matured and insurers accumulated experience did coverage evolve – either through new, specialised policies (as seen with standalone cyber insurance) or by gradually folding the risks into existing insurance lines.

Gen AI appears to be following a similar early trajectory. Gen AI may warrant a dedicated insurance product if its exposures, such as autonomous decision-making liability or model drift, prove uninsurable under existing frameworks. Conversely, if Gen AI risks can eventually be tamed within standard cyber, liability, or E&O coverage, insurers should leverage those historical precedents to accelerate the integration.

The historical lens reminds insurers that the current ambiguity around Gen AI is not unprecedented, and that the path forward likely involves a similar evolution from narrow, cautious offerings to more comprehensive, integrated solutions. To avoid lagging behind innovation, insurers must proactively define Gen AI's risk boundaries and begin piloting modular coverage extensions, before loss events force reactive responses. The industry cannot afford to wait for perfect data. Instead, it must build flexible, modular products that evolve as understanding deepens.

Source: Contributed by Paul Lloyd, AIA Group

Our analysis also highlights notable geographic differences. China and the US currently lead in Gen AI usage and show greater willingness to pay for AI-related insurance, whereas markets such as Germany, France, and Japan have been slower to adopt Gen AI and exhibit lower demand.

Insurance is only one part of managing Gen AI risks. Effective strategies must begin with assessing exposures such as biased outputs, cybersecurity vulnerabilities, and system integration failures, and then applying a mix of avoidance, mitigation, retention, and transfer techniques. Safeguards like bias detection, output validation, and secure data governance reduce the frequency and severity of failures, making residual risks more insurable. Combining these proactive measures with insurance creates stronger resilience and a more balanced foundation for the insurability of Gen AI risks.

Insurance solutions should be accompanied by risk assessment, safeguards, and mitigation to strengthen resilience to Gen AI risks.

Based on these findings, incumbent insurers are advised to take a proactive stance toward Gen AI. We recommend that insurers actively develop new and refine existing insurance solutions to accommodate Gen AI risks – for example, by enhancing coverage for misinformation liability, intellectual property disputes or AI-driven operational failures – and continuously adapt underwriting as Gen AI usage grows. By doing so, insurers not only protect their commercial clients but also stand to create new revenue streams and reinforce their role in absorbing emerging technological risks. Insurers should collaborate with technology developers, insured firms, and regulators to establish common standards for AI risk management and accountability, ensuring that evolving Gen AI risks are transparently and effectively insured.

Insurers should take a proactive stance toward Gen AI and collaborate with other stakeholders to establish standards for risk management.

Finally, our analysis offers a snapshot of Gen AI adoption and risk perceptions as of early 2025, based on a survey of 600 business customers in six selected markets. Future research may investigate how these dynamics unfold as the technology evolves. The insurability assessment is necessarily conceptual at this stage, since legal and technical standards for Gen AI are still in flux. This report also focuses solely on Gen-AI-induced risks for commercial enterprises; however, Gen AI may also introduce societal risks, such as election-related deepfakes or declining public trust, which warrant separate investigation.

Future research should monitor Gen AI's development over time, with a particular focus on distinguishing between applications and risks that are fast maturing

and those which remain nascent and ill-defined. Such monitoring will be crucial for adapting insurance products, pricing models, and regulatory approaches to the rapidly changing AI landscape.

In the field of Gen AI risks, what we know is much less than what we do not know. What we know is that Gen AI will introduce risks but it is not clear how fast Gen AI technology will develop and how it will shape the boundaries of insurability. Future insurance research should explore the evolving nature of Gen AI, assess the pace of its technological maturity, and address emerging risks to develop responsive insurance solutions.

Appendix 1: Existing AI risk classifications

TABLE 5: AI-INDUCED RISKS

Category	Specific risks	Description
Performance risks	Errors, bias, and black-box issues	AI systems can be prone to prediction errors, propagate biases, and lack transparency.
Security risks	Cyber intrusions, privacy concerns	AI-driven cyber threats pose risks to privacy and critical infrastructure.
Control risks	Rogue AI and oversight failure	Superintelligent AI poses a risk if controls fail, potentially threatening societal stability.
Societal risks	Autonomous weapons, intelligence divide	Inequities can arise due to unequal access to AI capabilities, impacting prosperity.
Economic risks	Job displacement, liability issues	AI can displace jobs and may lead to high-stakes liability risks if systems fail.
Ethical risks	Misalignment of values	Without ethical safeguards, AI decisions may conflict with societal values.

Source: Eling[46]

FIGURE 15: GEN-AI-INDUCED RISKS

Gen-AI-related risks that organisations consider relevant and are working to mitigate, % of respondents*

* Asked only of respondents whose organisations have adopted AI in at least 1 function. For both risks considered relevant and risks mitigated, n=913.

Source: Adapted from McKinsey[47]

There is also a framework to describe Gen-AI-induced risks that includes contract risk, tort risk, regulatory developments, intellectual property rights, deceptive trade practice risk, discrimination and defamation, and cybersecurity risk.[48] Furthermore, Aon has created a matrix (see Table 4), which outlines common coverage starting points for basic available coverage and exposes significant gaps in existing insurance.

46 Eling 2019.
47 McKinsey 2023.
48 Aon 2023.

Appendix 2: Insurability of Gen AI risks

TABLE 6: INSURABILITY OF GEN AI RISKS (EXTENDED)

Category	Criteria	Description and assessment
Actuarial criteria	Randomness of loss occurrence	Loss occurrence should be random; frequency and predictability of risk events should be identifiable. Gen AI output exhibits a degree of randomness and thus requires validation to avoid hallucination or harmful content. Where such systematic validation is lacking, randomness in AI failures is difficult to assess. Rapid AI development and learning from complex data make predicting risks difficult, complicating premium pricing and claim frequency estimation. Gen AI output exhibits a greater degree of randomness than traditional AI or traditional machine learning (e.g. hallucinations, misinformation, unauthorised content generation). Losses often stem from emergent, unforeseen risks, complicating risk modelling.
	Maximum possible loss	Potential maximum loss should be manageable for insurers. AI failures in critical sectors (e.g. healthcare, finance) can lead to catastrophic losses, threatening insurers' solvency. Gen AI misuse (e.g. creating deepfake content or automating cyberattacks) could result in cascading reputational and financial harm, with systemic risks spreading across industries.
	Average loss amount	The average loss per incident should be moderate. AI failures can lead to significant financial and reputational damage, resulting in high average losses. Gen AI incidents, such as large-scale misinformation campaigns or regulatory fines from copyright violations, can result in unusually high average losses.
	Loss frequency	Losses should occur frequently enough for accurate risk assessment; a large pool of similar risks helps diversify and mitigate individual losses. AI risks are highly context dependent and with limited historical data, accurately estimating loss frequency for Gen AI (e.g. model misuse or unintended output harms) remains difficult; diverse AI applications hinder the formation of large, homogeneous risk pools. In the mid-term, though, sufficient frequency is to be expected.
	Information asymmetry (moral hazard and adverse selection)	Information asymmetry between insurers and insureds should not be excessive. Insured parties may neglect AI system integrity with insurance coverage (moral hazard), while riskier AI systems may seek coverage (adverse selection). Gen AI systems often rely on algorithms that may be modified post-deployment, increasing asymmetry. Insured parties may lack transparency on safeguards and overlook maintenance of content filters or safeguards against misuse, heightening moral hazard. Insurers may struggle to verify how businesses manage Gen AI risks.

● Minimal challenges to insurability ● Some challenges to insurability ● Violation of insurability under traditional insurance models

Category	Criteria	Description and assessment
Market criteria	Adequate premiums	Premiums should cover expected losses and costs and also be affordable for the target market. Heightened uncertainty about processes underlying Gen AI and the associated ways in which harm can arise may mean additional premium loading and pressure affordability of smaller businesses or startups relying on these technologies. High potential AI failure costs may necessitate substantial premiums, potentially making coverage unaffordable.
	Acceptable coverage limits	Policyholders should find coverage limits acceptable. Insurers may hesitate to offer high limits for Gen AI due to uncertainty in potential liabilities, such as damage from widespread content misuse or errors in AI-generated decisions.
Societal criteria	Consistency with public policy	Insurance should align with societal values and public policy. Gen AI raises ethical issues, such as creating harmful or biased content, which may conflict with societal norms and reduce policymakers' acceptance of certain insurance products.
	Legal permissibility	Coverage should comply with laws and regulations. For Gen AI, the evolving landscape of copyright, intellectual property, and liability laws makes defining insurable risks challenging. Legal conflicts over AI-generated content ownership or accountability can further complicate underwriting decisions. Evolving AI regulations and legal uncertainties also affect insurability.

● Minimal challenges to insurability ● Some challenges to insurability ● Violation of insurability under traditional insurance models

Source: Geneva Association

References

Abraham, K.S. 1988. Environmental Liability and the Limits of Insurance. *Columbia Law Review* 88 (5): 942–988.

Acharya, D.B. et al. 2025. Agentic AI: Autonomous intelligence for complex goals—A comprehensive survey. *IEEE Access* 13: 18912–18936.

Aon. 2023. Use AI and Insurance Insights to Make Better Decisions.

Aldasoro, I. et al. 2025. Generative Artificial Intelligence and Cyber Security in Central Banking. *Journal of Financial Regulation* 11 (1): 119–128.

Al-kfairy, M. et al. 2024. Ethical Challenges and Solutions of Generative AI: An interdisciplinary perspective. *Informatics* 11 (3): 58.

AXA XL. 2024. AXA XL Unveils New Cyber Insurance Extending Coverage to Help Businesses Manage Emerging Gen AI Risks.

Berliner, B. 1982. *Limits of Insurability of Risks*. Prentice Hall.

Braun, A., and R. Jia. 2025. InsurTech: Digital technologies in insurance. *The Geneva Papers on Risk and Insurance—Issues and Practice* 50: 1–7.

Cremer, F. et al. 2024. Enhancing Cyber Insurance Strategies: Exploring reinsurance and alternative risk transfer approaches. *Journal of Cybersecurity* 10 (1): tyae027.

Deloitte. 2024. Generative AI in Insurance.

Eling, M. 2019. How Insurance Can Mitigate AI Risks. *The Brookings Institution's Artificial Intelligence and Emerging Technology (AIET) Initiatives.*

European Union. 2023. Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts.

FortiGuard Labs. 2025. *Global Threat Landscape Report 2025*.

Gatzert, N. et al. 2016. Assessing the Risks of Insuring Reputation Risk. *Journal of Risk and Insurance* 83 (3): 641–679.

Gen Re. 2024. Generative Artificial Intelligence in Insurance – Three lessons for transformation from past arrivals of general-purpose technologies.

Gen Re. 2025. Decision-making in the Era of Generative Artificial Intelligence.

Geneva Association. 2018. *Big Data and Insurance: Implications for innovation, competition and privacy*. Author: Benno Keller. March

Geneva Association. 2022. *Responsible Use of Data in the Digital Age: Customer expectations and insurer responses*. Authors: Isabelle Flückiger and Kai-Uwe Schanz. October.

Geneva Association. 2023. The Value of Insurance in a Changing Risk Landscape.

Google DeepMind. 2023. Evaluating Social and Ethical Risks from Generative AI.

Harris, L., and M. Heikkilä. 2025. Insurers Launch Cover for Losses Caused by AI Chatbot Errors. *Financial Times*. 10 May.

Hermann, E., and S. Puntoni. 2024. Artificial Intelligence and Consumer Behavior: From predictive to generative AI.

Journal of Business Research 180: 114720.

Hofstede. 2025. Uncertainty Avoidance Indexes.

Hu, K. 2023. ChatGPT Sets Record for Fastest-growing User Base. *Reuters*. 2 February.

IBM. 2024a. What Is Generative AI?

IBM. 2024b. Examining Synthetic Data: The promise, risks and realities.

International Organisation for Standardization and International Electrotechnical Commission. 2023. Artificial Intelligence – Guidance on risk management.

Joyce, S. 2025. Breaking Through the Hype of AI in Cyber. *InfoRiskToday*. 5 May.

Kim, J.J. et al. 2025. Generative AI Can Effectively Manipulate Data. *AI Ethics*.

KPMG. 2024. The Impact of Artificial Intelligence on the Insurance Industry.

Li, S., and M. Faure. 2025. The Insurability of AI-related Risks: Implications from the recent legislation in the European Union. *The Geneva Papers on Risk and Insurance—Issues and Practice* 50 (3): 524–544.

Lu, J. 2024. Generative AI And Personalization at Scale: Crafting customer experiences. *Forbes*. 7 June.

McKinsey. 2023. The State of AI in 2023: Generative AI's breakout year.

McKinsey. 2024. The State of AI in Early 2024: Gen AI adoption spikes and starts to generate value.

McKinsey. 2025. The State of AI: How organisations are rewiring to capture value.

Murugesan, S. 2025. The Rise of Agentic AI: Implications, concerns, and the path forward. *IEEE Intelligent Systems* 40 (2): 8–14.

NACD. 2025. AI as a Cybersecurity Risk and Force Multiplier.

National Institute of Standards and Technology. 2024. Artificial Intelligence Risk Management Framework (AI RMF 1.0).

NVIDIA. 2024. What Is Agentic AI?

OECD. 2019. Recommendation of the Council on Artificial Intelligence.

Perez, S. 2025. ChatGPT Doubled its Weekly Active Users in Under 6 Months, Thanks to New Releases. *TechCrunch*. 6 March.

Peters, G.W. et al. 2011. Impact of Insurance for Operational Risk: Is it worthwhile to insure or be insured for severe losses? *Insurance: Mathematics and Economics* 48 (2): 287–303.

Ramakrishnan, R. 2025. When to Use GenAI Versus Predictive AI. M*IT Sloan Management Review*.

Relm Insurance. 2025. Relm Insurance Launches AI Liability Solutions to Address Emerging Risks in the AI Ecosystem.

Walkowiak, E., and T. MacDonald. 2023. Generative AI and the Workforce: What are the risks?

Wang, Y. 2023. Generative AI in Operational Risk Management: Harnessing the future of finance.

Wei, X. et al. 2025. Addressing Bias in Generative AI: Challenges and research opportunities in information management. *Information & Management* 62 (2): 104103.

Xu, H. et al. 2024. Security Risks Concerns of Generative AI in the IOT. *IEEE Internet of Things Magazine* 7 (3): 62–67.


INSURANCE FOR A BETTER WORLD