Facilitating a better future

LMA Survey on AI Risk Management

In partnership with Barnett Waddingham

16 April 2026

Introduction

This report presents the findings and key insights from our latest survey on Artificial intelligence (AI) Risk Management, which was distributed to LMA members. We received responses from a wide range of professionals such as Chief Operating Officers (COOs), Chief Risk Officers (CROs), Head of Operations and Risk Analysts from various managing agents and syndicates.

We received 39 survey responses, representing over 60% of the market stamp capacity.

11 participants were interviewed to deepen our insights on the AI risk management and use cases.

This survey builds on our previous survey, which explored the level of adoption of AI and ML within the insurance market as well as the key barriers and concerns hindering progress. The previous survey was distributed to Chief Risk Officers and Chief Actuaries. The findings from that survey revealed that AI and ML adoption in the Lloyd's Market was still in its infancy, with respondents expressing concerns around regulatory oversight and the absence of a robust AI framework. Further information can be found in the report titled "Artificial intelligence and machine learning in actuarial and risk", which was published in May 2025.

This follow-up survey was designed to assess the maturity and breadth of existing AI frameworks within the Lloyd's Market, with particular emphasis on the governance processes in place to reduce exposure to risks associated with the use of AI.

The key takeaway of the survey is: Over the last year, we have seen significant progress in terms of AI frameworks and governance in place for various LMA members. AI use cases continue to develop across functions; however, the market remains at an early stage of its AI adoption journey.

The slides below include the following:

- Current state of AI framework and risk management
- AI use cases
- Deeper insight into the survey results

The LMA, with support from Barnett Waddingham LLP (BW), has published another report titled **"AI Adoption Toolkit"** which builds on the findings from the two surveys. The report provides guidance on best practices for LMA members to consider when designing or enhancing their AI framework, which is an essential part in the journey towards integrating AI in their business operations.

Current state of AI framework and risk management

In our previous survey, only 25% of the participants reported the use of the AI in their workplace. One year later, this picture has changed significantly, with the majority of participants now adopting AI. Despite signs of progress, AI use cases remain limited and mainly focus on Generative AI tools, such as Generative Pre-trained Transformers (GPT) for summarising reports and creating meeting notes.

However, a large proportion of the survey participants have an AI framework in place and are actively managing the risks around AI systems and tools. This shows that the market appears to be building governance processes (policies, committees, clauses) ahead of scaled deployment. The open question is whether assurance depth will keep pace when AI moves from productivity tools into supporting underwriting/pricing/claims decision-making.

Survey highlights:

72% of survey participants already have an AI framework in place, with 37% having specific provisions for Gen AI.

21% of participants are in the process of developing an AI framework.

Over 60% of respondents enforce mandatory human oversight and review of AI-generated outputs/decisions.

Industry leaders agree that human-in-the-loop remains a key part of any AI rollout.

44% responded that the Chief Technology Officer is responsible for establishing and overseeing the AI governance framework.

33% of participants have an AI Governance Committee.

1 in 4 participants indicated that general third-party risk management are in place to mitigate external AI risk, rather than having specific provisions.

Over 60% of respondents have contractual clauses as safeguard.

** Base: n=39 completed responses. Multi-select questions: % of respondents selecting item. Rounding to nearest whole %.*

AI use cases – Slow but steady progress

AI and ML development is still primarily driven at the organisational level, with strategic oversight and initiatives managed across the entire business with expert support sought for specific use cases.

AI use cases have evolved since our survey from last year. There are broader AI use cases that are being experimented with in different business areas, such as:

Underwriting

AI in underwriting has largely been focused on data ingestion from slips and improving efficiency.

More recently, this has evolved into practical applications like virtual assistants for document and wording review and proof-of-concepts for sanctions risk and compliance checks.

Internal AI Tools

Previously, organisations relied on publicly available generative tools for coding and summarisation.

Now, organisations are building internal LLMs for document comparison and chatbots for HR and operational queries, ensuring better control and IP protection.

Compliance & Risk

In our previous survey, we noted that AI's role in compliance was minimal, limited to maintaining risk frameworks.

Respondents in this year's survey shared new use cases such as marine sanctions tracking, wording analytics for slip-level exclusions and risk reporting linked to external data sources, signalling a stronger focus on governance.

Claims

Previously, AI was used mainly for claims classification and converting PDFs into usable formats.

Now, it supports summarisation for board reporting and enhanced categorisation through vendor tools, providing richer insights and improving reporting quality.

Operations & Finance

In our previous survey, we noted that efforts centred on data augmentation and data cleansing for very specific areas such as the modelling of catastrophe risk.

In the latest survey, we learnt that AI is tackling broader challenges such as automated data ingestion, legacy system integration, finance document processing and driving enterprise-wide efficiency.

Pricing

Previously, AI supported coding automation and Python packages for actuarial work.

Now, pricing makes enhanced use of code completion and programming AI-assistants. Upcoming pricing transformation projects show a shift toward embedding AI in core pricing workflows.

CTO/IT specialists lead AI Governance Oversight

The survey results show that AI governance is most often overseen by the **Chief Technology Officer (CTO)**.

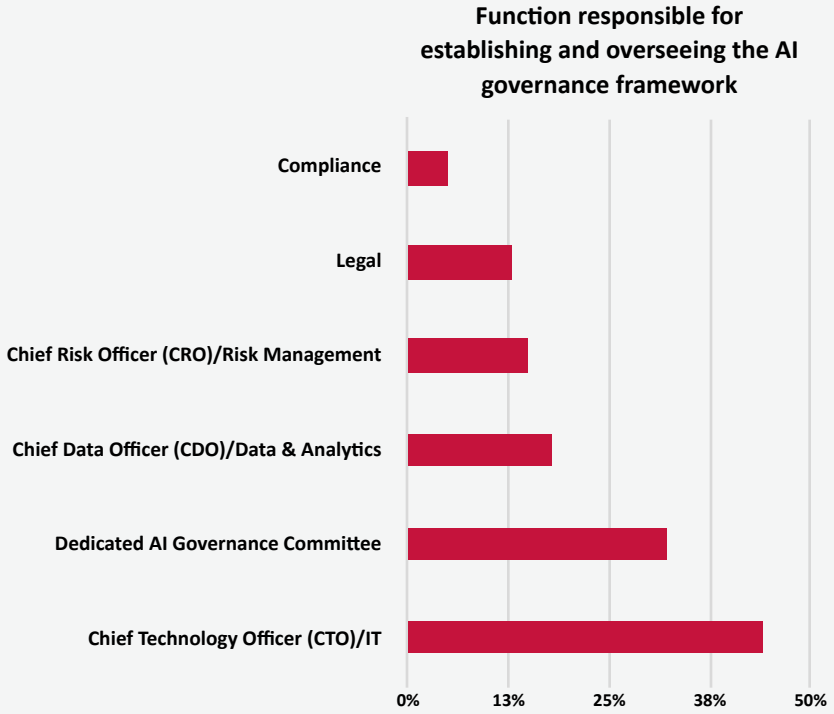
33% of participants reported having a **Dedicated AI Governance Committee**, making it the second most common response and highlighting a growing move toward formalised, specialised oversight structures. Generally, the AI Governance Committee would include key stakeholders from a range of departments such as IT, Legal, Compliance and Risk.

Several organisations have assigned AI governance to either the **Chief Data Officer (CDO)** or the **Chief Risk Officer (CRO)**, highlighting that a wider perspective may sometimes be more appropriate to capture all the relevant risks and opportunities in the decision-making process. This responsibility is also dependent on the existing organisational structures.

A smaller proportion of participants have allocated the responsibility to the **Legal**, **Compliance** and **Operations** teams.

Overall, there is no clear consensus on where the responsibility of AI Governance should reside within companies. However, the preferred approach was to involve stakeholders from different teams for better risk and opportunity coverage.

It is worth noting that following our discussions with industry leaders, at the moment not many respondents have hired AI specialists within their business.



Human oversight of AI outputs remains critical

Mandatory human oversight of AI decisions remains the most common accountability measure, with 62% of respondents using this approach, highlighting the strong preference for human review and intervention. Following our discussions with industry leaders, human-in-the-loop remains a critical part of any AI rollout.

54% of respondents have **clear ownership assigned to specific individuals or teams for each AI system**, reflecting growing structure and governance around AI.

Over 40% of respondents have also implemented **robust validation and testing processes** to ensure AI models perform accurately and reliably.

However, ambiguity persists: 36% of respondents have **not yet fully defined** the accountability around AI systems, signalling that this is a development area. In such instances, existing frameworks are being relied upon.

Few companies (10%) have **integrated AI governance into the existing Senior Managers & Certification Regime (SMCR)**, revealing a gap in formal regulatory alignment.

Overall, most firms employ multiple methods to ensure accountability and to mitigate the expansive risks that are associated with the use of AI.



Data Privacy & Cybersecurity remain high on the agenda

The results highlight that most respondents rated **Data Privacy & Security** as the highest area of concern relating to AI, with very few expressing low concern. This underscores the need for robust data protection and secure systems when adopting AI.

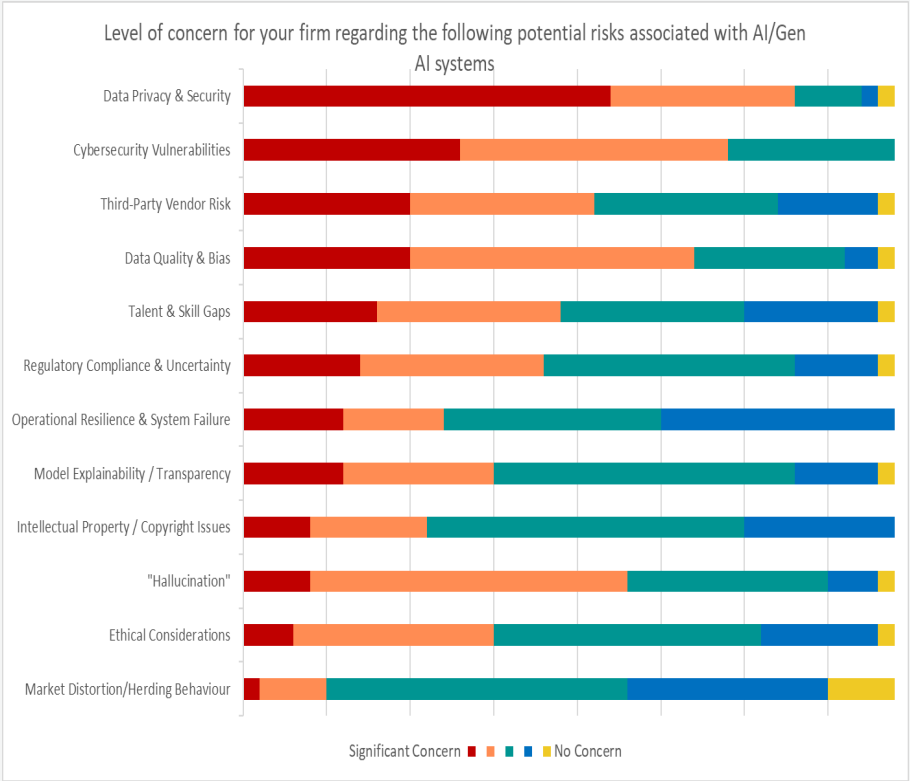
Cybersecurity follows closely with all respondents rating this as at least a medium concern. This highlights persistent fears around AI security and the importance of strong cybersecurity measures to avoid compromising other areas of the business.

Respondents also expressed concern with **Third-Party Vendor Risk and Talent & Skill Gaps**. This emphasises concerns over dependency on external AI providers and insufficient internal expertise to manage risks associated with AI.

Opinions were quite divided on **Model Explainability/Transparency** and **Regulatory Compliance & Uncertainty**, suggesting a neutral stance overall. This is likely due to the measured implementation of AI within insurance businesses.

A fair share of participants emphasised high concern on the **Data Quality & Bias**, with similar concerns shown for "**Hallucination**". The general sense remains that there is significant concern around the accuracy and reliability of the outputs being produced by AI.

Respondents currently perceive **Market Distortion/Herding Behaviour** as lower concern, plausibly reflecting limited deployment in core decision-making processes. It suggests that participants are taking time to assess business needs before implementing AI tools. However, if in the future common vendor models and workflows start to dominate, systemic correlation could occur.



External AI risks should also be managed

Given the significant concerns around data security and cybersecurity, contractual clauses and due diligence procedures remain popular options to manage AI risks arising from third-party providers. Other measures currently being used are shown in the chart below.

