Facilitating a better future

LMA AI Adoption Toolkit

In partnership with Barnett Waddingham

16 April 2026

Introduction

Artificial intelligence (AI) now plays a pivotal role in our society. The possibilities that AI unlocks are vast, enabling applications that were once unimaginable. These technologies are driving a profound wave of digital transformation. The insurance industry is no exception. AI is already being experimented in key areas, such as pricing, underwriting, claims handling and risk.

As adoption increases, the opportunities are significant, but so are the risks. Many of these risks are hard to identify, measure or mitigate without a structured approach. The growing opportunity of AI highlights the importance of managing agents establishing a robust, transparent and adaptable framework to enable informed decision-making and maintain accountability around AI usage.

This report aims to offer guidance to LMA members by supporting them in developing or enriching their existing AI governance frameworks to ensure a responsible, transparent and effective use of AI systems across their operations. This framework has been developed using insights from the two recent surveys on AI and ML (Machine Learning) titled *"AI and ML in Actuarial and Risk"* and *"AI Risk Management"* conducted with Chief Risk Officers (CROs), Chief Actuaries and Chief Operating Officers (COOs), supplemented by interviewing 11 industry leaders at Lloyd's managing agents.

This guide is written for senior risk, actuarial, and operations leaders. It contains the following sections:

- AI Adoption Toolkit
- Overview of existing guidance from other organisations

Please note that this AI Adoption Toolkit is not intended to be perceived as a regulatory requirement, but rather as a set of suggestions designed to provide practical guidance to LMA members to devise or augment their AI policy or framework. The governance needs and risks faced by each LMA member is likely to be different. We recommend that local AI rules relevant to your business as well as your business needs are reviewed in detail when formulating your AI policy or framework.

Definitions of AI and ML

AI covers a vast array of tools and systems and hence definitions are always key when discussing these tools in a business context. On this slide, we provide high level definitions of key terms used in this space. However, these should be defined in your internal taxonomy to ensure consistent use across your organisation. It should be noted that other definitions exist, e.g. by the UN and EU AI Act

Artificial intelligence (AI)

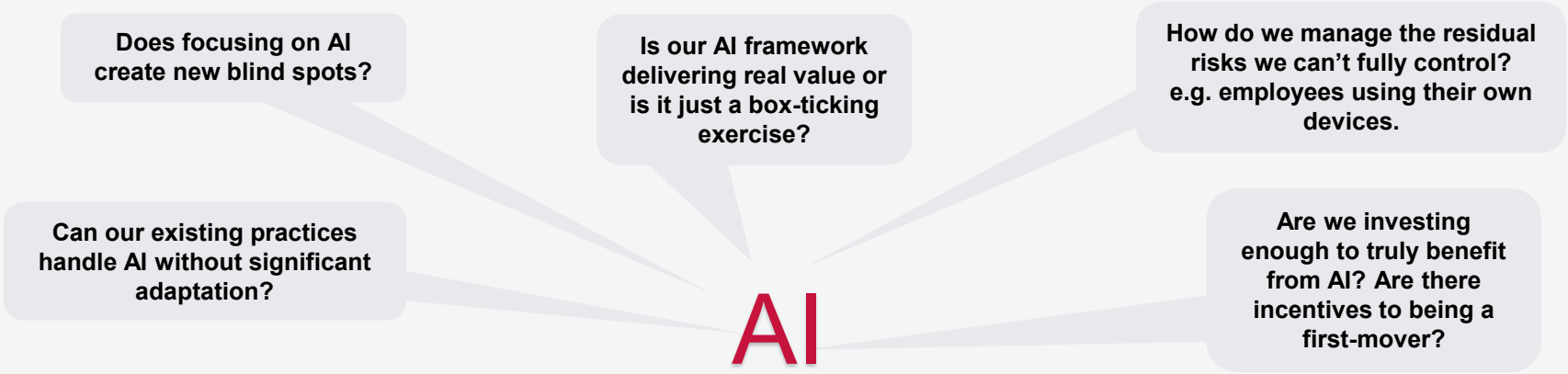
- **Technologies that develop machines with the ability to imitate intelligent human behaviour.**
- **Can be seen as a 'black box' where decisions are not easily interpretable by humans.**
- **Includes Generative AI and Large Language Models.**

Machine learning (ML)

- **A form of intelligence that enables a machine or system to learn and improve from experience.**
- **Uses algorithms to analyse large amounts of data and learn from insights to be able to form decisions.**
- **Includes Generalised Linear Models (GLMs), neural networks and image recognition algorithms.**

Insights from industry leaders

Across all the interviews, one theme stood out clearly: there is no consensus around what an ideal AI framework would look like. Many leaders want to embrace AI as a force for progress, yet they acknowledge the risks, uncertainties and organisational shift that come with it. It is apparent that AI is full of promise, but leaves managing agents with the following unresolved questions:



The reality is that there is no single "right" or "wrong" approach to an AI framework. AI is new territory that has the potential to impact across various functions. What matters more is maintaining flexibility and being ready to adapt as new risks and technological developments emerge, while continuing to meet your business needs.

In the slides that follow, we outline several practical suggestions to help address the concerns and questions raised by industry leaders. These are not definitive answers, but starting points for building a resilient, responsible and adaptable approach to AI.

Insights from industry leaders

Common themes

1. AI as an augmentation tool
AI adoption is focused on efficiency and augmentation rather than autonomous decision-making. Companies prioritise use cases that streamline workflows, reduce manual effort and enhance data quality without replacing human judgment. All participants were keen to keep a “human-in-the-loop”.

2. Some form of AI framework exists
The majority of participants have established some form of AI framework to meet regulatory requirements. However, many remain uncertain whether it adequately addresses all possible risks.

3. Mandatory staff training
Companies have invested in staff training related to AI. A few examples include awareness campaigns, training provided by external experts as well as mandatory training and policy reading before use.

4. Guidelines and regulations
AI frameworks are designed using existing regulations and guidelines available (See page 11). However, respondents continue to face significant challenge in navigating the constantly evolving landscape.

5. Cross functional governance
Most aim to implement a cross-functional governance structure involving legal, compliance, risk, IT and other key stakeholders from the business. The views from multiple subject matter experts is used to identify risks in the use of AI systems given its extensive application.

Key differences

1. Extent of AI use
A few managing agents have embedded AI into their core processes such as underwriting, pricing and claims handling, while others limit its application to supporting processes for time efficiency, e.g. coding, summarising documents. It should be noted that in certain cases companies have developed their own internal large language model.

2. Set up of AI monitoring groups
A few participants have established a dedicated AI Governance Committee to oversee AI usage, while others currently assign this responsibility to Chief Technology Officers.

3. Different practices to mitigate risks
Risk mitigation approach differs by LMA member, and this includes contractual clauses to protect data and Intellectual Property, more detailed due diligence for third-party providers and in some instances even prohibiting the use of generative AI throughout the supply chain.

4. Range of controls
A range of controls are applied based on each firm’s risk appetite. Some companies rely on training and AI frameworks, other deploy controls that ban or restrict AI use and others enforce compliance via mandatory tests and human oversight.

5. Depth of AI framework
While most companies have implemented AI frameworks, the structure varies: a few are principle-based while others are embedded within broader technology and data governance policies.

AI Adoption Toolkit

The AI Adoption Toolkit has been designed to support the safe, responsible and value-driven adoption of AI across managing agents. Its purpose is to help organisations unlock the benefits of AI while ensuring that risks are managed effectively. We introduce **five principles** that LMA members can consider when designing their own AI policy or framework:

AI Adoption Toolkit - Principles

1 Governance & Accountability

There should be clear AI governance and accountability. Governance should be multi-layered, with clearly defined roles, oversight mechanisms and ongoing monitoring. An example of a governance structure is provided below:

- The Board defines the organisation's risk appetite to AI.
- The firm assigns a centralised team or an operational owner (e.g. the CTO or COO), who is responsible to oversee the AI operations across the organisation. Alternatively, AI governance responsibility is allocated within existing governance structures (e.g. risk committee) and mapped to the firm's responsibility map/Statement of Responsibilities where relevant.
- The firm establishes an AI working group for the supervision of specific AI models. This involves evaluating AI use cases, assigning a risk tier (see next page) and defining required controls and validation tests. Given the wide implications of AI, inputs are provided by all relevant departments e.g. legal, compliance and IT. Whilst not essential, hiring AI specialists could be beneficial.
- The firm monitors governance and accountability as part of its internal audit, to provide independent assurance on governance and control effectiveness. Examples of effective monitoring include:
  - Implementing automated monitoring dashboards to flag misuse and detect over-reliance.
  - Blocking unauthorised tools using network filters.

AI Adoption Toolkit - Principles

1 Governance & Accountability (cont.)

Validation

A consideration for managing agents in earlier days of adoption is over-reliance on AI. Human oversight checkpoints are essential for AI systems to ensure credibility of the outputs. This could be in the form of validation processes e.g. comparing the outputs from AI tools to those produced by existing processes and considering divergence.

Regulation

Where possible, align internal policies with the relevant regulations, such as the EU AI Act, and consult with the legal team to confirm that AI policies remain compliant for entities operating across multiple territories (e.g. US, EU, UK).

AI Adoption Toolkit - Principles

2 Risk Tiering

Managing agents can adopt a risk tiering approach to determine the appropriate level of controls, oversight and validation necessary when rolling out AI systems or tools. An example is shown below:

	Low risk	Medium risk	High risk
Example	AI use for non-critical operations with minimal impact on customers, e.g. summarising documents, drafting emails, internal chatbots, automation of routine tasks.	AI systems that could influence business processes or customers but used only for limited decision-making. E.g. AI data processing, fraudulent claims detection.	AI systems that make autonomous decisions with significant impact to customers. E.g. automated underwriting decisions, automated claims approval.
Suggested actions/ controls	Apply general AI use policy and check for acceptable use, include an entry in the AI inventory, carry out training.	Document validation procedures followed, maintain human-in-the-loop, supplier due diligence, regular reviews of AI tools.	Consider whether this level of risk is acceptable, use independent AI model validation, fairness/bias assessment, formal sign-off, enhanced monitoring and incident response.

AI Adoption Toolkit - Principles

3 Data Protection, Security & Intellectual Property

Managing agents should prioritise data protection, security and intellectual property safeguarding at every stage of AI usage. They should maintain an AI inventory (both internal and external/vendor) with vendors required to declare AI usage. Examples:

- **Data handling:** limit the use of public AI bots strictly to publicly available data, prohibit the input of confidential or sensitive content into unsecured AI systems, enforce robust encryption standards.
- **External vendors:** require vendors to disclose all AI components used in their solutions, require a notification of any new AI features or changes from the third-parties, prohibit training on client data from external vendors unless explicitly authorised.
- **Monitoring:** conduct systematic audits of existing vendor agreements to identify hidden AI elements. Also monitor/control internet traffic to limit use of unauthorised AI.

AI Adoption Toolkit - Principles

4 Training & Awareness

Training and employee awareness are critical when it comes to the responsible use of AI. Inexperience or inappropriate use of these technologies can lead to additional risks. Thus, to mitigate these risks, managing agents could consider providing internal or external training on:

- Data protection
- Safe and responsible use of generative AI tools

Managing agents could also consider:

- Setting up an 'AI Champions' group to act as internal advocates. Their responsibility is to identify AI knowledge gaps raised or observed by the employees and address them by providing or suggesting the relevant training.

It is important to note that the level of training required depends on the specific needs of each business and the current stage of AI integration. Investing heavily in training when it is not necessary can divert time and resources away from more impactful priorities. It should be noted that training alone is not a sufficient control. It must be backed by technical restrictions and monitoring for unauthorised usage.

To ensure that training is effective, some factors to consider are:

Digestible | **Real-world examples** | **Role-specific** | **Regular refreshers** | **Test staff knowledge (e.g. quiz questions)**

AI Adoption Toolkit - Principles

5 Pragmatic Adoption

Adoption of AI should deliver value efficiently, without creating unnecessary complexity or risk. Start small, embed controls early and scale gradually. There is an opportunity cost of not adopting AI and hence its roll-out should be done in a controlled yet effective manner. It is also important to remain flexible.

Companies could begin with productivity and efficiency tools that pose minimal regulatory or customer impact, e.g. a large language model to draft documents and to review codes for internal models. Slowly deploying these AI tools will allow the managing agents to iterate and learn from these AI use cases and gradually increase usage while managing the associated risks.

Further considerations

While the AI Adoption Toolkit provides a foundation for building an effective AI governance structure, there are additional measures that could be considered to reinforce existing policies in place for effective AI usage.

Independent verification for high-risk decisions

- Conduct second-line of external validation for models and processes that materially impact customers or conduct risk.
- Provides assurance and regulatory readiness.
- Apply only to use cases in the high-risk tier and validate for accuracy and bias.

AI Metrics & Key Performance Indicators (KPIs)

- Maintain a registry capturing value and adoption of each AI tool.
- This could include time saved per task, coverage improvements, user adoption and satisfaction, potential incidents (such as data leakage, unauthorised tool usage).
- This will provide managing agents a clear view of the tangible benefits and risks associated with AI tools, enabling better decision-making.

Exit and contingency planning for vendor-enabled AI

- Define practical steps for service disruption, regulatory non-compliance or strategic exit.
- Helps to reduce dependency risk and improves resilience.

Ready-to-Use Templates

- Companies could prepare a template to be filled in when deploying an AI tool.
- This will assist them in classifying the AI tools into an appropriate tier and go through the right governance procedure.
- An example of such a template can be found in the appendix A of this report.

Existing guidance from other organisations

ABI AI Guide

ABI in their AI guide sets the 5 AI principles:

Safety, security and robustness
- AI systems needs to be reliable, resilient and secure throughout their lifecycle.

Transparency & Explainability
- AI decisions should be clear and understandable to users and stakeholders.

Fairness
- AI must deliver consistent and equitable outcomes across all customer groups.

Accountability and governance
- Clear roles, responsibilities and oversight must be established for AI systems. Organisations should also define liability.

Contestability & Redress
- Customers should have accessible channels to challenge or appeal AI-driven decisions.

UK Government: AI Assurance

UK Government introduces the AI Assurance Toolkit which focuses on three phases:

Measure, Evaluate and Communicate

Some practical methods mentioned in the AI Assurance Toolkit are:
- Performance Testing & Model Evaluation
- Data Assurance
- Risk & Impact Assessments
- Bias Audits & Compliance Checks
- Conformity Testing & Certification
- Formal Verification
- Cybersecurity Measures

EIOPA: Opinion on AI governance and risk management

EIOPA's Opinion follows a principle-based approach and aligns with the underlying principles and requirements of the AI Act.

Principles

1. **Governance & Risk Management:** Clear frameworks to oversee AI and manage risks.
2. **Risk-Based Approach:** Classify AI and apply proportionate controls.
3. **Transparency & Explainability:** Make AI decisions understandable.
4. **Human Oversight:** Keep humans in control of critical decisions.
5. **Data Governance & Quality:** Use accurate, representative, bias-free data.
6. **Fairness & Non-Discrimination:** Avoid unfair or discriminatory bias.
7. **Robustness & Security:** Ensure resilience and protection against attacks.
8. **Accountability:** Define roles and responsibilities for AI outcomes.
9. **Monitoring & Continuous Improvement:** Ongoing performance checks.
10. **Stakeholder Engagement:** Involve internal and external stakeholders.
11. **Compliance Alignment:** Align with laws and sector-specific rules.

NIST: AI 100-1

The National Institute of Standards and Technology (NIST) developed an AI Risk Management Framework (RMF) to offer organisations guidance in this area.

Part I:

Sets the foundation: it explains how to frame AI risks, intended users of the framework and how to measure the framework effectiveness.

Part II:

Core Functions of the AI framework:
- **Govern:** Establish organisational policies, accountability and oversight for AI use.
- **Map:** Identify AI systems, their context and potential risks.
- **Measure:** Assess risks, performance and impacts of AI systems.
- **Manage:** Implement risk mitigation strategies and monitor outcomes.

Appendix A: AI Risk Tiering Template

1. Title & Owner:
2. Business Area & Sponsor:
3. Use Case & Expected Benefit:
4. Data Types & Sensitivity (classification):
5. System Description (tool / vendor / internal):
6. Decision Impact (none / influence / replace):
7. Initial Risk Tier (Low, Medium or High) & Rationale:
8. Proposed Controls (human review, logging, Data Protection Impact Assessment (DPIA), validation):
9. Validation Plan (dataset, metrics, acceptance criteria):
10. Operational Plan (rollout, training, change management):
11. Dependencies (IT / security / legal / vendor):
12. Sign-offs Requested (AI Working Group / Risk / Legal / Parent):

Appendix B: Example of Risk Tier Scoring

For each use case, a simple scoring structure could be used to classify into a risk tier. The table below shows an example of 5 simple binary tests that could be used:

Criteria	Score (0 or 1)
Impacts customer outcome?	
Influences underwriting / pricing / claims decisions?	
Uses special category / sensitive data?	
Externally sourced model / data / vendor dependency?	
Limited explainability / auditability?	
Total (sum of all the above)	

Then, a set of rules could be used to allocate a specific use case to a risk tier. For example:

- If there are two or more triggers, then the use case falls into “Medium” risk tier.
- If there are three or more triggers and/or any other “hard trigger”, then the use case falls into the “High” risk tier.
- Otherwise, a “Low” risk tier is selected.

Appendix C: AI Inventory Template

Identity & ownership: Unique ID; name; business area; business owner; technical owner; vendor / internal.

Purpose & impact: Use case description; “assist vs influence vs decide”; customer impact (Y / N); model outputs used downstream (where).

Risk & compliance: Risk tier; rationale; applicable regulations / jurisdictions; DPIA / privacy assessment status (if relevant).

Data & security: Data classification; access pathways; retention; vendor training-on-data terms (Y / N / conditional); security controls summary.

Assurance & monitoring: Validation completed (Y / N); last review date; monitoring in place (logs / KRIs); incidents / breaches; next review date.

Sample entry

- AI-023 | Claims summarisation assistant
- Owner: Head of Claims Ops | Tech owner: IT Platforms
- Tier: Low | Decision impact: Assist only
- Data: Internal non-sensitive docs (policy: no customer personal data)
- Controls: Approved tool only; logging enabled; prompt guardrails
- Validation: Pilot completed; quality checklist in place
- Monitoring: Monthly usage review; incident log = none
- Vendor: Yes (contract includes data/IP clauses; no training on client data)
- Next review: 30/06/2026

Appendix D: Links to other AI guidance

1. **ABI AI Guidance**
2. **UK Government AI Assurance**
3. **EIOPA - Opinion on AI Governance and Risk Management**
4. **NIST AI Risk Management Framework**