# AI Governance

Version: 1.0
Date: 2nd October 2024

A guide to developing an effective and
responsive AI policy within Financial Lines.

**AVIVA**

# AI Governance



## Introduction

In today's digital age, artificial intelligence (AI) is becoming an indispensable tool across multiple industries and sectors, with efficiency savings often cited as a key driver for wider use. However, the combination of fast-moving technology with an increasing reliance on AI comes with inherent risks that all businesses should be wary of.

This guide is designed to help businesses develop policies specific to their sector which effectively manage these risks and harness the full potential of AI while safeguarding against its pitfalls.

## What is AI?

Artificial Intelligence (AI) refers to the simulation of human intelligence in machines, enabling them to perform tasks that typically require human intelligence. These tasks include learning, reasoning, problem-solving, perception, and language understanding. In simpler terms, AI allows computers to mimic human-like thinking and decision-making processes.

## Why do businesses use AI?

Businesses use AI for various reasons, including:

1.  Increased efficiency: AI can automate repetitive tasks, allowing businesses to streamline processes and operate more efficiently.

2.  Improved decision-making: AI algorithms promise to analyse vast amounts of data quickly and accurately, providing valuable insights to support better decision-making.

3.  Enhanced customer experiences: AI-powered chatbots, recommendation systems, and personalised marketing campaigns can improve customer interactions and market presence.

4.  Cost reduction: By automating tasks and optimising operations, AI can help businesses reduce labour costs and other expenses.

5.  Competitive advantage: Adopting AI can give businesses a competitive edge by enabling them to innovate faster, adapt to changing market conditions, and deliver superior products and services.

AI technologies are playing a significant role in transforming industries and driving digital transformation initiatives across the world. Organisations that strategically implement AI solutions tailored to their specific needs and objectives are more likely to achieve success with AI and realise the benefits of AI technology. Data from the first 6 months of 2024 estimates that around 60% to 65% of organisations in the UK have implemented AI in some form. This percentage is constantly growing as more organisations recognise the potential benefits of AI in improving operational efficiency, enhancing decision-making, and driving innovation.

## How can I ensure my business is using AI safely and effectively?

- Understand AI Limitations – It is crucial for businesses to properly understand what AI can and cannot do. Artificial intelligence (AI) presents significant potential for transforming businesses, addressing complex challenges, and fostering a positive global impact. However, the efficacy of AI systems is contingent upon the quality of the data they are fed. Businesses using AI must recognise that AI systems are not infallible. They possess limitations, biases, and are susceptible to errors.

  As AI becomes increasingly involved in all areas of our lives, it is critical that businesses ensure they are training their systems with data that is fair, interpretable, and unbiased. Businesses will only be able to reap the full advantages of AI if they have robust processes to guide its responsible development of trustworthy AI. Businesses without these in place could exacerbate the negative consequences of unconscious bias.

  The first step in developing this is to ensure businesses understand the limitations of AI so they can mitigate risks associated with over-reliance. AI-generated insights must always be verified and never blindly accepted without critical assessment. AI platform disclaimers are there for a reason, including most commonly:
  (i) avoiding reliance on the output,
  (ii) likelihood of inaccurate data/information
  (iii) no intention to give advice.

- Implement Effective Backup Measures: To minimise the impact of AI failures, businesses should have reliable backup plans in place. This could involve cross-referencing AI-generated insights with traditional methods or having alternative AI solutions ready to deploy in case of system malfunctions.

- Establish processes and practices to test for and mitigate bias in AI systems: Consider the potential risk associated with poor transparency from AI developers and providers regarding the algorithms, data sources, and decision-making processes underlying AI systems, and whether your business is comfortable with how your AI is making decisions. The technical tools can highlight potential sources of bias and reveal the traits in the data that most heavily influence the outputs. Operational strategies can include improving **data collection through more cognizant sampling and using internal "red teams" or third parties to audit** data and models.

- Develop Skills for Adaptation: As AI continues to evolve, businesses may wish to consider focussing on developing skills that are less susceptible to automation, such as critical thinking, creativity, emotional intelligence, and complex problem-solving. By cultivating these skills, individuals can remain adaptable and resilient in the face of technological disruptions.

- Ethical Considerations: Be mindful of the ethical implications of AI usage, including privacy concerns, data biases, and potential societal impacts. Businesses must adhere to ethical guidelines and regulations governing AI usage in their respective fields to prevent legal repercussions and maintain trust with clients and stakeholders.

- Human Oversight and Intervention: Human oversight of AI remains essential. Businesses should not delegate critical decision-making solely to AI systems but instead use them as tools to support and enhance human judgement. Human intervention can catch errors, assess contextual nuances, and inject empathy into decision-making processes that AI lacks.

- Continuous Training and Education: Stay informed and educated. Keep abreast of the latest advancements, trends, and potential risks associated with AI technology. Attend seminars, workshops, and conferences, and engage with reputable sources of information to deepen understanding and awareness of AI developments. This empowers businesses to keep up with fast moving industry developments, make informed decisions and interpret AI-generated outputs accurately to limit unintended exposures.

## AI Supervision

The importance of AI supervision cannot be overstated. As AI systems become increasingly integrated, effective supervision is essential to ensure safe, ethical, and responsible use.

Establishing clear performance metrics will help to evidence supervision and as a minimum should include a review of accuracy, reliability, and fairness. Feedback loops and an auditable trail of inconsistent AI outputs audits will allow users, stakeholders, and domain experts to identify issues, improve system performance and address emerging challenges.

## Preliminary risk guidelines for Generative AI

Even if your business is not at a stage of developing or purchasing its own AI products for specific industry uses, it is likely that your employees are already considering the potential application and benefits of generative AI, such as Chat GPT or Copilot.

While this document sets out our views on best practice for mitigating the risks posed by all forms of AI, businesses might want to consider the following preliminary risk guidelines to help employees understand and mitigate the risks posed by widely available generative AI platforms.

- Get familiar with what it does, and its limitations.
- Educate your employees on basic pitfalls and risks (dissemination of confidential data, unforeseen consequences, biases).
- Be clear on what your employees are allowed to use it for within your business.
- Use it as a starting point for ideas or structure, not as an end point.
- Never enter any genuine client information or data.
- Ensure it is flagged to managers when it has been used as a tool.
- Treat it like a trainee – check everything carefully and flag up any concerning results.
- Ensure the author remains accountable for the ultimate output.
- Feedback successes or concerns to colleagues or management.

## Checklist

A generic Financial Lines: AI Policies Checklist is presented in Appendix 1 which can be tailored to your own business.

## Specialist Partner Solutions

Aviva Risk Management Solutions can offer access to a wide range of risk management products and services at preferential rates via our network of Specialist Partners.

For more information please visit:

Aviva Risk Management Solutions – Specialist Partners

## Sources and Useful Links

- National AI Strategy - GOV.UK (www.gov.uk)
- Guidance on AI and data protection | ICO
- SRA | Risk Outlook report: The use of artificial intelligence in the legal market | Solicitors Regulation Authority

## Additional Information

To find out more, please visit Aviva Risk Management Solutions or speak to one of our advisors.

Email us at riskadvice@aviva.com or call 0345 366 6666.*

*The cost of calls to 03 prefixed numbers are charged at national call rates (charges may vary dependent on your network provider) and are usually included in inclusive minute plans from landlines and mobiles. For our joint protection telephone calls may be recorded and/or monitored.

# Appendix 1 – AI Governance Checklist

| Location | |
|---|---|
| Date | |
| Completed by (name and signature) | |
| Next review date | |

| | | Y/N | Comments |
|---|---|---|---|
| 1. | Does your AI supervision policy clearly outline the scope of the policy, specifying which AI systems and applications it applies to? | | |
| 2. | Does your policy include a clear statement outlining the purpose of AI usage and its supervision within the business? | | |
| 3. | Do you have systems and ongoing checks in place to ensure your use of AI complies with relevant laws, regulations, and industry standards, both now and as they develop? | | |
| 4. | Does your policy identify key individuals or departments responsible for overseeing AI usage, including their roles and responsibilities? | | |
| 5. | Have you conducted a comprehensive risk assessment to identify potential risks associated with AI usage within your specific industry and considered strategies to mitigate industry specific risks? | | |
| 6. | What are your protocols for protecting sensitive data used by AI systems and ensure compliance with data privacy regulations? | | |
| 7. | Do you require transparency in AI decision-making processes, including disclosure of algorithms, data sources, and decision criteria where applicable?  How is this recorded and monitored? | | |

| | | | |
|---|---|---|---|
| 8 | What training and educational resources are provided to employees involved in developing, deploying, or using AI systems to ensure competency and awareness of best practices? | | |
| 9 | Does your policy ensure appropriate individual accountability for the outcomes of AI systems and processes? How? | | |
| 10. | Have you implemented measures to detect and mitigate biases in AI algorithms and data sets to ensure fairness and equality? How? | | |
| 11. | What procedures do you have in place for testing and validating AI systems before deployment to ensure accuracy, reliability, and safety? | | |
| 12. | What are your systems for ongoing monitoring and evaluation of AI systems to detect and address performance issues or unintended consequences? | | |
| 13. | What are your protocols for managing changes to AI systems, including updates, upgrades, and modifications, to maintain their effectiveness and integrity? | | |
| 14. | Do you have a comprehensive incident response plan to address AI-related incidents, such as system failures, data breaches, or ethical violations, in a timely and effective manner? | | |
| 15. | Do you maintain comprehensive documentation of AI systems, including their design, development, deployment, and usage, to facilitate transparency and accountability? | | |
| 16. | How do you communicate with stakeholders (including employees, **customers, regulators, and the public) about your business's AI** usage and its implications? | | |
| 17, | Do you create and support a culture of continuous improvement (e.g. by soliciting feedback loops, conducting regular reviews/audit, and implementing lessons learned) to enhance AI governance practices? | | |
| 18. | Have you developed ethical guidelines for AI usage, addressing issues such as privacy, confidentiality, fairness, transparency, and accountability? | | |

| 19. | How to you monitor your supply chain's use of AI and the associated risks? | | |
|---|---|---|---|
| 20. | Do you frequently review your AI policies and supervision to ensure it is up to date with latest developments? | | |
| | | | |

## Please Note

This document contains general information and guidance only and may be superseded and/or subject to amendment without further notice. Aviva has no liability to any third parties arising out of ARMS' communications whatsoever (including Loss Prevention Standards), and nor shall any third party rely on them. Other than liability which cannot be excluded by law, Aviva shall not be liable to any person for any indirect, special, consequential or other losses or damages of whatsoever kind arising out of access to, or use of, or reliance on anything contained in ARMS' communications. The document may not cover every risk, exposure or hazard that may arise and Aviva recommend that you obtain specific advice relevant to the circumstances.

2nd October 2024

Version 1.0

ARMSGI2092024