Spaced Learning Series

Artificial Intelligence

Artificial Intelligence (AI) is a broad term used to describe "models and systems for the performance of functions generally associated with human intelligence, such as reasoning and learning." In simple terms, AI allows machines to mimic the human mind, enabling them to rationalise and take actions to achieve a specific goal.

A subset of artificial intelligence is machine learning (ML), which refers to computer programs that can automatically learn from and adapt to new data without being assisted by humans.

#1

The use of AI in financial services

AI is commonly used in financial services. In most cases, firms do not replace their existing processes, but use AI to augment or upgrade them. For example:

- **Customer relationship management**, where AI-powered tools (e.g. chatbots) manage engagement with customers.
- **Financial apps**, which use facial recognition and voice command access to improve security.
- **Anti-money laundering (AML) and anti-fraud**, where AI is used to identify data anomalies and suspicious transactions.

#2

Governance and oversight is key

Regulatory organisations, such as **IOSCO**, expect firms to have "adequate skills, expertise and experience to develop, test, deploy, monitor and oversee the controls over the AI and ML that the firm utilises."

Responsible use of AI depends on the **quality of the underlying data**, so firms must consider the provenance and completeness of the data, along with how representative it is.

The **'model risk'** that AI applications fail or perform inadequately is magnified due to the speed at which AI systems operate, and the complexity of the underlying models.

#3

Potential risks associated with AI

Firms must be alert to the potential for AI to cause **consumer harm**, and take steps to mitigate the risk of poor consumer outcomes.

AI tools are generally developed by tech firms, so it is important to **understand the methodology** used by these third parties, and assess any operational resilience and cyber-security risks.

AI tools are also used by **criminals** (e.g. scammers are using generative AI to impersonate tone and language in phishing emails). In addition, criminals may use 'deepfake' voice cloning to replicate a person's speech, leading to authorised push payment fraud or information security breaches.

CCL academy

Compliance is everyone's responsibility. If you have any queries regarding your firm's procedures, contact your Compliance team.