

**Thought Leadership: Risk Management  
Implications of AI and Machine Learning**

Presented by Barry Liddy

# Risk Management Implications of AI and Machine Learning Algorithms

*Today we will talk about the risks of using algorithms across different financial services sectors, as well as how algorithms can be used to manage core business risks*



## 1. Usage of AI & Machine Learning in Financial Services



## 2. Identifying risks in AI and Machine Learning Algorithms



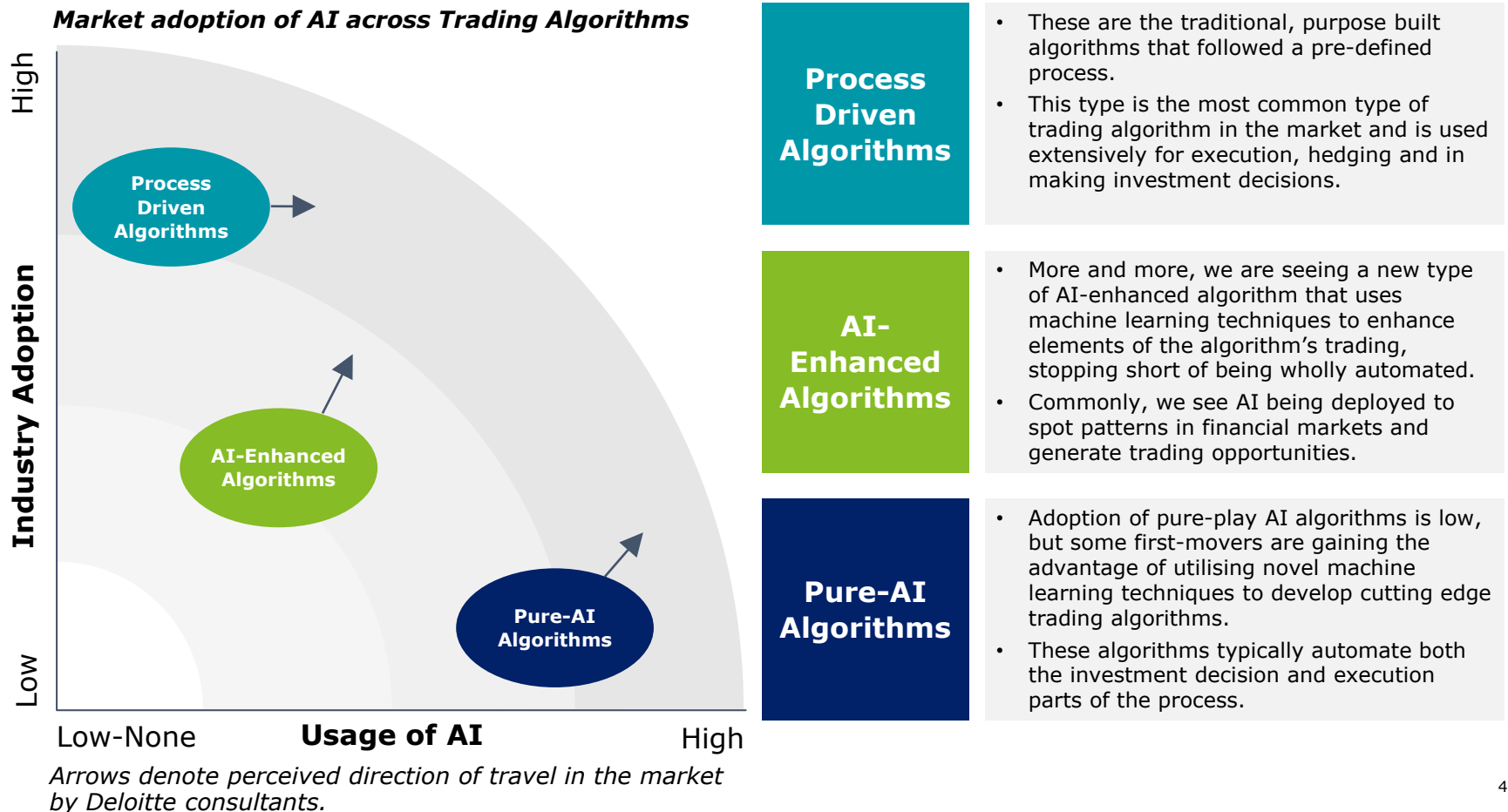
## 3. Managing the risks associated with AI & Machine Learning

# **Usage of AI & Machine Learning in Financial Services**

# Usage of AI & Machine Learning in Financial Services

## AI is frequently being used in developing trading algorithms

- Advanced AI and machine learning techniques are now being utilised across various different applications across financial services.
- The application of AI that has garnered the most interest from regulations is that of algorithmic trading.



# Usage of AI & Machine Learning in Financial Services

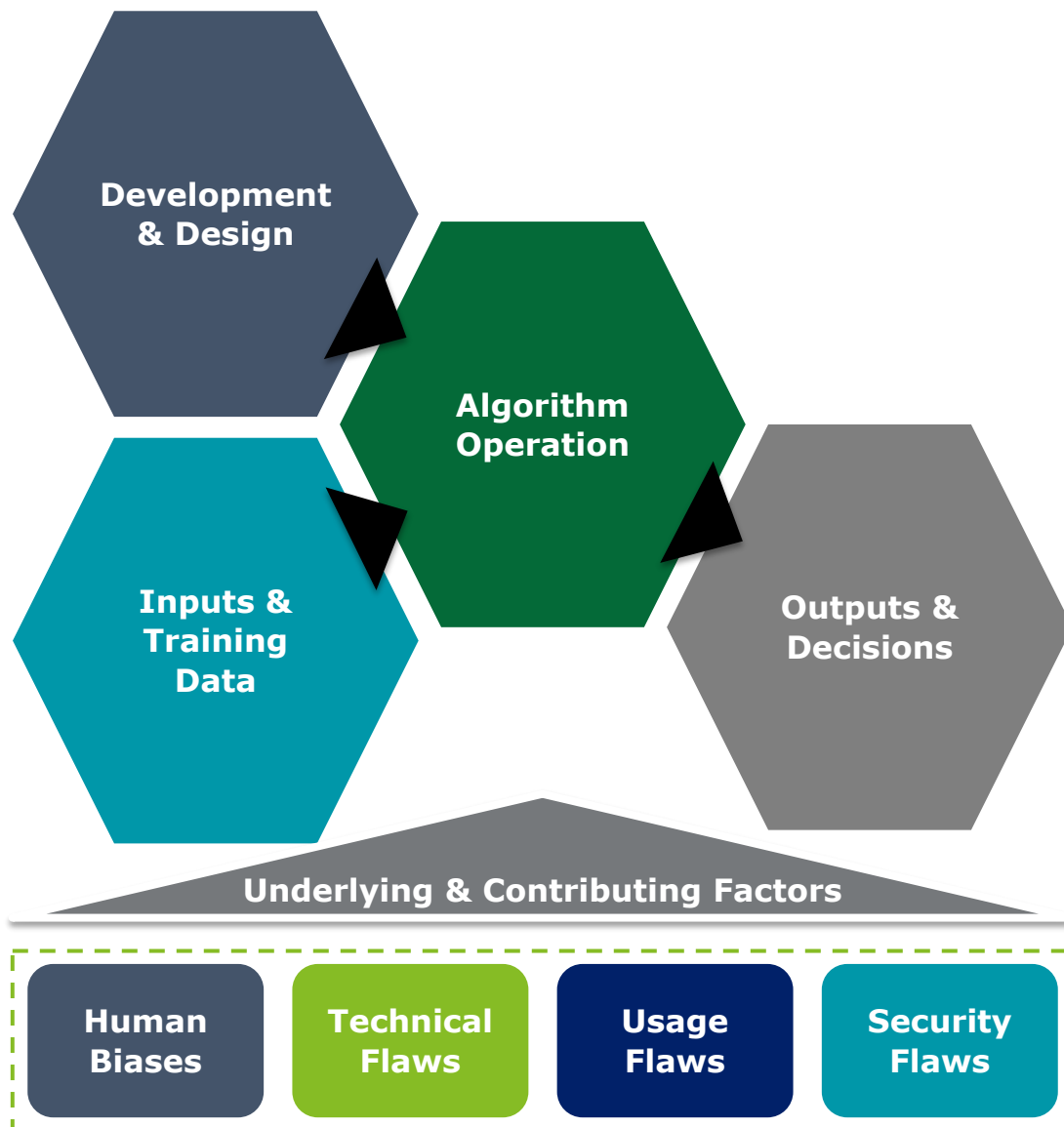
## Algorithms used to manage risks across financial services

|   | Commonly Associated Risks |            |         |              |       |
|---|---------------------------|------------|---------|--------------|-------|
|   | Regulatory                | Technology | Conduct | Reputational | Legal |
| <b>Intelligent Process Automation</b><br>Automating sets of repetitive tasks that are operationally costly. This is particularly useful in middle and back office as AI is capable of verifying, extracting and reviewing data from reports given pre-set parameters/ | ✓                         | ✓          | ✓       | ✗            | ✗     |
| <b>Fraud Prevention/AML</b><br>Applying Behavioural Profiling Analytics in Fraud Detection to determine which transactions are likely to be fraudulent, while significantly reducing false positives  | ✓                         | ✓          | ✗       | ✓            | ✓     |
| <b>Credit Decisions</b><br>Using Learning behaviours and patterns to determine an accurate representation of credit risk if a customer has limited credit history.  | ✓                         | ✓          | ✓       | ✓            | ✓     |
| <b>Personalised Marketing &amp; Communications</b><br>Offering personalized or targeted advertising/communications that are specifically tailored to an audience.   | ✓                         | ✓          | ✓       | ✓            | ✓     |
| <b>Cyber Security</b><br>Allowing firewalls to recognize patterns in web requests and automatically blocking those that could be a threat.  | ✓                         | ✓          | ✗       | ✓            | ✓     |

# Identifying risks in AI and Machine Learning Algorithms

# Identifying risks in AI and Machine Learning Algorithms

## Introducing the risk identification framework



### Introduction to the framework

- Using our insights into AI and machine learning algorithms, we have constructed a risk identification framework that organisations can use as the basis for understanding their algorithm risks.
- Despite the the complex and varied ways in which machine learning algorithms are developed, risks typically manifest across four key areas:
  - *In the development and design.*
  - *In the training data and inputs.*
  - *In the operation of the algorithm.*
  - *In the outputs of the algorithm.*
- Across the four key risk areas, human biases, technical flaws, usage flaws and security flaws contribute to embedding risks in algorithms.
- By using this framework, firms can identify and capture risks before they are allowed to cause disruption or harm.

# Identifying risks in AI and Machine Learning Algorithms

## Typical machine learning & AI risk factors

### Development & Design Risks

- A number of factors in the development and design of algorithms contribute to associated risks in algorithms. These encompass flawed modelling techniques, inappropriate assumptions and a lack of controls on more advanced machine-learning methods.
- Common development & design risks can occur due to:
  - *Flawed Modelling Techniques & Assumptions*
  - *Algorithm Bias*
  - *Overfitting*
  - *Rogue Dynamic Model Calibration*

#### Questions to consider:

- *Has the purpose of the algorithm been identified and is it sensible?*
- *Has an appropriate modelling approach been taken and has this approach been verified?*
- *Is there sufficient safeguards in place to prevent over-fitting of the data?*
- *Are there limits and controls on dynamic model calibration?*

### Inputs & Training Data Risks

- Flaws in both the inputs and the training data used to train the algorithm can introduce risks into the algorithm and lead to unintended consequences and negative outcomes. For any high-risk algorithm, it is important that the training data used is sufficient for the scope and scale of the algorithm and that the inputs are consistent with the limitations of the algorithm.
- Common inputs and training data risks can occur due to:
  - *Inadequate/incomplete training data*
  - *Inconsistent quality of inputs*
  - *Faulty Hyperparameters*

#### Questions to consider:

- *What limitations are there on the training data? How does this compare to the intended scope and scale of the algorithm's usage?*
- *Are the Hyperparameters used reasonable, given the scope and limitations of the training data set?*
- *Is there a mismatch between the input data used during operation and the training data?*



# Identifying risks in AI and Machine Learning Algorithms

## Typical machine learning & AI risk factors

### Algorithm Operation Risks

- Algorithm operation risks are those that occur when the algorithm is 'live'. They include aspects that can affect the ordinary normal functioning of the algorithm as well as security flaws that can leave the algorithm open to malicious interference.
- Common algorithm operation risks can occur due to:
  - *Implementation Risks (System Architecture)*
  - *Operational Risks*
  - *Technical Risks*
  - *Security Risks*

#### Questions to consider:

- *Given the nature, scope and scale of the algorithm, is the system architecture appropriate?*
- *Are there sufficient business continuity processes for the algorithm?*
- *Are there sufficient safeguards on both the algorithm and underlying data to prevent any malicious interference?*

### Outputs & Decision Risks

- Outputs and decisions made by the algorithm also pose significant risks. Flawed outputs can lead to significant disruption and potential legal claims depending on the nature of the algorithm. This risk factor focuses on how users are able to challenge and interpret the results.
- Common outputs & decision risks can occur due to:
  - *Lack of interpretability*
  - *Inadequate user training on algorithm functioning/operation*
  - *Failures to challenge the results of the algorithm*

#### Questions to consider:

- *Can outputs and decisions made by the algorithm be appropriately challenged?*
- *Do users of the algorithm have sufficient skills, knowledge and experience to interpret the results of the algorithm, or does the algorithm turn into a de-facto decision making tool?*
- *Could the results be biased?*

# **Managing the risks associated with AI & Machine Learning**

# Managing the risks associated with AI & Machine Learning

## Key risk management considerations

- Risk management plays a pivotal role in a firm's ability to innovate. Therefore, firms need to find ways to manage their risks whilst adopting the use of AI and Algorithms.

### Risk Management Framework

- Firms must embed AI into their Risk Management Framework; to do this they must enhance existing processes to fill the necessary gaps that emerge due to AI implementation.
- To commence the process explained above it is essential the firm:
  - a) Adapts an appropriate risk appetite;
  - b) Utilises their three lines of Defence.

### Risk Appetite

- The firm's risk appetite may need to be revisited to incorporate AI – specific considerations.
- AI solutions can inherently increase or decrease certain types of risk .e.g. model risk. The Risk Appetite needs to be reconsidered at different levels for each risk type.

### Three Lines of Defense

- Involve all three lines of defence in the management of algorithm risks. This includes: Business Lines, Risk Compliance and Internal Audit.
- As the guardians of compliance, controls and oversight; full participation in the sandbox will allow them to understand some of the critical technical aspects. Furthermore, it will help shape the start of appropriate AI governance and Risk Management policies.

Before firms deploy AI through their organisation; they should remember:

- a) That there is not a **"one size fits all"** approach to managing AI risks.
- b) Replacing manual processes with automated ones does not negate the need for appropriate governance and control frameworks.

# Managing the risks associated with AI

## What steps can firms take to implement AI risk management?

### 1. Identify

- Firms must understand their risk universe by **identifying which risk** should have a material adverse impact on their business strategy or operations.
- This process will involve:
  - a) Monitoring the internal/external operating and regulatory environments;
  - b) Ensuring the framework remains fit for purpose;
  - c) Performing periodic assessments;
  - d) Reviewing their governance and methodology.

### 2. Assess

- Firms need to **define and embed a risk assessment process** to assess the new level of risk exposure.
- This process will involve:
  - a) Constant evolution - as AI models evolve over time their assessment process must also evolve;
  - b) Adopting an agile development approach rather than a traditional development approach;
  - c) Increased engagement and sign off from a wide set of stakeholders.

### 3. Control

- Firms must **embed a control framework** to mitigate inherent risk to a residual level that is in line with the risk appetite. Ideally, the control & testing processes will need to be more dynamic.
- This process will involve:
  - a) Regular testing & monitoring of AI solutions;
  - b) Adopting a risk-based approach which will determine the appropriate level of control;
  - c) Considering how AI interacts with a wide set of stakeholders on all levels.

### 4. Monitor & Report

- Firms must design a methodology for **assessing the effectiveness of the control environment**; this must include relevant metrics for measuring effectiveness, tolerance and threshold limits.
- This process will involve:
  - a) Reporting the status of the residual risk profile, the control environment and remediation programmes;
  - b) Maintaining a dynamic monitoring approach to ensure a model is still performing as intended for its specific use case;
  - c) Regularly monitoring KPIs.

# Managing the risks associated with AI & C

## What will regulators be looking for?

### Governance, Oversight & Accountability

Supervisors will expect firms to have in place **robust and effective governance**, this will consist of:

- a) Risk exposures & associated controls being reviewed regularly;
- b) Clearly identifying the owner for each AI application;
- c) Governance committees being trained;
- d) Increased stakeholder engagement;
- e) Documenting procedures and controls in relation to manual kill switches.

### Documentation & Audit Trails

Firms should have **a clear & full overview of all AI applications** deployed through the firm; this will consist of:

- a) Testing & approval processes being documented;
- b) Processing, tracking & managing any identified issues;
- c) New variations to all existing Algorithms being documented.

### Capability & Engagement of Controls

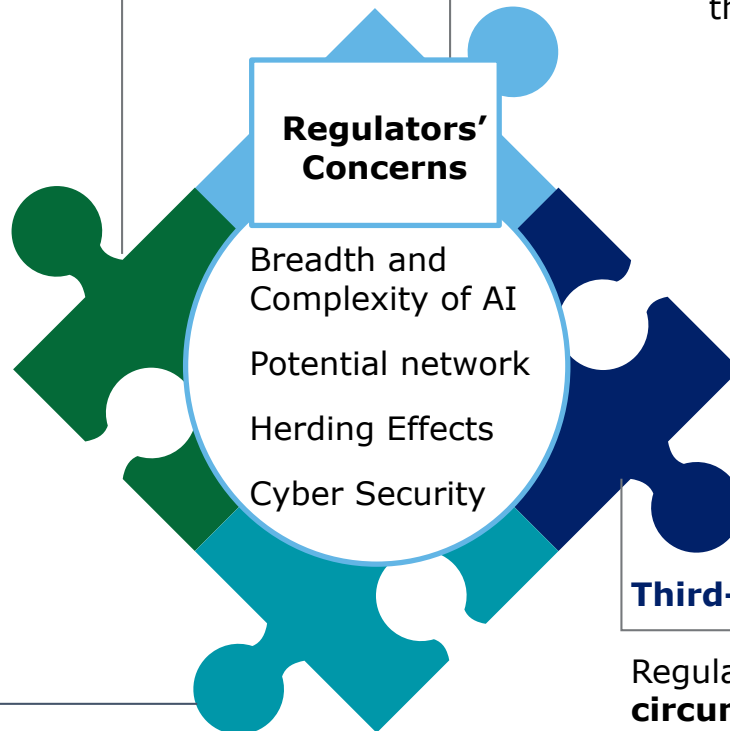
**Risk, Compliance & Internal Audit teams** must have **adequate expertise**, this will consist of:

- a) Risk & Compliance functions being meaningfully involved at each key stage;
- b) The Internal Audit team ensuring that reviews of AI applications & models are part of the audit planning and this must be a continuous process.

### Third-Party Risk & Outsourcing

Regulated **firms cannot, under any circumstance, outsource regulatory obligations to a 3rd party**; this will consist of:

- a) Designing effective Business Continuity arrangements.





This publication has been written in general terms and we recommend that you obtain professional advice before acting or refraining from action on any of the contents of this publication. Deloitte LLP accepts no liability for any loss occasioned to any person acting or refraining from action as a result of any material in this publication.

Deloitte LLP is a limited liability partnership registered in England and Wales with registered number OC303675 and its registered office at 1 New Street Square, London, EC4A 3HQ, United Kingdom.

Deloitte LLP is the United Kingdom affiliate of Deloitte NSE LLP, a member firm of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"). DTTL and each of its member firms are legally separate and independent entities. DTTL and Deloitte NSE LLP do not provide services to clients. Please see [www.deloitte.com/about](http://www.deloitte.com/about) to learn more about our global network of member firms.

© 2019 Deloitte LLP. All rights reserved.