

AI & Machine Learning Model Development Considerations

August 07, 2024

Explore the nuances between AI and machine learning and the benefits and risks associated with each.

Financial institutions (FI) of all sizes are looking to harness the power of artificial intelligence (AI) and machine learning (ML) to help increase efficiency, enhance processes, and empower their teams. In financial services, traditional modeling approaches are being assessed for replacement and/or supplemented by complex AI- or ML-based algorithms across the domains of stress testing, fair lending, fraud detection, and a host of other applications. The increasing interest and soon-to-be prevalence of AI and ML tools highlight the need for key decision makers and risk managers to understand not only the benefits of such tools but also the associated risks. This is critical because AI and ML model risk is different from traditional model risk.

AI has become a widely discussed topic, garnering much attention across industries and popular culture. This “buzz” leaves many unsure about its definition (or varying definitions), implementation requirements, and how it differs from other common modeling methodologies.

How Is AI/ML Model Development Different?

Despite often being used interchangeably, AI and ML are distinct concepts. AI is a broader umbrella term referring to technologies designed to mimic human decisions, while ML is a subset of AI. More specifically, ML is the process by which a machine observes patterns from past events to improve performance or predict future events. The nuances between these concepts can help inform decisions influencing model development activity and provide valuable insight into the risks associated with each.

Traditional model development processes are based on clear statistical and mathematical theories and assumptions. Many traditional models, such as linear regression, are simplistic in nature and often easy to interpret or explain. The number of data parameters used in a traditional model is far less than what the industry currently uses in AI/ML models. For example, common financial models utilize regression techniques, time series forecasting, and rules-based logic to drive decision-making. While these models and strategies are widely understood and applied within the industry, model accuracy may benefit from more complex AI or machine learning methodologies, which is the crossroads where the industry now finds itself. By opting for accuracy and performance, risk managers should recognize, understand, and accept the trade-off between increased accuracy and decreased explainability.

Primary AI/ML Model Development Distinctions

Purpose & Design of the Model



AI model development introduces additional model risks when compared to traditional models through the dynamic nature of AI technologies, model complexity, explainability and interpretability, bias and fairness, privacy and data security risks, IP risks, insufficient training of associates in handling AI models, and vendor model risks, among others. Financial institutions have identified complexity and explainability as challenges when considering model risk management for AI models under the existing model risk management framework and should confirm that the purpose of AI models aligns with the broader business objectives of the organization and relevant

Use of Data



FIs should consider that the development data is of sufficient quality, quantity, and diversity to support robust model development and testing. This includes designing relevant features and variables that capture the underlying connections and relevant relationships in the data. Through exploratory data analysis, model developers can identify pivotal features and potential predictors and look for any imbalances in the data. Fine-tuning the hyperparameters of the AI model using techniques such as grid search, random search, or Bayesian optimization, as well as performance metrics such as accuracy, precision, recall, and F-1 score, should be utilized. Since AI models can possess inherent bias within the training data, leading to unfair or

Testing



Many AI models, especially deep learning models, are “black boxes,” making it difficult to understand how the model arrives at its decision, and the lack of interpretability that accompanies AI models has hindered trust and accountability. In addition, AI model output is hard to assign to individual attributes due to the inherent nature of these models, which leads to questions about explainability. The output of an AI model change can be hard to assess. To help mitigate these challenges, FIs should implement rigorous validation and testing procedures to gauge the performance, robustness, and fairness of AI/ML models before deployment. For instance, FIs can use techniques such as cross-validation, holdout validation, out-of-time validation,

Adjustments



Monitoring changes in data sources and incorporating new data streams or sources, as necessary, are important considerations with AI models. FIs should consider the impact of data source changes on the model performance and recalibrate the model accordingly while also continuously monitoring and improving the data quality by performing data cleansing and anomaly detection. Also, FIs should adjust model training and validation procedures to account for improvements in data quality and continuously recalibrate the AI models to help ensure that they remain accurate and relevant over time. This can be achieved by retraining the model on recent data, adjusting model parameters, or

Documentation



The importance of maintaining detailed documentation has not changed. If anything, rigorous documentation of AI models, including

the architecture, training data, assumptions, and limitations, is even more critical in order to possess a solid understanding of the more dynamic and complex AI models. The model documentation should be regularly updated and accessible to relevant stakeholders. FIs should also communicate adjustments to the AI/ML models and the reasons

Supporting Systems



FIs should consider the implementation of systems for continuous monitoring and maintenance of AI models in production, including monitoring for performance degradation, drift detection, and security vulnerabilities. Continuous monitoring tools such as model explanation, bias detection, and performance monitoring should be built into the support framework, so there is constant oversight around the results generated from the model.

Key Takeaways

By focusing on explainability and responsible AI, FIs can help mitigate risk to their business and brand. Organizations should aim to establish an AI model development policy and standard that provides requirements and guidance to employees involved in AI model development and usage. Although not exhaustive, the representative list of action items below should be top of mind:

- Address potential risks involved in AI model development by clearly defining the purpose of the AI model, including the problem it aims to solve, the decisions it will inform, and the expected outcomes.
- Understand the expansive use of open-source and third-party algorithms and libraries and become aware of various types of third-party risks that may accompany model development.

- Work toward a balance between model complexity and interpretability, which may involve conducting in-depth tests such as sensitivity analysis, stress testing, and fairness audits.
- Develop a robust validation strategy to assist the performance and generalization ability of AI models, which is why stakeholders and risk managers should work together to effectively manage model risk for AI/ML models.

Recognizing and understanding the main distinctions between traditional models and AI/ML models is critically important for suitable model implementation and effective model risk management, as differences in model risks exist between the two types of models. Decision makers and risk managers should aim to recognize and understand these distinctions to help reduce risks to their organizations. If you have questions or need assistance, please reach out to a professional at Forvis Mazars.