Grant Thornton

Controlling AI risks in financial services

AI governance's role in controlling the risks of the cognitive enterprise

Increased use of Artificial Intelligence (AI) and Advanced Data Analytics in financial services exposes the industry to new risks. But how can financial institutions ensure that they are assessing and measuring the risk associated with these technologies? What controls do institutions need to mitigate the inherent risks to fit their risk appetite? While most companies include model, technology and data risks in their operational risk controls, they must evaluate those efforts to ensure that they have a formal risk management framework around AI algorithms and advanced predictive analytics. Establishing such a framework facilitates robust AI governance and a coherent change management strategy.

What is algorithmic risk?

Today, there is more data available across different business functions surrounding customer behaviors and transactions than ever before. Data is the most valuable asset of this century. Organizations across all industries are looking to extract actionable insights from data to function as cognitive enterprises, thus optimizing business strategies, enhancing customer experience, making pricing decisions and creating differentiation in the marketplace. Financial institutions are using AI-based systems (particularly machine learning (ML) algorithms, natural language processing (NLP) and robotics) along with advanced predictive analytics to drive success.

With the use of chatbots such as Alexa and Siri, self-learning algorithms are getting into the consumer mainstream and rapidly learning in an unsupervised manner. Google's Duplex AI uses an algorithm that can make outgoing calls to schedule appointments and uses NLP to mimic real human speech. In the next few years, most consumers will interact with banking and insurance institutions via chatbots. For example, the chatbot will go beyond the basic functions of digital banking to start a conversation about each customer's finances. Chatbots can use predictive analytics and cognitive messaging to perform tasks ranging from making payments to checking balances, paying down debt, and even notifying customers of personalized savings opportunities.

What is an algorithm?

Wikipedia defines an algorithm as an explicit specification of how to solve a class of problems. Algorithms can perform calculation, data processing, and automated reasoning tasks.

Generally speaking, an algorithm is a more generic form of a model. This term covers an extended spectrum of applications from risk quantitative models to intelligent virtual assistants.

AI algorithms have the unique characteristic to perform cognitive functions and learn how to solve problems without being explicitly programmed with a predefined set of rules.

AI is rapidly reaching business practical applications, the awareness about AI risks is limited. Business leaders and risk managers have started raising questions to understand how to govern AI, including controls over the transparency of data sources, training process and algorithms.

To gather industry insights on the emerging risk from the use of algorithms and advanced quantitative approaches, Grant Thornton collaborated with MIT Golub Center for Finance and Policy in a joint survey that reveals that applying quantitative methodologies, including advanced algorithms for modeling and analytics, is increasingly a required practice for most financial services executives to help manage risks and facilitate business decision-making.

Which of the following do you foresee implemented in your institution's risk management function?
(Number of respondents)

Source: Grant Thornton and MIT Golub Center for Finance and Policy

As management teams are incorporating AI in their strategic agendas, these algorithms gain a stronger foothold and create new challenges resulting from their ability to make unsupervised decisions in key areas. Risk managers are increasingly concerned about transparency into and unintended bias of AI, which is driving the active management of algorithmic risk.

Major types of machine learning algorithms

The most widely practical applications of AI in financial services have been centered on the use of machine learning. ML algorithms can be classified into different categories:

Supervised learning: ML algorithm is trained using training labeled data with feedback from humans to learn the relationship between inputs and a given output.

Unsupervised learning: ML algorithm that learns by exploring input data without being given an explicit output variable.

Reinforced learning: ML algorithm that learns to perform a task simply by trying to maximize rewards it receives for its actions.

Deep learning (aka Deep Neural Net): ML algorithm that operates as interconnected layers where each layer learns to transform its input data into a slightly more abstract and composite representation. While deep learning can produce more accurate results than traditional machine learning approaches, deep learning algorithms consume vast amounts of data and a require a high-performing parallel processing computing infrastructure.

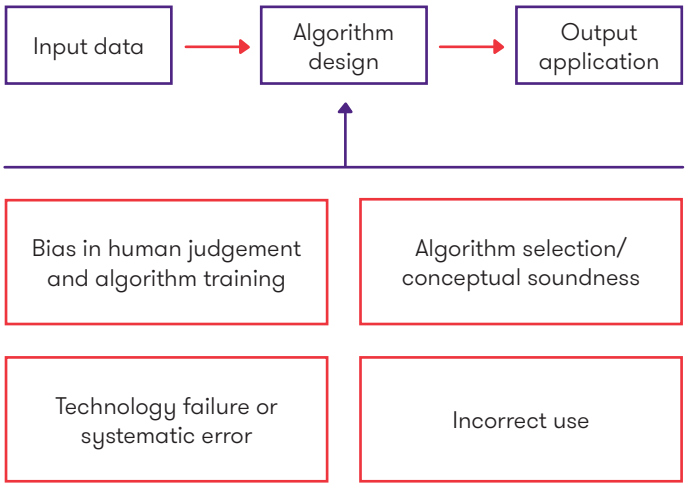
What leads to algorithmic risk?

Algorithmic risk could occur at any point during the process of collecting data, designing and training the algorithm, and applying the algorithm's output in the business setting. Algorithmic risk could also occur during implementation. To speed adoption, many companies must upgrade their backend rigid computational infrastructure. Machine learning algorithms ingest vast amounts of structured and unstructured information. A lack of synergies among integrated technologies could create implementation risk, slow down performance, and impact customer experience.

The three steps: input data, algorithm design, and output data are critical for both traditional and self-learning algorithms.

- **Data** Data is key in advanced algorithms. ML, NLP and other self-learning algorithms depend on the characteristics of their training data. However, AI data sources are often incomplete or contain unintentionally biased information. Feeding the algorithms with incorrect data is the main cause of erroneous AI outputs. For example, when the selected sample does not represent the population completely and accurately, the ML algorithm based on a biased data sample will produce a biased outcome. A fabricated data sample leads to false learning, and correspondingly, the model algorithm produces misleading predictions. Further, without controls and a rigorous design process in place to ensure data integrity, unintentional mistakes can occur.

Sources of algorithmic risk



- **Algorithm Design** Mathematical errors, programming malfunctions, incorrect logic, and the absence of rigorous controls over the design process are also causes for Algorithmic risk. Financial institutions must establish controls and a rigorous design process for model analysts/data scientists to follow, allowing for change management to oversee the algorithm design and implementation process. Otherwise, a poorly designed algorithm could result from a lack of governance and control for conceptual soundness. Management should also be cautious when using off-the-shelf vendor algorithms. One inherent risk of machine learning vendor solutions is that these applications come as a black box. Users don't understand how the ML arrived at its final solution. Institutions should design an effective test plan and robust ongoing monitoring and backtesting process for all vendor algorithms.

- **Output Application** The implementation of algorithms should be properly documented to mitigate risks due to unintended use and any ambiguity caused by the complexities of predictive analytics. The documentation should provide sufficient explanation about the training data, the characteristics of the domain, its specific techniques and the intended use of the output.

Algorithms are seldom used in isolation. The interdependencies among them could compound risks when the failure of one algorithm leads to the failure of all of its downstream algorithms. This risk is more prevalent when the upstream algorithm generates biased outcomes. A basic example of this risk would be a predictive algorithm providing a robot advisor with incorrect financial advice, and the advisor passes this inaccurate counseling onto a customer.

To avoid this type of risk, financial institutions should implement model risk management attributes, such as key controls for ongoing monitoring, regular algorithm optimization, and supervised training.

Techniques for validating machine learning algorithms

Standard validation techniques should be used when validating models that are built using ML algorithms. For example:

- Conceptual Soundness
- Ongoing performance monitoring
- Test of model overfitting/under-fitting

One main consideration when training ML models is to test for overfitting. A ML algorithm that lacks human interference tends to select abundant variables to increase the model's predictive power. Overreliance on input data could lead to overfitting based on the noise in the data.

Another concern with ML models in the financial industry is the lack of business intuition. Variables selected into the algorithm or business overlays might be restricted through a change control process. Consequently, it is difficult for the model to pass through model committees or for the end user to properly interpret the model.

How machine learning improves AML efforts

Conventional Anti-Money Laundering (AML) monitoring starts with a rule-based system, but the system comes with a high false-positive identification rate, requiring a significant investment in people and manual controls in the investigation stage. New, more robust AML solutions integrate AI and machine learning algorithms to identify consumer risk segments more accurately and efficiently in a continuously self-learning way. Integrating machine learning in the Look Back process can also provide significant benefits, including:

- Reduced number of false positive alerts.
- Significant investigation and operation savings driven by the reduced alerts.
- Identification of suspicious transactions that were not detected by the rule-based transaction monitoring system.
- Automated alert scoring, which increases efficiency and reduces manual review time.

The result? Financial institutions are able to lower compliance costs and reduce false positives while detecting more cases of money laundering activities.

Toward effective AI governance

Since the introduction of the SR 11-07 guidance during the last financial crisis, banks have focused on understanding, measuring and managing the risk of using quantitative models and logical algorithms for stress testing, liquidity and capital planning. In the Insurance sector insurance companies have been following ORSA and the Actuarial Standard Practice (ASOP) 38 to manage the model risk. In both sectors, however, there is currently no widely accepted algorithmic risk management framework. However, as more firms increase their awareness of the emerging risk, risk managers are using model risk management concepts to structure an AI governance and change management framework.

Change management and real-time continuous monitoring are crucial aspects of AI governance since algorithms are updating and learning from new information with each interaction. Accordingly, a more customized approach and agile change management strategy is required to deal with the complexities and nuances presented by advanced self-learning algorithms.

The following steps will help financial institutions speed their adoption and manage the risks of their AI journey toward being a cognitive enterprise:

- Establish an enterprise AI governance and change management framework over the use of algorithms.
- Establish an enterprise data strategy and governance strategy to enable algorithm access to data.
- Design an AI implementation blueprint that optimizes synergies among artificial intelligence, machine learning algorithms, data and computing infrastructure.

MRM & Algorithmic Risk Framework

Component	Key consideration
Risk: Algorithm data risk **Scope:** Model development and input data	Risk of incorrect or unreliable algorithms due to poor data quality, sparse data availability, missing key values, and/or incorrect value substitutions.
Risk: Algorithm bias risk **Scope:** Model development and algorithm design	AI decisions that depend on continuously evolving datasets have an inherent risk of model bias. Additional bias in inconsistent data may result in inefficient and/or unfair outcomes.
Risk: Algorithm inaccuracy risk **Scope:** Model development and algorithm design	Risk of incorrect type of algorithm(s) applied to a problem or suboptimal choice of algorithm parameters.
Risk: Algorithm misuse risk **Scope:** Model use and algorithm design	Risk that business users may lack adequate understanding of complex AI model limitations. Users may incorrectly interpret AI outputs leading to poor outcomes.
Scope: Model risk governance and controls, and output application	Risk that roles, responsibilities and accountabilities may not be clearly defined across the AI lifecycle.
Scope: Model use and algorithm design	Risk that incomplete or only periodic engagement and oversight from stakeholders in business, compliance and technology may increase the risk of impairments.

How Grant Thornton can help

Data scientists and quantitative experts on Grant Thornton's Advisory Service team can assist clients with reviewing, validating and implementing model risk management solutions. We deploy risk analytics, advanced forward-looking methodologies, and data science solutions for regulatory, business and RM decision making purposes.

Contacts

Ilieva Ageenko, PhD
Managing Director, Risk Advisory
T +1 704 632 6820
E ilieva.ageenko@us.gt.com

Jose Molina
Principal, Risk Advisory
T +1 704 632 6820
E jose.molina@us.gt.com

Grant Thornton

GT.COM