Deloitte.

Managing model and AI risks in the investment management sector

Enhancing model resiliency

Increasing focus on managing model risk: exploring investment managers' motivations

The investment management ("IM") industry is currently undergoing a transformation to harness **the power of data and analytics to drive strategic and day-to-day decision-making**. To capitalize on this transformation and enhance the speed and accuracy of the decision-making process, **investment managers are increasingly relying on models and complex algorithms for a host of activities**. These include investment decisions, risk management, and business operations.

This paper discusses the leading practices in IM organizations of enhancing model resilience and managing the related risks. This includes **new emerging risks** that are introduced with the adoption of **generative artificial intelligence (AI) models** and increasing **institutional interest in investing in digital assets**.

Models are pervasive in the IM industry and are used to facilitate important business activities, such as asset allocation, algorithmic trading and portfolio rebalancing, market and liquidity risk management, and regulatory compliance, to name a few. Models exist across the enterprise, drive competitive advantage, and achieve operational efficiencies. Hence, **investment managers are becoming more interested in comprehending the sources of model risk** and implementing controls to mitigate these risks while still allowing enough flexibility for business operations.

Moreover, investment managers are **under pressure** from investors and boards of directors to **boost risk oversight and model performance reporting**. Managing model risk enhances investor confidence and trust, as investors rely on investment managers to make sound decisions on their behalf. If models are not effectively managed, flawed predictions and erroneous decisions can erode investor trust and damage the reputation of investment firms.

Further, the **recent technology developments leading to massive data availability and the adoption of complex AI solutions**, are resulting in fundamental shifts in the business operations. These transformations may serve as catalysts for modernizing data infrastructure, enhancing risk management platforms, and refreshing risk reporting tools. Models play a fundamental role in developing and automating these processes.

> "The essence of investment management is the management of risks, not the management of returns."
>
> **— Benjamin Graham**

Model control failures and lack of appropriate disclosures may result in significant **regulatory penalties, financial losses, lost clients, or damaged reputations**. Although IM is one of the financial sectors with limited regulatory oversight related to models, there are several regulatory rules that mandate enhanced governance for data and risk modeling frameworks (e.g., SEC 22e-5, 2a-5, 18f-4). Additionally, regulators including Financial Industry Regulatory Authority (FINRA) and the Securities and Exchange Commission (SEC) have also issued industry guidance specifically related to the use of robo-advice models. Given the increased attention to models by investors, stakeholders, and regulators, investment managers need to **proactively design and implement risk governance practices that enhance models' resilience** to mitigate the strategic, regulatory, and operational risks for business.

Defining model risk and model risk management for investment managers

There is no industrywide "model" definition, but banking and securities regulators define a model as being "a quantitative method, system, or approach that applies statistical, economic, financial, or mathematical theories, techniques, and assumptions to process input data into quantitative estimates." Investment managers can use this definition and tailor it to align with their organization's business considerations, model-use environment, and risk appetite. "**Model risk**" can thus be understood as the risk of experiencing monetary loss, harm to clients, erroneous performance or risk metrics, improper investment or managerial decisions, or damaged reputation, resulting from poorly built, used, or controlled models.

To mitigate the model risk, **Model Risk Management (MRM)** is a discipline of risk management that provides a structured approach across the model lifecycle. MRM helps to define the shared roles, responsibilities, and accountabilities (inclusive of decision rights) across business functions, and facilitates the development of an effective control environment, including policies, procedures, and corollary controls.

MRM offers tools and accelerators that can be customized based on the organization's business and risk profile, helping to design a model risk framework that will be different for each investment manager as there is **no "one-size-fits-all" model risk framework**. Investment managers that are interested in setting up an MRM framework should consider stakeholders from across the organization and identify the underlying factors of model risk. This includes the nature, number, and riskiness of existing models, and the existing control environment. Depending on the nature of the model-use environment and degree of existing MRM activities (formal or informal), investment managers can operate through a spectrum of MRM programs offering basic MRM "tables stakes" to a more advanced MRM "leading the industry" services and establish a plan or road map to achieving the MRM program that fits their business and risk appetite.

Leading modeling practices in the IM industry and risks associated with the model use

Overview

To establish a sound and resilient model framework, the first step for investment managers is to understand the organization's model environment. IM firms may develop their own modeling approaches based on their investment strategies, client base, and risk appetite. As the industry continues to make headway, data, models, and supporting technologies provide new opportunities for firms in pricing, alpha generation, portfolio optimization, risk quantification and monitoring, performance analysis, and daily operations. Effective business operations, robust performance, and risk management are essential for developing a sustainable growth in today's competitive environment.

The leading modeling practices in the IM sector aligns along the following five pillars: **data quality assurance, technology transformation, model development, model operations and lifecycle management, and performance evaluation and reporting**. These five focus areas lie at the core of modeling practices and encompass a host of activities impacting the model operating environment. The examples presented in table 1, provide insights to a variety of leading practices observed in industry, across the model lifecycle.

Commonly observed model-related deficiencies

In our experience and based on industry insights, there are a few common model deficiencies prevalent across the industry that can be catered by these five focus areas.

Model issues may occur due to inaccurate or incomplete data, and quality issues caused by manual input processing, leading to unreliable analytical results. Furthermore, technology infrastructure constraints, challenges in retiring legacy systems, or limited awareness of emerging risks associated with the use of AI models may lead to failure of models and potential financial losses. Other sources of model risks may stem from erroneous model assumptions and misalignment of model methodology with business logic or market reality.

The proliferation of models in the IM industry has increased the need for streamlining model development and model operations. Data drift between development and production data could impact the model validity. Lagged reporting, lack of proper granularity, and exposure coverage have put greater emphasis on timely and adequate performance evaluation and reporting requirements. With an increasing number of models, it is difficult for firms to track performance on an individual basis and track the need to begin implementing systematic strategies and deploy teams to manage them.

Table 1. Five pillars of the leading modeling practices in investment management industry

	Focus area	Examples of leading practices
Data quality assurance	Data is the foundation of model or algorithm development. Front-runner funds are managing data quality at volume using a rigorous and highly structured approach with a strong emphasis on data quality assurance processes, as poor data quality can lead to inaccurate and unreliable model results and potentially financial losses.	• **Automated data quality assurance metrics** by integrating data quality checking procedures with data ingestion process and use of quantitative and statistical metrics to identify outliers, missing values, changes in volatility patterns, and abnormal values detection. • **Ongoing monitoring** by implementing processes to timely monitor, track, and report data failures and error detection results. • **Data remediation** to resolve issues related to inaccurate data, identified in data pipelines, when reconciled against a "golden" dataset (considered as the source of truth). • **Quality reporting and data signoff** to communicate and summarize the performance of a data pipeline at each stage. Obtain data signoff procedure from downstream data users, as required.

	Focus area	Examples of leading practices
Technology transformation	Technology has provided an edge for investment management firms. However, leveraging innovative technology introduces risks for investment managers. Hence, firms are placing strong emphasis on streamlining their deployment and increasing the amount of governance placed on new infrastructure to manage these risks.	• **Scalable solutions such as cloud migration** to increase the extract, transform and load capability, optimize computation costs, and augment storage capabilities. • **Model automation tools** such as automated machine learning (i.e., DataRobot, H2O.ai) allows for efficient model development, including expediting processes for benchmarking and assessing model performance. • **DevOps infrastructure** to develop and deploy recent advances in the software engineering and project management technology, which is very efficient and at volume (DevOps, Jira, GitHub, Bitbucket, and other varied continuous integration tools). • **Standardize software release processes** for internally developed application programming interfaces and software and create a central document repository.
Model development	The model development process involves theoretical and comprehensive research, data acquisition, and reliable performance testing.	• **Comprehensive academic and industrial research and development** has become the core in the modern investment industry, applying state-of-the-art theory in profit generating and risk management. • **Use of nontraditional/alternative data** to develop trading and wealth management models is a widespread practice. • **Detailed model performance testing**, back testing with latest and/or stressed market data, and portfolio by industry leaders to assess model reliability. Establish error tolerance/thresholds to escalate model issues.
Model operations and lifecycle management	The model operations process can be described by a set of practices that enables a smooth and robust transition between model development, testing, and production for analytical/quantitative models.	• **Continuous testing** to assess if models work as expected. • **Continuous integration** to test and monitor if the developers team works on the same code base. • **Continuous delivery** involves pushing incremental (often small) changes to production in shorter cycles. • **Tracking real-time performance** includes testing and monitoring the performance of a model in real time by creating metrics to summarize and identify where there could be potential issues.
Performance evaluation and reporting	Comprehensive risk reporting provides firms with the required information to identify potential areas of concern and assess if risks are being managed appropriately.	• **Performance and risk metrics** to monitor portfolio performance (i.e., Sharpe ratio, information ratio, Sortino ratio, drawdown, Value at Risk, expected shortfall, capital utilization, stressed losses) to help assess the risk and return characteristics of their portfolios and make informed decisions. • **Dashboarding and reporting** to review position, profit, and risks at various levels of aggregation, designed to cater to the circumstances and requirements of various stakeholders, including portfolio managers, risk managers, board members, external investors, and regulators.

Leading practices in enhancing model resilience

Rigorous model development processes, a broad model testing and evaluation approach, and an effective model operations framework serves as the cornerstone for an organization's robust model environment. This section explores leading practices to enhance model resiliency with a focused lens on AI models.

Rigorous model development

The model development process should include a rigorous set of steps to solve a problem using data and analytics. The leading practices in the industry place strong emphasis on the problem definition as a first step to fully understand the business issue.

Model developers should perform a thorough review of academic literature, data collection, and data preparation to ensure that data is properly collected, processed, and relevant to the population for use. Further, developers should perform a model selection, parameters calibration, and model outputs evaluation to assess if the model is fit for purpose. Figure 1 further illustrates the specific steps of the model development process.

Systematic and independent model validation

Another critical process to ensure robust model outputs is by performing systematic and independent model validation, to assess whether the model is developed in line with the intended use and purpose and consistent with leading industry practices. **Model validation plays a crucial role for investment managers in determining the accuracy, reliability, and appropriateness of the models and their use in the investment decision-making processes**.

Model validation activities may be tailored to the specifics of the model. For example, when assessing the conceptual soundness of a machine learning model, the activities can be expanded to include the review of model selection with respect to speed, predictive accuracy, robustness, scalability, and business applicability. This is in addition to the conventional testing performed to assess the conceptual soundness of the modeling approach, the quantitative and qualitative variables, or judgmental factors.

Similarly, while assessing the input data and model assumptions, model validations may focus on data extraction, transformations, feature engineering, algorithm manipulation, and hyperparameter tuning. Periodic monitoring of model performance is required to assess the model staleness, data drift, slow leaks, slow bias, and variance.

Efficient model operations (ModelOps) and machine learning operations (MLOps)

Expanding on our understanding of leading practices, **MLOps** is an engineering framework of tools and practices used to streamline and manage the lifecycle of machine learning (ML) models in the production environment.

Figure 1. Business model strategy

1 Define and design

- Identify the problem that needs to be solved.
- Perform initial research on the model feasibility, candidate methods, industry leading practice, etc.

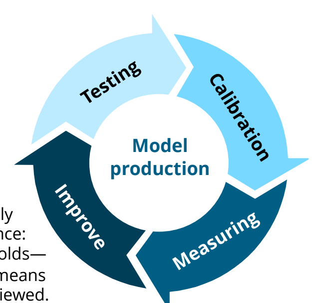
2 Data collection

- Identify appropriate data sources including vendors, internal or alternative datasets.
- Assess the data quality, accuracy, appropriateness, and completeness.
- If feasible, use multiple sources to validate the accuracy and reliability of modeling data.

3 Model formulation (prototype)

- Review literature.
- Assess the universe of variables, and discuss the model/product segmentation, variable selection, and data transformation process.
- Build candidate models; perform evaluation on model outputs, compare statistical properties of candidate models, and provide a rationale for the final model.

4 Model production



Design a plan to systematically monitor a model's performance:

- Define metrics and thresholds—metrics that, if breached, means the model needs to be reviewed.
- Define roles and responsibilities: Assign team members to monitor specific models.
- Define processes to identify when a model will be recalibrated (e.g., for regime shift, etc.).

Timely measure and calibrate the model outputs based on the latest data and predefined metrics/thresholds, enhancing the model or controlling performance degradation as needed. This can be implemented with automated testing procedures to increase efficiency.

Despite being a poplar tool for managing ML model operations and lifecycle, the approach proposed by MLOps could be adopted for a broader category of models, such as risk models. When the framework is expanded to include model governance processes, it is branded as **ModelOps**.

Organizations encounter several challenges during model production implementation, deployment, and operations stages, which results in a large number of ML models that are developed and not deployed. This includes building a scalable infrastructure for complex data storage and data preparation, lack of continuous integration, optimization of hyper parameters, test automation, and intrinsic software development operations such as version control and proactive notifications. Furthermore, models and AI systems often require allocating resources on an ongoing basis for model performance monitoring purposes.

Following are the core components of an MLOps value chain.

Planning

- **Data acquisition**: Define the required data and collect from appropriate sources.
- **Stakeholder coordination**: For internally sourced datasets, identify the data owners and data infrastructure, existing users, and proposed users of the data, and agree upon how the data will be used.

Data preparation

- **Database selection**: Plan the type of databases based on the speed and ease of access requirements, maintenance efforts, and the frequency of requests that will be made to the database.
- **Data quality**: Continuously apply tests to the data before downstream models ingest it.

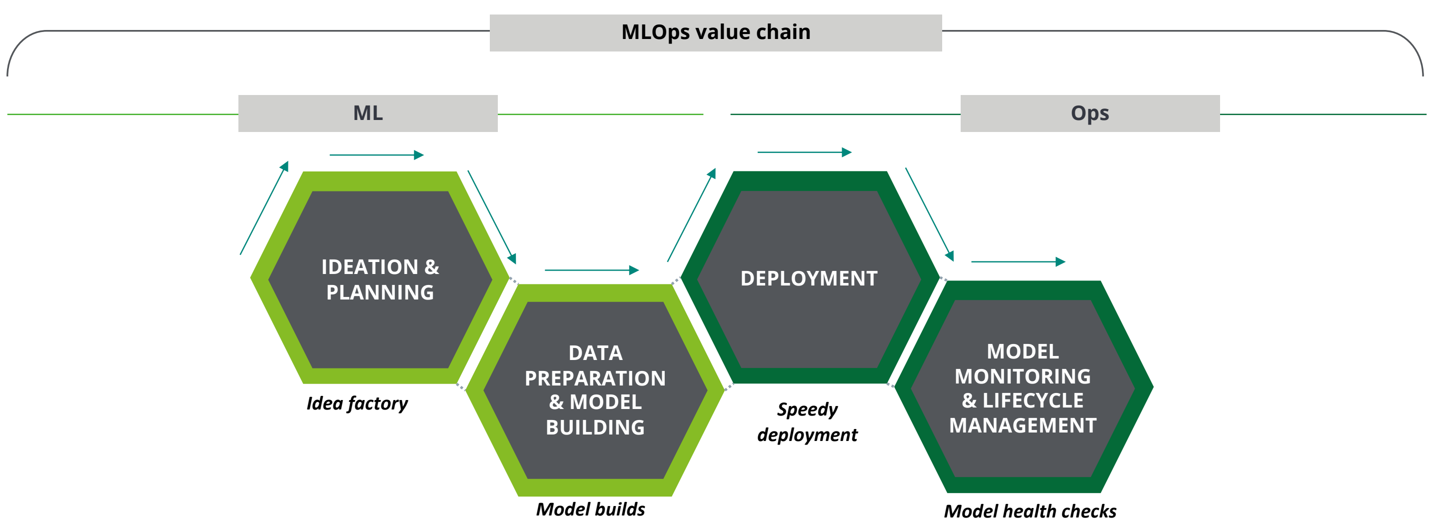
Deployment

- **Data and model infrastructure**: Select the appropriate technology stacks based on the production need, speed, and cost.
- **Automation**: Automate code testing, code delivery to production, and escalation process as needed.
- **Continuous delivery**: Push incremental (often small) changes to production in short cycles.

Model monitoring and lifecycle management

- **Model metadata**: Define metrics to monitor in production, including successful execution and timeliness of the script.
- **Model governance**: Define roles and responsibilities for stakeholders to manage the data preparation and deployment of the model.

Figure 2. MLOps chain processes



Beneath the surface: effective approaches to manage emerging risks related to generative AI

Recent technologies and evolving market trends present a wide range of opportunities in the investment management industry. With that, as new risks emerge, a notable example is the risk associated with the use of **generative artificial intelligence tools**.

Generative AI is a form of artificial intelligence that leverages open- or closed-source datasets to generate content across various modalities (e.g., text, images, audio, code, voice, video).

Generative AI: Investment management use cases

Generative AI is poised to bring a revolutionary transformation to the investment management industry.

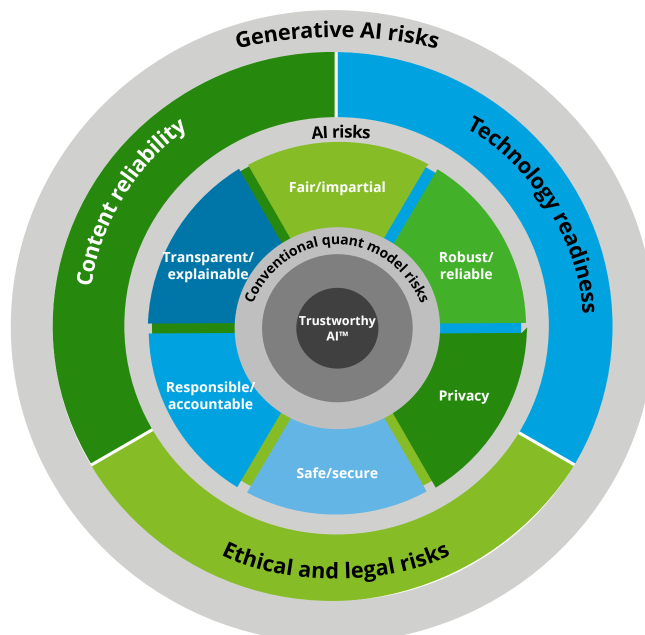
One of the specific areas where generative AI is having a significant impact is in generating investment insights and recommendations. By analyzing vast amounts of financial data, market trends, and historical patterns, generative AI models can identify innovative investment strategies tailored to specific goals and risk preferences. These AI-generated strategies can help investment managers discover new opportunities, optimize portfolio allocations, and potentially outperform traditional investment approaches.

Moreover, generative AI can assist in time-consuming tasks, such as data processing, report generation, and compliance summary and checks. By utilizing generative AI tools, investment professionals can streamline their workflows, freeing up valuable time and resources to focus on higher-level decision-making and client interactions. This increased efficiency and automation can lead to improved operational scalability and cost-effectiveness within the IM industry.

Further, domain-specific large language models (LLMs) can be customized for different areas of the firm and have demonstrated substantial performance improvements over generic LLMs.

Generative AI can play a significant role in financial risk management within the IM industry. By analyzing historical market data and simulating various scenarios, generative AI models can help investment managers identify and mitigate potential risks. These models can provide insights into market volatility, stress testing, and potential downside scenarios, enabling investment managers to make informed decisions and manage risks more effectively.

Figure 3. Generative AI risks



Managing risks associated with generative AI

Due to the powerful analytical capacity and the ease of use and deployment, generative AI is disrupting many economic and business sectors, while introducing risks such as market manipulation, ethical considerations, and intellectual property concerns.

It is crucial for investment managers to thoroughly assess and understand the emerging risks associated with generative AI. These are a **broader set of risks than those associated with AI in general** (figure 3).

Organizations that aim at managing generative AI risks should consider beginning by managing the risks already identified with "traditional" AI. These risks can be mitigated by addressing model risks such as the potential for bias in data or models, or lack of accuracy of the output. This is in addition to ethical considerations, data privacy, and safety issues. Investment firms need to determine the proper oversight, validation, and monitoring of generative AI systems to maintain transparency, fairness, and accountability in their operations.

Generative AI technologies have a tendency to amplify the exposure to certain risks that were previously identified as AI risks. For example, data bias and fairness risks are much more acute for generative AI, given that LLM models are trained on large amounts of historical data that are by nature biased.

In addition, there are specific generative AI risks that are due to their individual characteristics and capabilities. Two notable examples are the generative AI feature of producing hallucinations and the generative AI ambiguity about content attribution and copyright, and hence the risk of plagiarism.

By considering the following risk focus areas of **fairness, reliability, transparency, accountability, privacy, and security**, organizations will be able to design a robust governance framework that mitigates effectively the risks associated with AI and generative AI, in particular (figure 4).

By embracing generative AI technologies responsibly, investment management firms can gain a competitive edge, provide more value to clients, and adapt to the evolving landscape of the industry.

Figure 4. Managing AI risks

	Responsible / Accountable	Privacy	Fair / Impartial	Transparent / Explainable	Safe / Secure	Robust / Reliable
AI Risks	! Poor AU/data/model oversite driven from ambiguous and overlapping responsibilities in the organization ! Uncontrolled changes to models may lead to technology failures or poor model outcomes	! Unapproved sensitive data used in AI/ML pipelines ! Lack of data privacy governance in AI strategy may lead to potential sensitive data risks ! Unintended data use by third-party model vendors or APIs can lead to strategic risks	! Unfair or biased outcomes when utilizing certain demographic data that may be correlated with a protected class ! Under/over representation of certain parts of population when AI is trained on incomplete data population	! Model complexity and architecture may make model behavior difficult to understand or explain (e.g,. multilayered neural networks) ! Complex feature transformation can result in obfuscation of original data attributes yielding difficult to explain outcomes	! Prototype code on unofficial infrastructure may be vulnerable to cyber threats ! Unauthorized usage of data in AI systems may lead to legal risks (e.g., usage of data beyond consented time period or applications may be perceived as authorized)	! Data treatment to address poor data quality(e.g., missing data, outliers, etc.) may impact the model outcome ! Model degradation due to changes in underlying data leads to poor performance
Model Lifecycle	Feasibility	Discovery	Modeling	Acceptance	Integration	
AI Controls	! All models should be initiated and managed through a centralized inventory, with a dedicated change control function, with accountability assigned to key stakeholders	! Application-based data pull controls in model environments and limited sensitive data transfer to third-party environment ! Data usage complies with privacy notices ! Sensitive data is encrypted, masked, etc. prior to experimentation	! Perform fairness testing and analyze event rates across multiple classes of the demographic indicators or proxies ! Cross-validation testing and stability analysis	! Utilize model-agnostic interpretation methods to generate model explanations and increase interpretability ! Document data scientist decisioning on feature engineering choices ! Assess impact of data quality treatments	! Model development and validation documentation should contain evidence conformance to security standards in place ! Complete vulnerability and penetration testing of production system	! Include ongoing monitoring of model performance to ensure the model performs as intended using pre-defined thresholds and ranges of acceptable performance ! Apply input data quality monitoring

On the horizon: managing model risk related to digital assets

Another area that is gaining significant attention, especially in the investment management industry, is the emergence of cryptocurrencies and digital assets. While they offer potential benefits like decentralized transactions, new investment opportunities, and portfolio diversification, they also present specific **market risks** such as **high volatility and price uncertainty**, in addition to regulatory uncertainty, liquidity challenges, security, and cyber risks.

Modeling risks associated with digital assets

As institutional interest in investing in digital assets continues to rise, there are **additional financial risk management** challenges to consider. **Market risk models designed to evaluate the risks and returns of traditional financial assets do not address the idiosyncrasies of risk factors of cryptocurrency and digital assets** as an alternative asset type. Price discovery is a particular challenge for cryptos, as there is no "tangible and real" asset under the tokens. In addition, limited liquidity and fragmented markets for certain cryptos with smaller market size make **valuation methodologies inadequate to estimate the market value for instruments based on digital assets**. Data inconsistencies between exchanges and poor data quality may render the digital assets market very inefficient, by creating arbitrage opportunities.

Figure 5 outlines the specific **challenges of modeling and valuating digital assets** along with examples of risk mitigating techniques, highlighting the need for a broad risk management framework, advanced data analytics capabilities, secure operational processes, and proactive engagement with regulatory developments to address the individual complexities associated with digital assets.

Figure 5. Modeling considerations for digital assets

Key challenges

Valuation and risk management challenges
Due to the nature of the high volatility and intercorrelations in crypto assets, it is challenging to valuate, set risk appetite, and design hedging strategies for them; as a result, though there are derivatives available to hedge certain market risks, valuation of these derivatives are less straightforward because the underlying prices are usually contingent on demands rather than an innate value of a "real" asset. Traditional market risk models may fail (e.g., conventional stress test may not work due to the weak linkage to macro variables).

Fragmented cryptocurrency data and integration challenges
Echoing to the enormous types of coins, the data distribution channels are highly diverse as well, given that there are thousands of exchanges generating trading information. When liquidity is low, there can be considerable spreads from different market data sources, which may create challenges in price finding and data ingestion/integration into funds' internal systems.

Operational, regulatory, and legal challenges
There is no international consensus on the regulation of cryptocurrencies. Regulators continues to take "a careful and cautious approach" to firms to handle exposures to cryptocurrencies; however, the industry does not have a clear view on regulatory requirements. In addition, there are security concerns in digital asset custody as there can be additional cyber risks for virtual assets.

Principles to mitigate the risk

- **Hedging strategies development and review**
- **Market data quality control and data model design/review**
- **Algorithm and code review and quality assurance**
- **Risk metrics design and development**
- **Valuation review and testing and PnL analysis**
- **Establish crypto risk management governance, processes, and controls**

Conclusion

The paper explored the various sources of model risk, provided insights into the leading modeling practices in the investment management industry along with tailored solutions to tackle the ever-evolving areas of risk with a conscious effort toward acknowledging recent technologies and market trends.

By recognizing the importance of model risk management and taking appropriate actions, investment managers can navigate the complexities of the industry, adapt to changing market dynamics, and strive for sustainable long-term achievements.

How can Deloitte help?

As global leaders in providing professional services to the US Investment Management industry, Deloitte assists clients with addressing a range of critical issues brought on by regulatory changes, competition, globalization, advances in technology, and the changing demands of their customers. We have a long and distinguished record of serving thousands of mutual funds, registered and unregistered hedge funds, investment advisers, and funds of funds.

Deloitte's Trustworthy AI framework is designed to help organizations implement an ethical framework, as well as identify and mitigate potential risks related to AI ethics at every stage of the AI lifecycle. With more than 400 model risk management professionals, Deloitte has helped organizations of all sizes design, implement, and execute their model and AI governance programs. Our team includes former regulators, academics, industry modeling specialists, data scientists, programmers, and risk professionals.

Contacts

Krissy Davis
US IM Practice Leader | Risk & Financial Advisory
Deloitte & Touche LLP
kbdavis@deloitte.com

Clifford Goss, PhD
Partner | Risk & Financial Advisory
Deloitte & Touche LLP
cgoss@deloitte.com

Anca Ferent
Senior Manager | Risk & Financial Advisory
Deloitte & Touche LLP
aferent@deloitte.com

Contributors

Dan Han
Manager | Risk & Financial Advisory
Deloitte & Touche LLP
danhan6@deloitte.com

James Stanley
Consultant | Risk & Financial Advisory
Deloitte & Touche LLP
jamstanley@deloitte.com

EJ Donelson
Analyst | Risk & Financial Advisory
Deloitte & Touche LLP
edonelson@deloitte.com

Palak Kaur
Senior Consultant | Risk & Financial Advisory
Deloitte & Touche Assurance & Enterprise Risk
Services India Private Limited
palkaur@deloitte.com

Deloitte.