CAMBRIDGE ASSOCIATES

INSIGHTS

ODD IN FOCUS

Artificial Intelligence Usage Governance and Compliance

Published March 31, 2026

Overview

As artificial intelligence (AI) reshapes how investment managers conduct research and streamlines a wide range of operational processes, the governance frameworks surrounding its use have become a defining factor in assessing operational risk. One of the key areas reviewed during operational due diligence (ODD)—a critical part of the manager selection process—is a manager's information security controls. ODD now evaluates if a manager's use of AI and if the accompanying governance measures in place, including the policies and controls, appear sufficient to adequately safeguard proprietary and confidential information.

Why

- The adoption of AI by investment managers introduces risks and governance challenges. Model errors—instances in which AI tools generate false or misleading output—can occur where AI tools generate false or misleading output. Managers may inadvertently expose confidential or proprietary information when using AI tools, as this data can be stored, used for future model training, and potentially reappear in responses to other users. If not appropriately controlled and monitored, these vulnerabilities can lead to operational failures, cybersecurity risks, regulatory violations, or reputational damage, directly impacting investors.
- AI governance practices can vary significantly depending on the manager's size. Emerging managers, particularly those still building out a fully institutional infrastructure, are more likely to rely on open access models with fewer restrictions to safeguard sensitive data. These firms are less likely to implement secure, bespoke AI solutions or invest in staff training. and. In contrast, larger managers tend to enforce stricter controls and invest more in staff training, with some developing proprietary models. This disparity highlights the need for enhanced governance frameworks and ongoing training to ensure responsible and secure adoption of AI technologies.[1]
- Transparent disclosure of AI usage to investors is increasingly important as regulators have increased their focus on AI-related claims and have pursued enforcement actions against firms that made misleading statements about their AI capabilities or usage in investment processes. This underscores the need for accurate representation of AI adoption.

How

- Robust data governance and verification of AI outputs are essential. Without strict controls to validate outputs and prevent unauthorized access or inadvertent disclosure of confidential, sensitive, or material non-public information (MNPI), both the integrity of investment decisions and the security of sensitive data may be compromised.
- Operational failures and data breaches are more likely if controls around access management, output verification, and staff training are weak or absent, allowing errors or unauthorized use to go undetected.

The Cambridge Associates Business Risk Management Group contributed to this publication.

ODD risk potential: Medium

- Although AI adoption introduces significant data governance risks—especially in environments with weak controls—these risks can generally be mitigated through robust governance frameworks, strict data controls, tailored employee training, and effective oversight of AI outputs. The regulatory environment surrounding AI use in the asset management industry is still developing and lacks specific, standardized rules. As such, ongoing monitoring of regulatory guidance and industry best practices is essential.
- Risk assessments will vary based on the manager's AI use, as well as the strength of the governance controls and oversight in place.

Manager relevance

AI technologies are being adopted across asset classes and manager types to support diverse functions. Investment teams use AI to enhance research and streamline analysis, while compliance and legal teams employ it for tasks like compliance testing and surveillance that involve processing large data volumes. Client-facing teams may use AI to generate marketing materials and respond to due diligence questionnaires and requests for proposals (RFPs).

HEDGE FUND MANAGERS: Hedge fund managers are frequently at the forefront of adopting advanced technologies—including AI and machine learning—to identify trading opportunities, optimize portfolio construction, and enhance research and administrative processes. Without robust governance and control frameworks, there is an increased risk of operational failures, model errors, and unintended consequences from AI-driven decision making.

PRIVATE FUND MANAGERS: Private managers may leverage AI and machine learning to support deal sourcing, due diligence, portfolio monitoring, and operational efficiencies. The integration of these technologies can introduce risks related to the handling and analysis of confidential company data and proprietary information.

LONG-ONLY FUND MANAGERS: Long-only managers—particularly those managing large, diversified portfolios—may use AI and machine learning to support investment research, portfolio construction, risk management, and client reporting. In instances where long-only managers serve a large client base across many different products, appropriate human oversight is essential to ensure accuracy and quality of AI-generated information distributed to clients.

Key Control Review

A thorough review of key controls is essential to ensure that confidential and proprietary data are sufficiently protected. Three main areas of focus are incorporated into reviews: a review of internal processes, clear documentation of policies, and strong compliance oversight mechanisms. By examining these controls, we can better assess whether a manager's governance framework is robust and protects investor interests.

#1 Internal processes

- Establish a formal approval process for onboarding new AI tools, including required due diligence, risk assessments, and sign-off from compliance, legal, and IT teams.

- Conduct thorough due diligence on all AI tools and models prior to implementation, including assessment of vendor reputation, technology capabilities, and security protocols.
- Understand how manager and client data will be accessed, used, stored, and protected by the AI solution. Assess the AI provider's data security protocols, such as encryption, access controls, and compliance with data privacy regulations like GDPR.
- Conduct ongoing monitoring and periodic reviews of AI tools to identify emerging risks, ensure continued compliance, and adapt to changes in technology or regulation.
- Block the use of prohibited or unauthorized AI tools on firm equipment and networks.
- Restrict all internal development work to a segregated environment and require testing and review before going live when using third-party AI tools for coding purposes.
- Track version prompts for critical processes, as large language models can be sensitive to even minor changes.

#2 Documentation of policies

- Maintain clear, accessible, and documented policies governing the AI use by staff, including explicit guidance on acceptable and prohibited uses.
- Customize policies to accurately reflect the firm's specific AI use cases and operational practices. The policies should address how data is collected, stored, and managed throughout the AI workflow. This includes maintaining proper audit trails for AI-generated insights and managing proprietary data used for model training.
- Review and update policies regularly to ensure they remain relevant and effective amid the rapid evolution of AI technologies.
- Publish and regularly update a list of approved AI tools and platforms, ensuring staff are aware of which solutions are permitted.
- Define what types of information may be input into AI tools, with strict prohibitions on entering confidential, sensitive, or MNPI into unapproved or unsecured platforms.
- Require that all output generated by AI tools are subject to human review and validation.
- Document procedures for monitoring and auditing AI tool usage, including escalation protocols for policy breaches or incidents.

#3 Compliance oversight

- Provide regular staff training on responsible AI usage and raise awareness of core risks such as hallucinations and data privacy concerns. Advanced and tailored training, based on roles and level of expertise, in prompt engineering can also be provided to help employees generate more accurate and relevant AI outputs.
- Require that AI usage and adherence to related policies are included in the firm's annual compliance attestation process, ensuring all employees formally acknowledge their understanding and compliance.

— Implement ongoing surveillance and periodic audits of AI tool usage, including review of access logs, data inputs, and outputs, to detect and address any policy breaches or inappropriate activity.

— Review key vendor agreements to understand and document how firm data is accessed, used, stored, and restricted within vendors' internal AI systems, ensuring contractual protections are in place to safeguard sensitive information.

Case studies

Case studies provide valuable insights into the real-world applications of AI and the governance measures employed.

Hedge fund 1 (HF1)

Summary	Description of controls
— HF1 employs machine learning and natural language processing across the business. Non-investment teams use these technologies for data mining, classification, cyber defense, and communication surveillance, leveraging both off-the-shelf and proprietary solutions. Systematic investment teams apply AI for entity recognition, sentiment analysis, and key steps in predictive modeling. — HF1 has developed a proprietary system as a centralized access point for AI services.	✓ Only AI tools that meet onboarding criteria (data protection, cybersecurity, ethics, and testing) are made available through the proprietary system. ✓ Legal, compliance, and IT teams collaboratively define and enforce onboarding criteria for AI tools, ensuring comprehensive oversight of contractual, data security, and ethical considerations. ✓ HF1 enforces robust policies and guidelines for safe AI usage. Employees must complete compliance training before accessing the centralized platform, ensuring they understand system controls, best practices, and potential risks such as AI fabrications.

Hedge fund 2 (HF2)

Summary	Description of controls
— HF2 is actively pursuing multiple AI implementation projects across the firm. The manager has enabled AI and machine learning experimentation for researchers and adopted advanced AI tools. — Machine learning and robotic process automation are integrated into operational processes like cash reconciliation processes.	✓ An AI usage policy is in place to govern staff's use of AI tools and technologies. ✓ Robust processes have been established for onboarding new AI models and signals, ensuring proper evaluation and oversight before deployment. ✓ An audit trail of prompts is maintained to track staff activity and monitor how AI tools are being used.

Hedge fund 3 (HF3)

Summary

— HF3 allows staff to use AI tools in the investment process. However, instead of firm-controlled enterprise accounts, which can be monitored, staff are permitted to use personal accounts for platforms such as Gemini and ChatGPT.

Description of controls

- ✗ The firm does not have an AI policy, formal controls, or restrictions governing staff AI usage.
- ✗ There are no safeguards to prevent employees from entering confidential, sensitive, or MNPI into AI tools.
- ✗ No oversight mechanisms, such as compliance reviews, usage logs, or regular audits are in place to monitor staff activity on AI platforms.