NOYACK

Risks of Agentic AI in Finance

Model Hallucination

AI generates false or misleading outputs that appear plausible.

- *Has the AI provided outputs that cannot be verified with primary data sources?*
- *Would acting on this output expose us to financial or reputational loss?*

Bias & Discrimination

AI models may reinforce or amplify existing societal or financial biases.

- *Are certain client groups consistently disadvantaged by AI-driven outputs?*
- *Have fairness checks been applied to the training data and decision rules?*

Data Privacy Breach

Sensitive financial data could be leaked or misused.

- *Could client or firm data be exposed to unauthorized systems during AI processing?*
- *Does this AI comply with GDPR, CCPA, or relevant financial privacy regulations?*

Autonomy Overreach

Agentic AI may execute financial actions beyond intended scope.

- *Can the AI trigger or execute transactions without explicit human approval?*
- *Are there safeguards to ensure actions remain within a pre-approved mandate?*

Market Manipulation

Unintended consequences could distort pricing or liquidity.

- *Could this AI's trading or recommendations influence market behavior at scale?*
- *Is there a risk of collusion or herding effects from similar models acting together?*

Regulatory Non-Compliance

Outputs or decisions could violate financial laws and standards.

- *Does the AI's output align with SEC, FINRA, or equivalent regulations?*
- *Is there a clear audit trail that regulators can review?*

Cybersecurity Threats

AI could become a vector for attacks or exploits.

- *Could adversarial inputs or prompts cause the AI to behave maliciously?*
- *Is the model environment protected against data poisoning or injection attacks?*

Accountability Gaps

Difficult to attribute responsibility for autonomous decisions.

- *Is it clear who is accountable if the AI makes an error or causes loss?*
- *Do governance frameworks define escalation procedures when AI acts unexpectedly?*

NOYACK

Risks of Agentic AI in Finance

How to Use This Checklist

This checklist is designed to help you identify whether each AI-related risk applies to your financial workflows.

1. Review the Definitions: Each risk is clearly defined on Page 1.

2. Ask the Guiding Questions: For each risk, use the two diagnostic questions to test if it applies to your context.

3. Evaluate and Mark: If either question raises concern or if the definition matches your environment, mark the column for Agent A or Agent B below.

Tip: Use this checklist during project planning, risk audits, or governance reviews to ensure potential issues are not overlooked.

Risk Term	Agent A	Agent B
Model Hallucination		
Bias & Discrimination		
Data Privacy Breach		
Autonomy Overreach		
Market Manipulation		
Regulatory Non-Compliance		
Cybersecurity Threats		
Accountability Gaps		