DiligenceVault

GENERATIVE AI · 30 QUESTIONS · 6 SECTIONS

Generative AI Due Diligence Questionnaire

A structured assessment of AI strategy, investment applications, governance, model architecture, data protection and resilience.

INSIDE THIS QUESTIONNAIRE

01 Strategy and Adoption — Questions 01–04

02 Investment Process and AI Autonomy — Questions 05–08

03 Governance and Oversight — Questions 09–13

04 Models, Architecture and Build vs. Buy — Questions 14–18

05 Citizen Development, Data Security and Privacy — Questions 19–26

06 Proprietary Data, Economics and Resilience — Questions 27–30

RESPONDENT

FIRM NAME _____

COMPLETED BY _____

TITLE _____

DATE _____

SECTION 01 · QUESTIONS 01–04

Strategy and Adoption

01 What are the primary objectives for your firm's use of AI over the next 2–3 years?

- ☐ Productivity / operating efficiency
- ☐ Cost reduction
- ☐ Investment research / alpha generation
- ☐ Investment decision support
- ☐ Risk management
- ☐ Client / investor experience
- ☐ Distribution / fundraising
- ☐ Software development
- ☐ Development of proprietary capabilities
- ☐ Other

02 Where is AI currently being used within the firm?

BUSINESS FUNCTION	PRINCIPAL USE CASE	WORKFLOW STEP
Investment research		
Portfolio management		
Trading		
Risk management		
Operations		
Compliance / legal		
Client service		
Distribution / RFP / DDQ		
Software development		
Corporate functions		
Other		

03 Approximately what percentage of employees regularly use AI as part of their work?

☐ <10% ☐ 10–25% ☐ 26–50% ☐ 51–75% ☐ 75%+

04 What are the firm's three most important AI initiatives over the next 12–24 months?

SECTION 02 · QUESTIONS 05–08

Investment Process and AI Autonomy

05 **For AI used within the investment process, what activities may it perform?** Select all that apply.

- ☐ Information retrieval
- ☐ Summarization
- ☐ Research / analysis
- ☐ Idea generation
- ☐ Recommendation
- ☐ Portfolio / risk analysis
- ☐ Decision making
- ☐ Trade or other execution

06 **Are any investment, trading, risk, client, or material operational actions permitted to occur without human approval?**

☐ Yes ☐ No

07 **How does the firm evaluate material AI-generated investment outputs for accuracy, unsupported conclusions, consistency, bias, and deterioration in performance over time?**

08 **How does the firm assess whether AI is improving investment decision quality rather than simply increasing the speed or volume of research produced?**

SECTION 03 · QUESTIONS 09–13

Governance and Oversight

09 **Who has executive accountability for AI strategy and AI risk?**

10 **Describe the firm's AI governance framework, including acceptable-use policy, risk classification, approval requirements, governance oversight, and escalation of higher-risk use cases.**

11 **Does the firm maintain a centralized inventory of material AI applications, models, agents, vendors, and employee-developed tools?**

☐ Yes ☐ Partially ☐ No

12 **Has the firm's AI governance or control environment been independently reviewed by internal audit, compliance, risk, information security, or an external party? If yes, summarize the most recent review.**

☐ Yes ☐ No

13 **Has the firm received any regulatory inquiries, examination requests, or findings related to its use of AI (from the SEC, FINRA, or other regulators or self-regulatory bodies)? If yes, briefly describe the nature of the inquiry or finding and the firm's response.**

☐ Yes ☐ No

SECTION 04 · QUESTIONS 14–18

Models, Architecture and Build vs. Buy

14 **Which model providers or model families are currently approved or materially used by the firm?**

PROPRIETARY / FRONTIER

- ☐ OpenAI
- ☐ Anthropic
- ☐ Google / Gemini
- ☐ Microsoft / Azure-hosted models
- ☐ Amazon Bedrock
- ☐ xAI
- ☐ Cohere
- ☐ Other (Proprietary / Frontier)

OPEN / OPEN-WEIGHT

- ☐ Meta / Llama
- ☐ Mistral
- ☐ DeepSeek
- ☐ Alibaba / Qwen
- ☐ Moonshot / Kimi
- ☐ Other (Open / Open-Weight)

15 **How does the firm select models for different use cases and manage dependency on individual model providers, including changes in capability, pricing, availability, or contractual terms?**

16 **Which best describes the firm's AI development philosophy?**

- ☐ Build internally primarily for core or differentiated capabilities
- ☐ Build internally across both core and non-core use cases
- ☐ Buy / partner for most capabilities and build selectively
- ☐ Primarily use AI embedded within existing enterprise software
- ☐ Other
- ☐ Other (please specify): _____

17 **Which AI capabilities does the firm consider sufficiently core or differentiated to build internally, and what framework is used to determine when to build, buy, or partner?**

18 **How is AI resourced within the firm?**

SECTION 05 · QUESTIONS 19–26

Citizen Development, Data Security and Privacy

19 **Are employees permitted to create AI applications, agents, automations, scripts, or workflows using generative AI or low-code/no-code tools?**

☐ Yes ☐ No

20 **Do employees receive training on responsible AI use, including prompt hygiene and how to identify AI errors or hallucinations?**

☐ Yes ☐ No

21 **How does the firm identify and manage unapproved AI tools, applications, or "shadow AI"?**

22 **What is the firm's process for vetting and approving a new AI tool or vendor before it is used?**

23 **What categories of firm, client, investor, portfolio company, counterparty, or employee information may be processed by AI applications, and what categories are prohibited?**

24 **For material AI providers, describe the firm's controls and contractual requirements regarding data retention, model training, data residency, encryption, access controls, subprocessors, data deletion, and prevention of unauthorized data exposure.**

25 **What controls address AI-specific cybersecurity risks, including prompt injection, malicious documents, data exfiltration, excessive agent permissions, credential exposure, and unauthorized actions?**

26 **Does the firm have a defined escalation and disclosure process for incidents where AI itself is the cause, such as a hallucination that led to an inaccurate client-facing statement, or a prompt injection that exposed data? If yes, describe the escalation path, who is notified internally, and any client or regulatory disclosure obligations that apply.**

☐ Yes ☐ No

SECTION 06 · QUESTIONS 27–30

Proprietary Data, Economics and Resilience

27 **Has the firm licensed, sold, contributed, or otherwise provided proprietary data, employee expertise, work product, operational data, or other non-public information for training, fine-tuning, evaluating, or improving third-party AI models?**

☐ Yes ☐ No ☐ Under consideration

28 **Follow-up (if yes): Please describe the arrangement.**

29 **Does the firm maintain a dedicated or separately identifiable AI budget, and how does management measure realized value from AI investments?**

30 **Which investment or business processes are materially dependent on AI, and what is the business continuity / disaster recovery strategy if a material AI model or provider becomes unavailable or materially degraded?**