ETHISPHERE®
GOOD. SMART. BUSINESS. PROFIT.®

SpeakUp®

Davis Wright Tremaine LLP

THIRD-PARTY RISK MANAGEMENT

VENDOR AI REVIEW FRAMEWORK

Most artificial intelligence (AI) will enter the enterprise through vendors, concentrating risk. The following review framework makes AI due diligence a standard gate by plugging into sourcing without slowing the business and giving E&C a consistent and defensible way to approve, track, and roll back vendor AI (if needed).

DUE DILIGENCE CONSIDERATIONS:

When conducting due diligence on vendors, consider these questions for key risk areas related to AI.

GOVERNANCE

- What framework and regulations does the vendor follow?
- Does the vendor have an established AI Steering/Governance Committee and/or responsible roles assigned?
- Does the vendor have a publicly available Transparency Statement? Does their Privacy Policy include how their AI system has been designed, what data is being used, how they are using the data, and how customers can report issues related to the AI system?
- Can clients request access to IT security documentation, including policies, audit reports, and testing reports?

DATA PROVENANCE & RETENTION

- What data is being collected, processed, or stored in their AI system?
- Where is that data being stored?
- How is that data being protected at rest and in transit?
- How is the data provided by the customer being used in the AI System (e.g., training, informing the service, providing direct responses or delivery)?
- How can the customer request that the data be deleted or removed?
- For how long is the data retained? Can it be permanently deleted upon request?

TRAINING DATA SOURCES

- What sources were used to train the AI model?
- Is the AI system using a publicly available foundation model (e.g., Claude, Gemini, ChatGPT) or a model built in-house?
- Does the vendor have a Secure Software and System Development/Architecture policy and procedure that covers the AI system?
- How was the data used to train the model sourced?

TESTING/RED-TEAM RESULTS

- What testing frameworks are used to evaluate the model (e.g., red team, bias, general, and explainability testing)?
- Has an independent red-team test been conducted? If so, how frequently?
- Do you have an internal red-team or adversarial team that conducts testing on the AI system? If so, how frequently?

BIAS & ROBUSTNESS

- How are biases detected and remediated?
- How do vendors report potential bias?
- What type of robustness testing has been conducted?
- What are the metrics used to measure bias and robustness?

EXPLAINABILITY

- Does the vendor provide a transparency statement or other documentation that describes the overall design of the model?
- Can the customer review or audit model decisions?
- Does the AI system provide explanations for how it provided a particular output?

ROLLBACK PROCESS & CHANGE MANAGEMENT PLAN

- Does the vendor have a documented Change Management plan?
- Is the vendor document rollback process specific to changes to the AI system or models that include when the model become unstable or non-compliant?
- Does the vendor have defined service-level agreements (SLAs) that cover the AI system? If not, does the vendor have a defined maintenance window?
- How are changes to the AI system or model communicated to customers?

To learn more about leveraging AI to benefit and improve your ethics and compliance program, check out the **full report**.