

How to ask corporate vendors the right questions when it comes to responsible AI

The better the question. The better the answer.
The better the world works.

EY
Shape the future with confidence

As artificial intelligence (AI), which includes generative AI (GenAI) and agentic AI, becomes part of business as usual, leaders are establishing and implementing strategies for their own organizations' responsible AI (RAI) adoption. The next phase is gaining an understanding of business vendor and partner AI use, which could extend its reach into regulatory compliance.

Most EY client vendors have probably started to embed AI into their products and processes or are charting a roadmap for an AI-powered future. Evaluating a vendor company's AI portfolio to assess current and future AI capabilities isn't simple, but it is important, especially in cases where the package selection, system implementation and maintenance process are decentralized.

RAI inventory requires linking of data, models and use cases for inventory and tracking purposes, which even large tech companies don't necessarily have the capabilities for yet. So vendors should be evaluated to minimize risk and facilitate positive, transparent business relationships.

When evaluating third-party RAI, it is a company's responsibility to thoroughly assess:

- RAI framework adoption
- Risk assessment
- Data management
- Technical documentation
- Post-production monitoring
- Disclosure practices
- Incident response
- Insurance coverage
- Responsibilities of deployer
- Contractual obligations to ensure AI systems are secure, compliant and ethically managed

What companies should consider when evaluating third-party vendors for responsible AI:

The RAI framework:

- What framework or system the vendor has adopted

Risk assessment:

- The vendor risk assessment process and criteria
- What determines higher vs. lower risk
- What governance addresses fairness, bias and accountability

Access and data management:

- Specific rights and data management protocols in place to secure the AI system's access to the environment
- How the third party will use data and transactions to train its models to clarify the ownership of any intellectual property that may result from the use of the AI systems, including patents, trademarks and copyrights
- Whether the third party has access to the vendor's environment and/or data, and if so, how it is managed and logged

Technical documentation:

- Whether the third party provides risk-assessment documentation at the enterprise level as well as the individual model or system level
- What specific data and security regulations the AI system must comply with, including by regulation or jurisdiction
- What specific metrics are used to measure AI performance throughout the AI development lifecycle
- Specific limitations of the AI system and the necessary human activities to address them

Post-production monitoring:

- The process for post-production monitoring of AI solutions
- How the company will be informed when AI systems perform outside of the expected range
- Whether logging will be available for transactions interacting with sensitive data

Disclosure and communication:

- Whether the third party provides sufficient and specific information on each of the AI systems to facilitate the safe use of AI (think of food labels, included in the Singapore AI verification requirements)
- Whether a SOC report equivalent report will be available on the performance and compliance for AI systems

Incident response and recovery:

- Communication protocol if an incident occurs, including threshold to disclose and resolution process
- Third party's incident response capability and disaster recovery plans in case of AI system failures or security breaches, from incident management to crisis management
- Extent of the third party's insurance coverage

The company's responsibilities:

- What specific deployer responsibilities the third party is passing on (think of it as the CUECs (complementary user entity controls) for a SOC report)
- Any specific training and support needed to use the AI systems

Contractual obligations:

- The right to audit the third-party AI systems
- Specific data use restrictions
- Communication/escalation service-level agreements (SLAs)
- Define clear accountability and liability terms related to the AI solution's performance and impact

Access and data management:

- What specific access rights and data management protocols does the vendor need to put in place to secure the AI system's access to the environment?
- Will the third party use data and transactions to train its models to clarify the ownership of any intellectual property that may result from the use of the AI systems, including patents, trademarks and copyrights?
- Will the third party have access to the vendor's environment and/or data? If so, how is the access managed? Is it logged?

The above considerations are easier to manage in new vendor relationships. But many existing vendors have already started to embed AI into their products or plan to roll out new features using AI in the near future, so the picture can get murky.

It's often more challenging to evaluate a company's current portfolio of vendor systems and flag those that have AI capabilities or will implement AI in the next six months, especially in cases where the package selection, system implementation and maintenance process is not consistently centralized.

When evaluating third-party RAI, companies should use the above checklist to thoroughly assess the vendor's RAI and gain confidence that all AI systems are secure, compliant and ethically managed.

EY contacts:



Sarah Y Liang
EY Global Responsible AI Leader
sarah.liang@ey.com



Chris Watson
EY Americas Risk and Supplier Services Solution Leader
christopher.watson@ey.com

EY | Building a better working world

EY is building a better working world by creating new value for clients, people, society and the planet, while building trust in capital markets.

Enabled by data, AI and advanced technology, EY teams help clients shape the future with confidence and develop answers for the most pressing issues of today and tomorrow.

EY teams work across a full spectrum of services in assurance, consulting, tax, strategy and transactions. Fueled by sector insights, a globally connected, multidisciplinary network and diverse ecosystem partners, EY teams can provide services in more than 150 countries and territories.

All in to shape the future with confidence.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. EY member firms do not practice law where prohibited by local laws. For more information about our organization, please visit ey.com.

Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US.

© 2024 Ernst & Young LLP.
All Rights Reserved.
US SCORE no.
2411-10227. ED none.

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, legal or other professional advice. Please refer to your advisors for specific advice.

ey.com