KPMG

Managing key risks in deals involving proprietary AI systems

Minimize risks to maximize deal value

January 2023

Introduction

01 **We have seen a growing trend of AI technologies enabling key operational processes across industries, and increased deal activity in the AI space.**

02 **However, M&A deals involving such technologies can create several commercial, technology, organizational and data security risks.**

03 **We have presented a framework containing key considerations for buyers to mitigate these risks.**

This whitepaper is part of a series focused on how IT can increase deal value and minimize business risks during a transaction. The series will highlight principles that the Technology M&A team in KPMG in Canada leverages to help maximize value and minimize risks for clients across industries.

In today's market, there is a growing trend of Artificial Intelligence (AI), which is intelligence demonstrated by machines, helping modern businesses increase revenue and boost operational savings. In particular, the applicability of AI technologies for a variety of use cases has enabled value creation for organizations across multiple industries, including IT services, health care, cybersecurity, financial services, retail, manufacturing, and transportation and logistics.

In recognition of AI's benefits, private equity firms and corporations are progressively acquiring companies that leverage AI capabilities. According to the Global AI market report published by Drake Star Partners, the M&A activity in AI has experienced sixfold growth since 2015, reaching $12.3-billion in total disclosed transaction value in 2022. While IT services has led in terms of volume of capital invested, cybersecurity has seen the highest growth in deal count with an astonishing compound annual growth rate (CAGR) of 135% between 2016 and 2021. Additionally, Canadian insights from a global survey by KPMG International reveal 95% of technology leaders at private- and public-sector organizations in Canada plan to invest in Web3, 70% plan to invest in 5G and edge computing, 67% plan to capitalize on quantum computing and 54% plan to invest in the metaverse over the same period. All of these technologies rely on AI to power the respective use cases.

While AI has increasingly embedded itself into organizational processes, we have seen a number of commercial, technology, organizational and data security risks inhibiting successful value creation in the deal context. Our objective for this whitepaper is to present a framework that would enable buyers to proactively identify and mitigate these risks in the pre-deal due diligence phase, in order to create value from proprietary AI systems after the deal.

The framework can help structure the assessment of the seller's product roadmap, technology tools and processes, talent strategy and data security mechanisms. Proactively managing the key risks early in the deal process can help maximize the value of AI systems and position the buyer for digital leadership.

Key Acquisition Risks

While driving the digital leadership use cases of AI can result in tangible business benefits, buyers need to consider the following risks in the acquisition of AI companies:

01. Commercial Risks

Sellers often showcase the commercial value offered by proprietary AI systems, which typically require several years to develop. However, the systems may be quickly outdated by off-the-shelf AI technologies, especially those developed by nimble software companies that have rapid product development cycles. In these instances, the revenue-generating potential and commercial standing of the acquired technologies would be limited.

02. Technology Risks

Integrating AI systems into the technology environment after an acquisition requires development of comprehensive data management platforms, use of modern software development methodologies, and reinforcement of mechanisms to extract advanced analytics insights. This requires robust technology capabilities, which the buyers may not have fully developed at the time of the transaction.

03. Organizational Risks

The rapid pace of innovation in AI requires that the talent pool be equipped with the required technological and operational skill sets, and able to quickly scale the organizational capabilities for evolving business requirements. An inability to identify, hire and retain suitable talent can pose a potential risk to the buyer's strategy to fully leverage AI.

04. Data Security Risks

AI engines are fuelled by data, much of which can be sensitive consumer or proprietary information. Failing to protect this data from cyberattacks can create legal liabilities for the buyer, especially when operating in regions with strict data protection and privacy rules, such as California's Consumer Privacy Act.

Due Diligence Focus Areas

There is an opportunity to mitigate the key risks by applying the following framework in the pre-deal due diligence phase:

Key Focus Areas for Due diligence

Sound Product Roadmap

To assess the product's value proposition in comparison with other products

Robust Technology Tools & Processes

To validate the enablement of product maintenance and future upgrades

Effective Talent Strategy

To evaluate the quality of seller's AI talent pool to maintain and develop the product

Reliable Data Security Mechanisms

To confirm the robustness of security frameworks to protect against data breaches

Sound Product Roadmap: In the acquisition of AI companies, it is important to confirm that the seller's technology is unique and that it cannot be rebuilt using AI tools and solutions already available in the market. Also, the product strategy that dictates the degree of customization of the AI modules and their applicability to the buyer's business requirements should be factored into the diligence process. These considerations are important to mitigate the **commercial risks**.

Robust Technology Tools and Processes: The buyer should validate that the seller's technology tools and processes can enable the maintenance and periodic upgrades of the AI technologies. These include AI development kits as well as maintenance modules from reputed vendors. These proactive steps would promote the seamless integration of the AI systems into the buyer's technology environment, thus mitigating the **technology risks**.

Effective Talent Strategy: In our view, while the rise of AI may appear to be eliminating the human element, the opposite is true. Skilled talent is still required to develop, monitor and fully leverage AI platforms. Ensuring that the seller's talent strategy fosters those skills from within and brings the right set of individuals into the team is an important step towards mitigating the **organizational risks**.

Reliable Data Security Mechanisms: An AI platform is enabled primarily by the data that drives the platform's algorithms. In many cases, however, the data owned and managed by the seller is deemed sensitive and is governed by regulatory constraints. The seller should, therefore, protect the data against breaches through robust cybersecurity controls and policies to mitigate the **data security risks**.

Careful consideration of the above risks and methodical execution of the mitigation actions would facilitate successful value creation for buyers in the post-deal environment.

Case Study

A case in point is the pre-deal due diligence for the acquisition of a health-care company that had developed a proprietary AI system. The system, which was hosted on-premise provided several functionalities, including AI-based predictive modelling for proactive disease diagnosis using Electronic Health Records (EHR) data and intelligent automation for billing verification. The primary objective of the diligence activity was to identify risks pertaining to the AI system for the private equity buyer, which planned to expand the scope of the acquired entity's operations across the U.S. and Canada following the deal. While the seller offered a unique value proposition to enable commercial viability and had developed a product roadmap that considered the requirements for future customization, there were potential risks for the buyer:

Technology risk due to the use of legacy development tools with limited scope for maintenance and upgrades of the on-premise system;

Organizational risk due to key-person dependencies on employees who were involved in the design and development of the proprietary system; and

Data security risk due to lack of compliance with the U.S. Health Insurance Portability and Accountability Act (HIPAA) regulation that provides provisions to secure sensitive patient information.

To mitigate these risks, we recommended the following steps, keeping in view existing and future scale of operations, timing constraints associated with the transaction, and cost implications:

Upgrade to the suite of **AI products offered on Microsoft Azure,** which provides tools and processes to build, deploy and operationalize the AI system with automatic maintenance and upgrades of the development platform, in order to mitigate the **Technology risk** and minimize the ongoing maintenance cost of the AI system;

Leverage **Microsoft Azure DevOps** solution with a comprehensive repository for all software and AI related artifacts to retain the proprietary knowledge in the event of key employee departures, in order to mitigate the **Organizational risk** and minimize the labour cost involved in potentially rebuilding the AI knowledge base; and

Adopt the **National Institute of Science and Technology Cybersecurity Framework** that encapsulates security standards for patient health information to ensure alignment with HIPAA regulation requirements, as well as incorporate intellectual property protection platforms provided by **Microsoft Azure Machine Leaning module** that secures the proprietary data sets used to train the AI model, in order to mitigate the **Data Security risk** and minimize the legal cost resulting from potential exposure of sensitive patient information to cyberattacks.

The tactical execution of the above steps mitigated the deal risks while reducing the maintenance, labour and legal costs. The pre-deal actions, therefore, added value to the buyer's investment and enabled the operational benefits of the AI system in the post-deal environment.

Summary and Conclusion

It is important for buyers to recognize the commercial, technology, organizational, and data security risks involved in the acquisition of companies that own proprietary AI systems. Early assessment in the pre-deal due diligence phase can help identify and mitigate these potentially material risks, and help position the buyer to maximize value by driving revenue generation and boosting operational savings.

To learn how KPMG can help navigate the challenges of AI and unlock the full potential from your merger or acquisition, please feel free to contact us.

Contact our Technology M&A Services team

Sharjil Salim
Partner
Toronto, Canada
416-791-2030
ssalim1@kpmg.ca

Aditya Narasimha
Manager
Toronto, Canada
416-791-2104
anarasimha@kpmg.ca