Professional Perspective

Key Considerations for an AI Strategic Plan: How to Acquire and Use AI Technology Safely to Grow and Protect Your Business

Kenneth N. Rashbaum and Lani E. Medina, Barton LLP

Bloomberg Law

Key Considerations for an AI Strategic Plan: How to Acquire and Use AI Technology Safely to Grow and Protect Your Business

Contributed by Kenneth N. Rashbaum and Lani E. Medina, Barton LLP

Any new business tool or system requires a strategic plan, and yet, many leaders are failing to consider such factors when implementing new artificial intelligence tools. The acquisition and use of AI tools also necessitate guidance from inside and/or outside counsel, especially since the laws regarding AI are rudimentary, uncertain, and often in conflict with one another. Counsel can help to frame the initiative and provide advice throughout the process in order to facilitate the safe acquisition and use of AI. Recognizing AI's complexities and legal uncertainties, a meticulously crafted business plan that includes how to negotiate a favorable agreement to obtain use of the AI tool serves as a roadmap to navigate these challenges by rendering the adoption of AI technologies innovative, legally sound, and closely aligned with the company's broader goals. The strategic, or business, plan, which will be described below, seeks to answer questions likely to be posed by those who will decide whether to acquire the AI tool and, if so, how its acquisition will be budgeted and deployed.

Start at the Very Beginning: Answer the Basic Questions on the Choice of AI and Its Uses

A basic understanding of the AI tool's utility is foundational to the strategic plan, and it comprises answers to the following questions that should also find their way into the plan, such as in the introduction or executive summary:

1. Why are you considering an AI tool – what would it do for the business (in specific terms)?

2. What sort of AI tool would be deployed? Do you want it to provide an analysis or predict a trend from a database, generate text or command a system or device to perform an action (i.e., directing an autonomous car)?

3. How would the tool be used – by which business units and for what business purposes?

4. Whose data will be, or was, used to train the algorithms that enable the tool? Is the data protected by law (privacy or confidentiality), contract (trade secret or proprietary information), or intellectual property protections (copyright, trademark, right of publicity, patent)?

5. Where will the tool be obtained? Are you developing it in-house or acquiring it from a third party?

6. What is the anticipated budget for development or license of the tool as well as deploying it and monitoring its use?

7. What is the state of your insurance coverage? Does your insurance cover legal, regulatory, or contractual risks in the use of the AI tool?

8. Who will be responsible for deployment? Who will monitor the tool's uses and outputs for accuracy and compliance?

9. What are the risks of using the tool? After an assessment of known risks and in consideration of unknown risks, do the benefits outweigh these considerations in a way that provides a comfort level in moving forward?

10. What is the ROI (Return on Investment) for this tool? What are the acquisition, deployment, and monitoring costs versus the business cost savings or business growth?

Getting the Tool in the Door: The License Agreement

Very few statutes or regulations in the US provide guidance on AI acquisitions or uses and so most of the governance between providers and users of AI tools will derive from their contractual relationship.

Beyond traditional license agreements, acquiring and deploying AI often involves a complex web of agreements, including development contracts, service partnerships, and tailored collaborations based on specific needs and contributions. This requires businesses and their counsel to, as the late Steve Jobs famously said, “Think different,”—at least where the business can insist on such an agreement rather than merely signing online Terms and Conditions that are generally non-negotiable.

The AI contract can include many traditional contract protections, but may require consideration of differing specifics such as:

a. The Statement of Work or Purchase Order.

What is being licensed or acquired, and how does the statement detail the tool's functionality, including obligations for its maintenance and future updates? Who is responsible for integrating the AI tool into the acquirer's systems, and what support, including workforce training, will be provided? This component should clearly outline the scope of the purchase or license, covering necessary updates and maintenance to maintain the AI tool's effectiveness and security over time.

b. Notice and Acceptance.

Does the licensee or purchaser get to “test drive” the tool before payment terms kick in? If so, what are the metrics for performance or non-performance, and how much time, if any, should the licensor or provider be granted to fix the problem? Should any issues arise during the trial, is there a clearly defined process for reporting, evaluating, and rectifying these issues before final acceptance? Introducing a “test drive” phase reduces the risk of unexpected issues, a critical step for aligning the AI tool with operational demands and compliance requirements.

c. Definitions.

What does the term “the Services” or “the Application” comprise? What is the scope of “Applicable Law” to which the parties must comport? What is “Personal Data” or “Protected Data”? These terms and others can provide the superstructure for the relationship between the parties, particularly as the technology develops and evolves.

d. Flow-down Terms.

What flow-down terms are included to ensure subcontractors or business partners adhere to the same standards as the primary contract? Are there any restrictions or conditions on the further or derivative uses of the AI tool by these third parties? Promoting AI tool consistency across all parties is essential for protecting intellectual property and regulatory compliance.

e. Limitations of Liability, Disclaimers, and Waivers.

Beyond the traditional limitations to a year's fees, how are liabilities for known and unknown AI risks addressed? Are disclaimers and waivers adequately formulated to cover potential damages from AI tool malfunctions or security breaches? Tailoring these provisions for AI-centric risks promotes a balanced and informed approach to this new area of liability.

f. Indemnification.

Does the contract include an indemnification clause that covers claims related to using the AI tool's inputs, outputs, and overall functionality? Is the indemnification language tailored to cover the unique risks associated with AI technologies, such as errors in data processing and decision-making inaccuracies? An indemnification clause tailored to the specific risks of AI can shift risk and thereby offer some protection against potential legal and financial liabilities arising from the tool's use.

g. Applicable Law and Governing Law.

What jurisdiction's laws will govern the contract, and how has this jurisdiction been chosen for its relevance to AI technology and disputes? Are specific legal frameworks or precedents in the selected jurisdiction particularly favorable or least unfavorable to AI applications and liabilities? How does the contract resolve potential legal conflicts, especially for cross-border AI use? Selecting a jurisdiction in which courts have some experience with AI intricacies can aid in protecting the contractual bond because disputes can be resolved with a nuanced understanding of AI's distinct challenges.

h. Dispute Resolution.

Is a specific notice period required to resolve a dispute with options for mediation before escalating the issue? Considering the technical complexity and novelty of AI-related disputes, do the parties prefer a judge or an arbitrator with expertise in AI technologies to resolve disputes? Choosing dispute resolution specialists knowledgeable in AI can help in securing equitable and well-informed decisions.

i. Intellectual Property Rights.

How are intellectual property rights for AI-generated outputs and data explicitly defined and allocated between parties in the contract? What provisions address the creation and use of transformative derivative works so that the parties' rights are protected and obligations are clear? The agreement must meticulously outline the ownership, use, and distribution of intellectual property generated by the AI tool.

j. Data Usage and Protection.

How does the contract specify the handling, security, and privacy compliance of data used by the AI tool, particularly in adherence to data protection laws and regulations? What mechanisms are in place for responding to and notifying relevant parties of data breaches? In addition to handling and breach notification, how does the contract address the rights and responsibilities related to anonymizing, sharing, and selling data collected or generated by the AI tool? Specifying data management practices in this way can address critical business and legal privacy and security concerns.

k. Compliance with Regulations and Standards.

How does the contract establish compliance with specific laws, regulations, and industry standards relevant to the AI tool's provision and support? Are there specific provisions for conducting regular compliance audits? If so, how do these audits interface with evolving legal standards and industry best practices? Integrating regular compliance reviews into the agreement demonstrates a dedication to legal and ethical AI practices, which is key to fostering trust and reducing compliance risks.

Deployment Considerations: Safely Integrating AI into Your Business Operations

There are many questions to be answered before the tool is deployed and others that will arise with experience, but it's usually best to have a rollout plan in place before new technology is deployed. This can include:

1. Access controls: Should all employees have access to the tool? If not, who is restricted and why?

2. Incident plan: What constitutes an “incident” and who should be contacted if one occurs (with backup if that person is unavailable)? How should that person commence, conduct, and document the investigation into the incident?

3. Performance metrics: How will the AI tool's success be measured? What benchmarks will indicate effective performance? How frequently will performance data be reviewed and evaluated?

4. Stakeholder notification: Is notification of this technology rollout to your cyber risk or technology errors and omissions insurance carrier(s) required by your policy? Do your contracts with your clients require that they be informed about the deployment, including the potential for an opt-out option, and should other relevant stakeholders also be notified?

5. Exit strategy: How can the tool be retired at the end of its useful life or if its performance doesn't live up to expectations? What happens to the outputs and records of inputs, as well as records of the data that was used to train the algorithm?

AI holds many benefits for organizations of all kinds. It also poses many challenges and risks. An understanding of how best to consider and meet them will be the key to successful rollout of this technology that will only grow and develop with use. This comprehensive approach will also keep the Risk and Compliance, Legal, and Finance Departments from acquiring a “Department of No” reputation through over-emphasis of these challenges and risks. Instead, these departments can remain part of the conversation and be seen as business and revenue facilitators through comprehensive planning for tool acquisition contracts, access controls, incident management, performance evaluation, insurance implications, and exit strategies. Embracing these considerations as part of a holistic AI strategy will enable businesses to leverage AI technologies as innovative tools and integral components of their growth and risk management frameworks.