

PUBLICATION

Top Five AI Procurement Questions General Counsel for Manufacturers Should Consider

Authors: Vivien F. Peaden

March 19, 2025

Artificial intelligence (AI) is reshaping the future of manufacturing. As manufacturing operations shift back to the U.S. in response to recent tariff policies, general counsels (GCs) in the manufacturing sector face a complex landscape. While reshoring may bolster domestic production, it also introduces challenges, such as higher labor costs and a shortage of skilled workers. As AI adoption has become a board-level priority, GCs are uniquely positioned to help business leaders navigate a rapidly evolving regulatory landscape. To that end, they should ask the following questions to help their companies maximize AI values and avoid legal pitfalls:

1. What AI technologies relevant to manufacturers should be considered?

While AI is not new to manufacturers, its applications have expanded significantly from traditional computer-aided design (CAD) to autonomous mobile robots. Today, manufacturers are evaluating the following AI tools to automate production and optimize business operations:

- **Robotic Process Automation (RPA):** RPA refers to software robots that automate repetitive tasks with precision. The "Bots" in RPA interact with existing business applications and systems to streamline production and business processes, such as data entry, inventory tracking, and invoicing.
- **Machine learning:** Machine learning (ML) is still in trend and enables better predictions and decision-making at every stage of manufacturing. For example, **predictive maintenance** continues to be a top AI use case, where an ML algorithm analyzes maintenance records to predict how and when equipment failure may occur.
- **Generative AI:** Generative AI (GenAI) is a subset of AI that generates content, design, and text, as opposed to traditional AI, which focuses on pattern detection. Manufacturers use GenAI to develop CAD designs and generate standard operating procedures (SOP). GenAI also enhances the aftersales customer experience through Chatbots, from parts replacement to maintenance scheduling.
- **AI architecture:** Forward-thinking manufacturers are actively integrating different types of AI architecture into their enterprise technology infrastructure. Similar to the cloud computing movement of the last decade, these enterprise architectures host AI applications that run the business operations of the next generation.
- **Cobots:** Cobots are AI-powered machines equipped with sensors to perform repetitive manual tasks, such as quality control inspections, and operate machinery while safely interacting with human workers. Automotive OEMs and e-commerce retailers rely on Cobots to enhance productivity and safety.

As manufacturers develop, procure, and use AI, understanding the specific AI tools and use cases is crucial to be assessed by GCs for legal implications and compliance obligations.

2. How do consultants deliver ROI for investment in AI strategies?

Business leaders in manufacturing are under pressure to move quickly with AI adoption. They often bring in management consultants to develop AI strategies and then invest in AI tools to execute those strategies. Instead of simply "getting legal sign-off" toward the final yard line, companies should involve the legal team **early** to quarterback the structure of these engagements, which often involve multimillions in upfront investment. Similar to any other transaction that impacts a company's bottom line, legal and commercial terms of an AI consulting engagement should go through due diligence for key stakeholders to assess the following:

- **Upfront Investment Without Measurable KPIs:** For any large-scale AI engagements, a portion of consultants' compensation should be tied to the output and key performance indicators (KPIs). To mitigate investment risks, GCs should partner with operations, finance, and IT stakeholders to define business goals and document measurable performance criteria for each milestone in the engagement letter or SOW.
- **Unrealistic Contingencies and Assumptions:** While many AI strategy engagements are proposed as fixed-fee engagements, the SOW often includes detailed contingencies and assumptions, such as company resource allocation, data quality, and existing IT structures. The legal team must carefully review these contingencies or risk the engagement exceeding the fixed-fee budget and project timeline.
- **AI Use Cases Under Regulatory Scrutiny:** In addition to production optimization, consultants are helping companies integrate AI in HR operations (for workforce management), marketing (for contextualized advertising), and procurement (for supply chain optimization). Some of these AI use cases are subject to increasingly tightening AI and privacy regulations. For these "high-risk" AI scenarios, GCs should partner with outside counsel to ensure regulatory compliance and protection of competitive-sensitive IP.

Companies don't invest in the "AI hype," they invest in output. By proactively ensuring AI adoption drives business values and aligns with compliance priorities, the legal team no longer serves as a legal gatekeeper, but as an enabler of these mission-critical transactions.

3. Should an AI roadmap focus on building in-house offerings or licensing tools from third parties?

When developing an AI roadmap, companies face a critical decision: invest in building in-house AI capabilities or license third-party tools. This mirrors the choices GCs make when structuring their legal function: which matters require deep internal knowledge versus those best handled by outside counsel. The answer is often a hybrid approach, balancing the following considerations based on a manufacturer's risk appetite:

- **Control vs. Costs:** Building proprietary AI offers greater control, allowing for customization and the potential to secure competitive advantages through exclusive IP ownership. However, this path demands significant upfront investment and an internal resource commitment for ongoing development. The legal review will focus on IP ownership of the deliverables, acceptance criteria and milestones, and other commercial terms in negotiating with trusted third-party software development and IT implementation consultants. Conversely, licensing third-party AI models enables rapid deployment and access to advanced technologies with lower upfront costs. Yet, it requires thorough vendor due diligence and contract negotiation, as discussed in the next section.
- **Data Sensitivity and Dependencies:** Some AI use cases involve hosting and analyzing sensitive personal data and proprietary business information. When engaging third-party AI licensors, companies must conduct due diligence and risk assessments to mitigate cybersecurity risks and safeguard their proprietary information. To the extent the AI tools support critical production or

business operations, a written service level agreement is essential for holding AI suppliers accountable for uptime, error response and resolution time, and for providing companies remedies through service credits and rights to termination for cause. If a manufacturer operates in a highly regulated sector, e.g., life science, national defense, etc., they should also consider hosting certain AI tools on company-controlled infrastructure to remove dependencies.

By taking a nuanced approach, this hybrid model enables manufacturers to leverage internal AI for competitive differentiation while benefiting from external providers' advanced technologies.

4. What questions to consider asking when negotiating with AI providers?

The legal team is vital in facilitating negotiations and onboarding the AI tools. Beyond facilitating the approval processes by IT, information security, and finance, they must balance compliance obligations and ethical considerations before, during, and after the negotiation. Beyond pricing and functionality, AI supplier contracts must address key data security, compliance, indemnity, and scalability concerns, as outlined below:

- **Data Protection and IP Ownership:** Who owns the data fed into the AI tools and the content generated by the AI tools? How can we protect trade secrets and proprietary information from being used to benefit other customers who license the same AI tools?
- **Compliance and Transparency:** Does the AI provider maintain an AI governance program that evolves with emerging AI regulations, security frameworks, and/or code of conduct? Has the AI provider completed any independent AI bias audits similar to [the one required under NYC Local Law 144](#)?
- **Risk Allocation and Mitigation:** Who is responsible when the AI system produces inaccuracies or causes harmful results? What measures are put in place to ensure the "human-in-the-loop" oversight? What policies should we implement to ensure our workforce uses AI responsibly?
- **Security Incident at Scale:** AI can turbo-charge technologies to cause significant harm. To this end, how will the AI provider indemnify customers for any IP infringement, breach of laws, and other harmful effects resulting from AI malfunctioning?
- **Scalability and Transition:** What's the pricing structure for any increase in user licenses, additional virtual computing capabilities, or multiyear service renewal? What will happen if we switch to new providers and require data migration?

Addressing these concerns upfront ensures that contracts protect the company's interests, align with strategic goals, and facilitate the successful integration of AI technologies.

5. What are the key AI regulations and guidelines in manufacturing?

As AI use cases in manufacturing continue to grow, legislators and trade associations are in the early stages of building a regulatory framework to balance innovation with responsible deployment. Some of these laws and guidelines relevant to the manufacturing sector include:

- **The EU AI Act and U.S. State AI laws:** Manufacturers play a unique role when leveraging AI. Under the [EU AI Act](#) and [various U.S. state AI laws](#), they may be [consumers, developers, and deployers of AI](#) throughout their production processes. The EU AI Act establishes a [four-tier risk-based framework](#), imposing stringent obligations on high-risk AI applications, such as those affecting workforce management and product safety. The state laws passed in California and Colorado and proposed regulations in Virginia follow a similar approach for automated decision-making tools and high-risk AI

use cases.

- **NAM's Advocacy for Innovation-Friendly Regulations:** The U.S. National Association of Manufacturers (NAM) emphasizes that AI regulations should support innovation and maintain leadership in AI. They advocate for simple, targeted regulations that avoid duplicative or contradictory rules.
- **FDA's proposed regulatory framework for AI integration in drug development:** Recognizing AI's potential, the FDA issued a draft guidance in January 2025 on employing AI to enhance drug safety. A central aspect of this guidance is a risk-based assessment framework designed to evaluate the reliability of AI models within specific contexts of use.

Staying abreast of these regulatory developments is essential for manufacturers to ensure compliance and leverage AI's benefits effectively.

What can manufacturers do to prepare for their AI options? As AI continues to transform the manufacturing sector, adopting appropriate AI strategies and tools and establishing a governance framework should be top priorities for all GCs. To help their organizations maximize the value of AI in manufacturing, planning, and forecasting, GCs must be kept up-to-date regarding the AI use case, ROI for investment, AI supplier due diligence, and evolving AI regulations. By proactively addressing these considerations, executive leadership and legal teams play an active role in driving competitiveness through AI adoption and ensuring the responsible and ethical use of AI.

The author, Vivien Peaden, is a former in-house counsel at a top-ranking management consulting firm. If you have any questions or concerns regarding this alert, please reach out to [Vivien F. Peaden, AIGP, CIPP/US, CIPP/E, CIPM, PLS](#) or any member of Baker Donelson's [Artificial Intelligence](#) team.