ADVISORY

Balancing Act: How Middle-Market Leaders Can Harness AI While Mitigating Risk

by John Verry and Rob McGillen

When it comes to the artificial intelligence (AI) boom sweeping through corporate America, today's middle-market leaders face a unique challenge. On the one hand, they need to adopt AI tools to maintain their competitive edge. On the other, they must navigate mounting AI-related risks — economic, regulatory, and reputational — with fewer resources and capabilities at their disposal than bigger players.

Given the stakes, it's mission critical that middle-market organizations have smart AI governance and business strategies in place. C-suite leaders must understand not only why and how their organizations are using AI, but also the key risks it presents and how best to mitigate them. The goal? Drive operational efficiencies and innovation without leaving the organization vulnerable to AI's potential hazards.

Here's what to know to get started.

Key AI Risks

To deploy AI successfully, it's critical that leaders understand the key risks at play. Yet many companies remain unprepared, with limited visibility into how AI is being used—and few guardrails in place. For instance, in a recent survey less than half of all organizations said they have implemented internal safeguards to promote responsible and effective AI development and use.

Middle-market companies may be especially vulnerable given the costs of addressing these risks and the increasingly competitive market for AI talent. Some important areas to consider:

Lack of Awareness of AI Use

The AI genie is out of the bottle, and most companies are now using some form of AI whether their C-suites know it or not. According to Microsoft's 2024 Work Trend Index, 75% of knowledge workers now use generative AI at work—and 78% of those are bringing their own AI tools to do so.

So-called "shadow AI" also lurks in the software-as-a-service (SaaS) tools companies use every day. A 2023 report found that more than three-quarters of SaaS companies were using or testing AI in their businesses. Yet only 28% were working on the kind of data quality programs needed to support robust and accurate AI models. This is of great concern seeing as a typical organization has hundreds of such applications deployed.

The problem runs all the way up to the boardroom. A recent Littler survey of C-suite executives shows misalignment among top leadership about which tools organizations are deploying: over 80% of chief human resources officers believe AI tools are being used in HR processes, while less than half of chief legal officers and general counsel say the same.

The challenge is clear: if you don't understand how, where, and to what extent AI is being used, it's difficult to effectively govern it.

Hallucinations

Generative AI — think ChatGPT — creates text, images and other content based on large quantities of training data. However, "hallucinations" can occur when these models generate incorrect or nonsensical information. This can be caused by missing data in the training process or limitations in the model's ability to understand the real world. For example, Google was in the news recently when its AI-assisted search feature recommended using glue to keep cheese on pizza, while several attorneys have come under fire for using generative AI to create inaccurate legal briefs.

Sensitive Data Leaks

If AI systems are trained on datasets containing personal and/or sensitive information, there's a risk this data could be leaked—as was the case at Samsung last May when an engineer input internal source code onto ChatGPT. This can have serious consequences for those whose data is exposed and create legal issues for the organization on whose watch the breach occurred. Executives should be on the lookout: in a recent study, 30% of employees said they thought there was value to their business from inputting sensitive customer information into public generative AI tools, 28% said the same of financial information, and 17% of confidential company news.

Bias and/or Discrimination

AI outputs can lead to unfair or discriminatory outcomes, as algorithms may reflect or amplify existing prejudices in the training data. For example, Amazon abandoned a machine learning tool it developed to review applicants' resumes when the company determined it was biased against women seeking STEM jobs. Such outcomes can also expose companies to legal and regulatory actions, as new laws (e.g., those in Colorado and New York City) make the deployer of AI decision-making systems liable for its decisions unless they have AI governance programs in place.

Third-Party Risk

Third-party vendors present significant risks, particularly for the middle-market companies who tend to depend on their expertise more than larger players. According to a report by Ponemon Institute, 51% of businesses have suffered a data breach caused by a third party. That threat surface is magnified when AI-enabled tools are added to the mix.

Regulatory Uncertainty

New AI regulatory frameworks are taking shape, from the European Union's AI Act (which could apply to U.S. employers even if they're not based in the EU) to the growing number of local and state laws—including several that address the use of AI in employment decisions. Federal agencies, including the Department of Labor and Equal Employment Opportunity Commission, are also issuing guidelines, while existing data privacy laws have their own AI implications. This complex, fast-evolving regulatory landscape can create significant headaches for those deploying AI, underscoring the importance of understanding how AI is being used.

Litigation

Legal experts warn that the above factors will open the door to a flood of AI-related lawsuits related to privacy, employment law, product liability, and intellectual property issues. Thus far, most claims have been brought against software vendors themselves — including class actions in Illinois, California, and Massachusetts — though this could change as the market continues to develop.

5 Steps to AI Governance

Executives cannot take a cookie-cutter approach to AI governance; it must be tailored to each particular business's needs, risks, and goals. That said, there are overarching best practices that businesses should follow as they get started:

Run an "AI Census" to determine how AI is used and to assess risks

To govern AI effectively, you've got to understand how and where it's being used. The goal is to create a list of all AI-enabled internal/external applications, their use cases, the data being shared, and the solution supplier. Ask yourself: How are your employees and vendors (and their vendors) using AI? For what purposes? With what data? What are the risks to our business relating to this use?

Running this exercise can also help configure acceptable AI use policies: for instance, certain areas (like HR) will be riskier than others and require more controls.

Adopt industry-standard controls to validate AI's sound, fair, and unbiased use

Organizations increasingly need to "prove" to clients, regulators, and boards that they're managing AI risk. Adopting and implementing ISO 42001, an internationally recognized standard for implementing and maintaining an AI management system, can help. The standard includes several controls and requirements that can help instill confidence among key stakeholders.

Run application security testing

Today's software engineers are incentivized to adopt AI technologies to improve efficiencies, increase employee utilization and code output, and introduce new AI-driven features to their clients. But the fundamentals of application security still apply. Companies should adopt proven practices around secure development and testing methodologies (e.g., OWASP Software Assurance Maturity Model, OWASP Application Security Verification Standard) for the AI they develop and potentially for business-critical applications that they procure.

Implement a business-specific AI acceptable use policy

AI use policies can help mitigate the risks listed above—but many organizations have yet to implement them. In Littler's survey, less than half of all executives reported having an AI policy in place at their organization, with key components including employee review of the policy, limiting use to approved tools (e.g., via access controls), or requiring employees to approve uses with their supervisors or a centralized AI decision-making group.

Developing such a policy is critical—but it must be tailored to your particular business. A gap assessment can help organizations identify gaps between current policies and controls and industry leading frameworks (e.g., NIST AI Risk Management Framework), standards (e.g., ISO 42001), and regulations (e.g., EU AI Act).

Update third-party risk management and procurement processes

Organizations outsourcing data and services to AI-driven applications and service providers should do their due diligence to ensure these tools have been designed and adopted in a reliable, fair, secure, and explainable manner. For instance: Have you updated your third-party risk management processes to identify the use of AI? Have you validated that vendors using AI are effectively managing the risks outlined above? Have you edited your outbound due diligence questionnaires to account for unique AI risks?

Balancing Innovation & Risk

The AI train has officially left the station, especially as generative AI tools and AI-enabled SaaS applications make these technologies readily accessible and widespread. Now is the time for middle-market leaders to take the reins and understand how AI is (and can be) used to drive their businesses forward in a safe and responsible manner.

CBIZ is a consulting, tax and financial services provider that works closely with CBIZ CPAs P.C., an independent CPA firm that provides audit, review and other attest services.