

HOW AI CREATES BUSINESS RISK EVEN WHEN YOU BARELY USE IT

By Michelle Bufano, Founder and CEO, Michelle Bufano Business Consulting LLC

“We don’t really use AI.”

That may be true of you personally. But what about the contractor writing your website copy? The software that summarizes your meetings? The vendor handling customer inquiries?

Your business can be exposed to AI risk without anyone making a formal decision to adopt it. That means your assessment needs to reach beyond the tools you purchased and into the work being done on your behalf.

In this week’s Tuesday Tip, I suggested a ten-minute AI risk checkup. Here is how to take that first look further and turn what you find into practical decisions.

FOLLOW THE WORK TO FIND THE AI

A list of AI subscriptions is a useful start. It will not tell you the whole story.

Choose one routine activity, such as preparing a client proposal. Follow it from beginning to end. Who gathers the information? Where is it stored? Does someone use AI to summarize a call, analyze a document or draft the proposal? Who checks the final version?

Now do the same for work you outsource. Ask contractors and vendors whether they

use AI in delivering your services, which tools they use and whether your information is entered into those tools.

LOOK WHAT GOES IN AND COMES OUT

Imagine a contractor uploads a client’s strategy document to an AI tool to help draft a presentation. The presentation looks excellent. The client is happy. But you have not established whether that upload was permitted or how the tool handles the document.

A good deliverable does not answer the information-handling question. Review the actual product, account settings and applicable terms. Ask what information is retained, who can access it and whether it may be used to train or improve models. Do not assume every account or version of a product offers the same protections.

Then look at the output. A meeting summary can omit an important limitation. A proposal can describe services you did not agree to provide. A marketing draft can include a statistic that sounds credible but has no reliable source.

Set a fact-verification checkpoint before an AI-assisted output is relied on or shared. The reviewer should compare it with the underlying information, confirm material

claims and understand the subject well enough to spot omissions. “Someone looked at it” is too vague to be a useful control.

MATCH THE CONTROLS TO THE CONSEQUENCES

Brainstorming names for an internal project and evaluating job applicants involve very different consequences. Treating them as the same kind of AI use makes your rules less useful.

For each use, ask: What information is involved? Who could be affected? What happens if the output is wrong? Can we catch a mistake before it causes harm?

Those answers help you decide whether a use can proceed under basic rules, needs specific approval and closer review, or should be paused while you obtain appropriate expertise. Uses involving sensitive information or decisions affecting people deserve particular attention.

Write down the decision in language your team can follow. For example: “Use the approved tool to brainstorm public-facing copy, but do not upload client documents. Verify factual claims before publication.” That is clearer than telling everyone to “use AI responsibly.”

CHECK WHETHER YOUR PROMISES MATCH YOUR PRACTICES

Suppose your website promises that every deliverable is entirely human-created. Your freelancer uses AI to produce the first draft. You now have a gap between what the

business says and how the work is performed.

Or perhaps a client agreement restricts disclosure of confidential information, while your contractor’s process sends that information to an outside AI service. Whether the process is permitted requires a closer look at the agreement, the service and the information involved.

Read customer, vendor and contractor agreements together. Look for consistency in confidentiality, permitted data use, approval requirements and ownership of deliverables. Ask whether existing language adequately addresses the AI use you have identified. A general confidentiality clause should not be treated as an automatic answer to every new workflow.

Also review statements about privacy, security, originality and human review in your marketing and proposals. If you make representations about your controls in insurance applications or renewals, confirm that they reflect actual practice. Discuss coverage questions with your broker; do not assume a policy covers every AI-related problem.

GIVE SOMEONE AUTHORITY TO ACT

A policy needs a person behind it. In a solo business, that may be you. In a team, identify who approves tools, answers questions and can pause a use when something looks wrong.

Give people a clear way to report a concern. If someone uploads the wrong document or discovers an inaccurate output was sent to a

client, they should know whom to contact and what information to preserve. Your response should address the facts, any applicable obligations and the steps needed to prevent a repeat.

Revisit the assessment when you add a vendor, change a workflow or enable a new feature. You do not need to start over each time, but you do need to check whether the change introduces information, access or decisions your current rules do not cover.

CHOOSE ONE IMPROVEMENT THIS WEEK

Start with one workflow that involves customer information or produces something customers rely on. Record the tools used, the information involved, the person reviewing the result and the most important

unanswered question.

Then close one gap. Ask a vendor about its process. Restrict an upload. Add a verification step. Clarify a contractor's obligations. Assign an approver.

NIST's voluntary AI Risk Management Framework and its Generative AI Profile offer a broader foundation for assessing and managing AI risk. They are useful resources, but applying them to your business still requires an honest look at how work gets done.

You do not need to become an AI expert to ask better questions. You do need to know where AI touches your business and who is responsible for the decisions that follow.



Need help turning the answers into a plan?

I help business owners identify how AI affects their operations and translate those risks into practical policies, processes and contract considerations.

Visit michellebufano.com to learn more about my AI risk and governance consulting services.

Further reading

[NIST AI Risk Management Framework](#)

[NIST Generative Artificial Intelligence Profile](#)

This article is for educational purposes only and does not constitute legal advice or establish an attorney-client relationship.



MICHELLE BUFANO

Michelle Bufano is the founder and CEO of Michelle Bufano Business Consulting. She is an experienced and strategic risk management advisor. She uses her legal background to provide counseling and coaching to female founders.

You can contact Michelle via email at:

michelle@michellebufano.com

Follow Michelle on [LinkedIn](#) & [Instagram](#)



MICHELLE
BUFANO

Business Consulting LLC

www.michellebufano.com