May 2026

Moonshot Insider

Insider Tips To Make Your Business Run Faster, Easier and More Profitably

Are You Getting Full Value From the Tools You Own?

Here's a scenario most business owners will recognize: You're paying for software your employees use every day.

Nobody's complaining and things are generally getting done. So, you leave it alone and focus on everything else that needs your attention.

But using a tool isn't the same as fully leveraging it, and that's one of the most common reasons businesses get less from their tools than they paid for.

WHY 'FULL VALUE' MATTERS

Most people measure the value of a tool by whether it runs and if people use it. That's a low bar. A tool can pass both tests and still be costing you more than it's giving back.

Full value doesn't mean the software runs without errors, people log in regularly or tasks get completed.

Achieving full value means employees are actively using features that save time, not just sticking to the basics they learned in training.

Manual tasks aren't simply managed with a separate spreadsheet; they're minimized. The tool seamlessly fits your current processes, and you're not paying for duplicate platforms that handle the same functions. Simply put, the tool should make work easier and faster, with clear benefits like saved time, reduced waste and smoother daily operations.

WHERE BUSINESSES FREQUENTLY LOSE VALUE

The gap between how you use your tools and what they're capable of usually doesn't come from one obvious mistake. It builds slowly across a few common areas:

Underused features are among the most common. When a tool is introduced, employees learn the basics they need and move on. Automation that could reduce repetitive work never gets configured. Built-in reporting never gets set up. Integrations never get activated.

License and subscription drift happens quietly. Seats stay assigned to employees who have left. High-tier subscriptions continue even though the features are never used.

Individually, these don't stand out. Collectively they cost more than any single line item would suggest.

WHAT A TECHNOLOGY PERFORMANCE REVIEW DOES

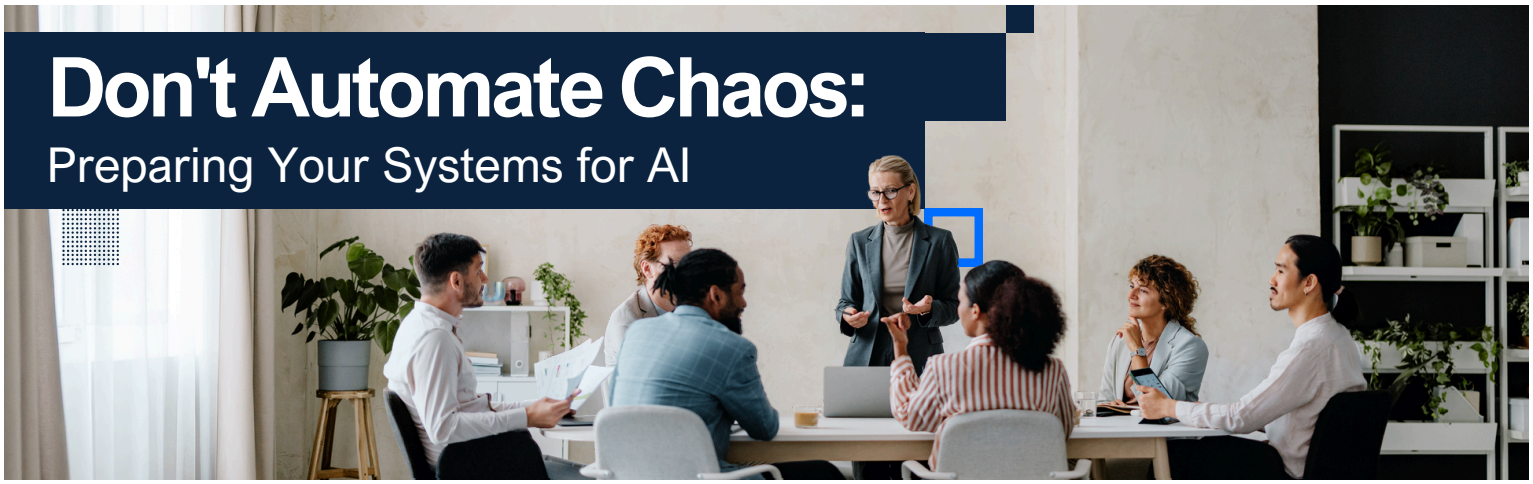
A review examines what tools you have and who's using them, as well as where platforms overlap and where manual workarounds have replaced functionality you already pay for. It also considers what you're spending compared to what you're getting back.

The outcome isn't a list of things to replace. It's a view of where your systems can deliver more, with practical steps your team can take without major disruption.

Key Takeaway:
Using a tool isn't the same as getting value from it. A technology performance review helps you close the gap between what you're paying for and what your business is getting back.

Don't Automate Chaos:

Preparing Your Systems for AI



AI is everywhere right now and the pressure to do something with it is real. Most business leaders are asking how they should be using it, but the more appropriate question is whether their business is ready for it. AI works best in an already organized business. It doesn't fix broken systems or an unclear process. It runs on whatever foundation is already in place, and if that foundation has cracks, AI will find them faster than you.

WHAT AI CAN AND CAN'T DO

Used well, AI helps businesses move faster with the resources they already have. It handles repetitive tasks, drafts communications, surfaces patterns in data and reduces the manual hand-offs that slow work down. For small businesses, those gains add up quickly because the time savings go straight back to the people doing the work.

What AI can't do is fix a disorganized business. It doesn't know what matters most to your organization. It doesn't understand your context the way your employees do. It works within the structure you already have, for better or worse. AI amplifies your systems. It doesn't organize them.

WHAT HAPPENS WHEN YOU AUTOMATE CHAOS

When AI is layered into a business that isn't operationally ready, the damage doesn't show up as a big, obvious failure. It shows up as performance quietly getting worse. The problems that existed before don't go away, they just move quicker and become harder to trace.

In practice, it looks like AI pulling from inconsistent data and producing outputs nobody trusts, employees independently adopting AI tools with no shared standard and sensitive business information flowing through AI systems without clear rules.

The knock-on effects are more complexity, conflicting versions of the truth and security exposure. These aren't disasters. They're distractions that, running at the speed of automation, are expensive.

SIGNS YOUR BUSINESS ISN'T READY TO LAYER IN AI

Readiness isn't about size or budget. It's about whether your current systems and workflows are organized enough to support automation without making your existing gaps bigger.

It's worth slowing down if you haven't reviewed your tools in over a year, if employees regularly use spreadsheets outside your primary systems or if multiple platforms handle similar functions without a clear reason why.

Access permissions that haven't been reviewed recently and manual workarounds that have quietly turned into the official process tell the same story. If your systems aren't aligned, AI will accelerate the inefficiency.

WHAT GETTING READY FOR AI LOOKS LIKE

Preparing for AI doesn't mean a lengthy project or a big upfront cost. It means making sure the foundation is solid before you build on top of it.

That means mapping your core workflows, ensuring your tools reflect how your business operates now, removing redundant systems, cleaning up user permissions and organizing your data so AI has something reliable to work with.

A technology performance review is a natural starting point. It tells you where your systems are aligned, where they aren't and what needs to be sorted before AI can do what it's supposed to do. No forced upgrades. Just a clear look at where you stand and what makes sense to do next.

Key Takeaway:
AI works best when the systems underneath it are already solid. Before layering in new capabilities, make sure your foundation is ready to support it.

Is Your Security Built Into Your Operations or Added On Later?

Marcus had been running his business for 11 years.

Antivirus was running, the team used two-factor authentication and backups were in place. Nothing had ever gone seriously wrong. Then one afternoon he asked a simple question: Who currently has access to our main systems?

WHAT THE ANSWER REVEALED

It took three days to get a clear answer. When it came, it wasn't reassuring. Former employees still had active credentials. Two departments were running duplicate tools neither knew about. Admin permissions had been handed out during busy stretches and never revisited.

Nothing had gone wrong, but nothing was quite right either. Marcus realized his business had security measures, not security structure. There's a difference.

THE GAP BETWEEN MEASURES AND STRUCTURE

Most businesses build security the way Marcus did: reactively. Something prompts a concern, a tool gets added, a setting gets changed and work moves on. Over time, that approach produces a patchwork of protections that each made sense individually but were never designed to work together.

The result is coverage that looks solid until someone looks closely. Access controls that haven't kept pace with how roles have changed. Tools that overlap without anyone realizing it. Processes that work fine for a business of 10 but quietly break down as the team grows. No single decision created the problem. The accumulation did.

WHAT SECURITY LOOKS LIKE WHEN IT'S BUILT IN

Built-in security isn't about having more tools. It's about having the right structure underneath the ones you already have.

That means access is tied to roles rather than individuals, so when someone joins, changes responsibilities or leaves, updates are straightforward. It means systems are reviewed for overlap on a regular basis, so the business isn't paying for redundancy or creating blind spots. It means purchases go through a consistent evaluation so nothing gets added without visibility into what's already in place. And it means onboarding and offboarding follow a standard process every time, because the moments when people enter and exit a business are exactly when security gaps tend to open.

GADGET OF THE MONTH

Dell UltraSharp 52″ 6K USB-C Display

Named a standout in Windows Central's Best of CES 2026, this 52″ 6K display is built for users who live in multiple windows.

Run dashboards, remote sessions, ticket queues and documentation side by side without constant tab switching. A single USB-C cable delivers power, video and data, keeping your desk clean. If you're building a true command center, this is the screen that anchors it.

The Business Technology Growth Checklist

Growing businesses add tools and licenses faster than they review them. These five areas help you spot what's slipping.

- **Tool utilization:** Are you fully using the tools you pay for?
- **Workflow alignment:** Do your tools support how your team works?
- **Overlap and redundancy:** Do you have multiple tools doing the same job?
- **Manual bottlenecks:** Where is work still being done manually?
- **Cost visibility:** Do you have a clear understanding of what you're paying for?

Takeaway: A quick review often pays for itself.

WHY THIS GETS HARDER AS A BUSINESS GROWS

The irony is that growth itself is often what weakens security. A small business with five people has natural visibility. Everyone knows who has access to what.

As the business grows, that visibility fades. More tools, more people, more complexity and less time to step back and review whether the setup still makes sense.

Security doesn't collapse under these conditions. It drifts slowly enough that nothing feels urgent, but steadily enough that the gaps accumulate.

And because it happens gradually, it rarely gets flagged as a problem. Over time, it blends into the way the business runs. With no clear point of failure, it doesn't get revisited.

WHERE A TECHNOLOGY PERFORMANCE REVIEW FITS IN YOUR BUSINESS

Marcus didn't need someone to tell him everything was broken. He needed a structured way to see what had quietly shifted over 11 years and put a framework in place that would hold up as his business kept growing.

A technology performance review looks at whether access controls reflect how the business operates today, where tools overlap or create blind spots, how onboarding and offboarding are handled in practice and the overall level of visibility into who has access to what.

It's not a crisis response. It's a routine check that catches drift before it becomes exposure.

Marcus's story didn't end with a breach; it ended with clarity. That's the goal.

Key Takeaway:

Security that's added on in pieces tends to drift over time. A regular, structured review keeps it aligned with how your business runs.

Cartoon of the month

"Great education. Now let's talk about your 15 years of experience."

COMING NEXT MONTH

VACATION-READY BUSINESS

Most business leaders can't fully step away without wondering what might go wrong while they're gone. That's a sign the business isn't as self-sufficient as it could be.

Next month we're looking at what changes that: reliability, security, automation and visibility. When these four work together, stepping away stops feeling like a risk and starts feeling like something you've earned.