

A Gut-Check on Third-Party Risk: Are You Actually In Control?

Larry Gordon, CAMS | July 14, 2025

When cross-functional teams don't coordinate, especially on tech stack decisions that affect people or compliance, risk exposure escalates quickly.

In a recent case covered by *Wired*, McDonald's used an AI-powered chatbot from ParadoxAI to assist with hiring ([McDonald's AI Hiring Bot Exposed Millions of Applicants' Data to Hackers Who Tried the Password '123456'](#)). According to reporting and legal filings, candidates allegedly experienced missed interviews, non-responses, and rejections for inaccurate reasons. While the core issues are still under litigation, the signals point to a larger breakdown: HR implemented a high-impact system without documented collaboration with cybersecurity, compliance, or legal teams.

This is what happens when business units operate independently on third-party technology decisions. Without shared oversight, risks to security, privacy, fairness, brand reputation, and regulatory compliance go unaddressed until they are already in play.

Here's what was likely missing:

- No structured cross-functional review of the third-party's operational or security controls
- No independent validation of system performance (e.g., fairness testing, audit logging, or pen testing)
- No clearly defined residual risk analysis after implementation

This is not speculation. These are known red flags that have played out in countless operational risk failures across industries.

If your company can onboard a third-party vendor that touches employee or customer data—without the CISO, Legal, HR, and Compliance all reviewing the risk posture—you are operating with a blind spot.

These are not technology failures; they are process failures. Risk leaders must enforce a repeatable structure that:

- Triggers third-party risk reviews based on impact and sensitivity, not just budget or project size.
- Defines control expectations for AI, automation, and customer-facing tools.
- Requires post-implementation testing and feedback loops from actual users.

Ask yourself:

- Does our third-party onboarding process force coordination between risk stakeholders?
- Is there a formal step for identifying the *inherent risk* and validating the *residual risk*?
- If something went wrong tomorrow, would leadership already know who was accountable?

If you're not sure, start with a Risk SWOT assessment or an infrastructure review. These issues don't stay invisible for long—and when they show up, they rarely stay small.

Don't wait for a "WHAT THE R*SK!"[®] moment

Get ahead of blind spots, breakdowns, and boardroom surprises before they define your next chapter.

Web: GordonRiskSolutions.com

Email: info@gordonrisk.com

Phone: (614) 859-0053

LinkedIn: [Gordon Risk Solutions](#)

This article is part of The Blind Spotter series—quick reads on risk you don't want to overlook.