TERAMIND

Predictive Edge | Powered by brAIn

The AI Risk Register Gap:

What Most IRM Frameworks Are Still Missing

Why Traditional Risk Frameworks Fail at AI Risk

Traditional IRM frameworks categorize risk by **domain**: credit, market, operational, compliance, strategic, reputational. This worked when risks stayed in their lanes.

AI risk doesn't stay in its lane.

Consider:

A financial analyst uses Microsoft Copilot to draft a client presentation, and Copilot pulls confidential merger details from an email thread to "enhance" the summary.

Where does this risk live?

Operational Risk (process failure)? Cyber Risk (data exfiltration)? Compliance Risk (MNPI disclosure)? Third-Party Risk (Microsoft vendor)? Reputational Risk (client trust)? Legal Risk (SEC enforcement)?

The answer:

All of them. And that's the problem. Your risk framework is built on discrete categories. AI risk is cross-cutting, emergent, and contextual.

AI Risks Falling Through the Cracks

1. Shadow AI (The Unauthorized Tools)

Employees use personal ChatGPT accounts because IT hasn't provisioned enterprise tools. Risk teams don't know these tools exist. IT doesn't monitor personal AI accounts. Sensitive data has been uploaded for months before discovery.

The gap

Shadow AI is simultaneously a procurement failure, data governance failure, policy failure, and technology risk. Which risk owner is accountable?

2. Prompt Injection & Data Leakage (The Behavioral Risk)

Account Executives ask Copilot to "summarize my last 10 customer emails." Copilot ingests confidential pricing, contract terms, competitive intel, then auto-shares summary with the entire team.

The gap

This isn't a system vulnerability. It's **authorized users doing their jobs with approved tools, creating risk through normal behavior. Your cyber controls see authorized access.** Your operational risk framework sees an approved process. Nobody sees the risk until the M&A strategy is in a sales deck.

Traditional risk frameworks don't account for "the tool is working as designed, but the design creates risk."

3. AI Hallucination & Automated Decision Risk

A compliance officer uses AI to review 500 vendor contracts for GDPR clauses. AI flags 480 as compliant. Auditor finds 50 contracts missing required agreements. AI hallucinated compliance.

The gap

Traditional risk frameworks assume **human review validates outputs and controls are deterministic.** AI breaks both, it's too fast for full human review and introduces probabilistic controls (AI reviewed it, with 10% error rate). How do you measure residual risk when your control is "AI reviewed it, human spot-checked 5%"?

4. Autonomous Agent Risk (The Superhuman Execution Problem)

Employee enables an AI agent to "monitor their inbox and auto-respond to routine requests." The agent processes 300 emails/hour, including one from a regulator. Agent auto-responds with data that should have triggered legal review.

The gap

Your operational risk framework assumes **human-speed execution.** AI agents can create 1,000 compliance violations in the time it used to take for one. Traditional frameworks assume human-in-the-loop at decision points. AI agents remove the human.

The Solution: AI as a Risk Multiplier, Not a Risk Category

Don't force AI into existing categories. **Recognize AI as a cross-cutting risk dimension that amplifies every traditional risk type.**

Instead of asking "Is this operational risk or cyber risk?", ask: **"How does AI amplify the likelihood or impact of risks we already manage?"**

Framework: AI Risk Overlay

Traditional Risk	AI Amplification	Controls Needed
Data Exfiltration (Cyber)	**HIGH** AI tools ingest data at scale	DLP for AI traffic, prompt monitoring, approved tool list
Data Exfiltration (Cyber)	**HIGH** AI agents auto-violate at machine speed	Activity monitoring, kill-switch, human-in-loop for regulatory work
Third-Party Dependency	**MEDIUM** Over-reliance on single AI vendor	Multi-vendor strategy, contractual SLAs, data portability
Reputational Damage	**HIGH** AI hallucinations misrepresent company	Output validation, AI content disclosure, brand monitoring

This approach:

- ✓ Preserves existing risk categories (no framework overhaul)
- ✓ Makes AI risk tangible (tied to risks board already understands)
- ✓ Assigns clear ownership (existing risk owners assess AI amplification in their domain)

The Solution: AI as a Risk Multiplier, Not a Risk Category

Month 1

AI Risk Discovery

Ask every risk owner: "If employees in your domain used AI tools, what could go wrong?"

Output: AI risk heat map by domain

Month 2

Control Gap Assessment

For each AI-amplified risk: Do we know when employees use AI? Can we prevent unauthorized AI? Do employees know what's prohibited? Can we detect AI errors before impact?

Output: Control maturity scorecard

Month 3-6

Prioritized Remediation

Prioritize based on: (1) Regulatory exposure, (2) Financial impact, (3) Adoption velocity

Output: Remediation roadmap with ownership and timelines

What Boards Should Ask This Quarter

- Show me where AI risk appears in our enterprise risk register.
- If Copilot made a regulatory error at scale tomorrow, how would we know, and how fast could we contain it?
- Can we detect when employees use unapproved AI tools? Can we see what data they're uploading?
- Which of our top 10 risks are amplified by AI, and by how much?

If you can't answer these, you're managing 2025 risks with 2015 frameworks.

Conclusion

The AI risk register gap exists because **we're trying to manage tomorrow's risks with yesterday's frameworks.**

AI isn't a risk type - i**t's a risk accelerant.** The solution: overlay AI amplification assessment across existing risk categories, assign AI risk ownership to existing risk functions, implement AI-specific controls while preserving traditional ones, and measure AI adoption vs. control maturity.

The organizations that solve this first won't just manage AI risk better - they'll unlock AI value faster. The real competitive advantage isn't adopting AI first. It's adopting AI safely, at scale, with confidence.

The question isn't whether AI creates new risks. It's whether your risk framework can see them before your regulators do.

Close the AI Gap and Secure the Risks

Book a Demo

TERAMIND

Predictive Edge | Powered by brAIn

www.teramind.co