riskonnect.

THE AI RISK SHIFT:
5 Risks and 5 Strategic Responses for GRC and Resilience Leaders



AI has already reshaped your risk profile. It's in your vendor platforms and operational workflows. It influences decisions and reduces the time you have to respond when something fails. However, most GRC and resilience frameworks are still built for a slower, more linear risk environment.

AI creates new dependencies across your organization. It also makes decision logic harder to trace, and its risks span teams. If you treat AI integration as a technology initiative instead of a resilience issue, you risk losing visibility and increasing fragility. The best approach is knowing where AI adds exposure – but also where it helps manage risk.

RISK ONE

AI Hides in Your Supply Chain

Your vendors' platforms and systems include AI you can't see. Those vendors rely on providers and infrastructure that extend beyond your contractual visibility. As those layers stack up, your supply chain grows more complex without more transparency.

When disruptions happen, that lack of visibility makes it harder to pinpoint what failed. Your business impact analysis may underestimate critical dependencies. Recovery plans may assume vendor stability that no longer exists. Over time, concentration risk intensifies, and leadership loses sight of total exposure.

HOW AI HELPS

Build Structured Transparency and Real-Time Awareness

You can reduce hidden exposure by requiring vendors to disclose how and where they use AI. For example, mapping your AI-enabled vendors to your critical services allows you to test how data failures would affect recovery. However, the value of that visibility depends on how well the data integrates into your own frameworks.

When third-party risk data feeds automatically into your impact analysis, resilience becomes more holistic. By positioning AI-enabled tools to monitor vendor threat detection, you create earlier warning signals across your business – and that visibility is an advantage.

Continuous monitoring can flag vendor instability and detect anomalies earlier than manual reviews. The same technology that may expand your dependency network can also help you see it more clearly.



RISK TWO

AI Decisions Leave You Dependent

AI-based tools now drive core operations. These systems rely on structured automation trained on historical data. As adoption expands, those models grow from support tools to decision authorities.

The risk emerges when teams stop interrogating outputs because they're overconfident in the automations working correctly. As that reliance grows, human review narrows, and escalations slow. Eventually, few people might be able to explain why certain decisions have been made – only that their models produced them.

Imagine a risk-scoring engine that determines which vendors receive more due diligence. Over time, staff rely entirely on the model's output. When business conditions change or new factors emerge, the model continues to apply outdated weightings. No one thinks to question the scoring distribution because review processes aren't in place. Vendor exposure quietly grows; not because the model is broken, but because oversight has disappeared.

That's not a sudden failure. It's a structural dependency. When decision-making is concentrated inside automated processes without clear override points, your business becomes beholden to assumptions it might no longer understand. During disruption, that confusion slows response and limits corrective action.

HOW AI HELPS

Simulates Disruption and Exposes Weak Points

AI doesn't have to create dependency. The same modeling capabilities can strengthen resilience when used deliberately.

Instead of allowing models to operate as silent authorities, you can use AI to generate alternative scenarios and expose how its outputs change under stress. Simulation tools can show concentration points and highlight cascading impacts before they happen.

When you define clear override thresholds and regularly test how the system behaves, automation becomes more transparent. With well-established guardrails, AI is a source of support during a crisis rather than instability.



RISK THREE

AI Accuracy Drops During Change

Generative AI and large language models operate differently from classic machine learning systems. They don't apply fixed rules to structured inputs. They generate outputs based on probability and context.

Accuracy in these systems exists on a slope. When the context given to them is incomplete or ambiguous, the quality of the outputs degrades. Generative AI can produce overconfident but inaccurate conclusions or misinterpret nuance. The model doesn't know when it's wrong. It depends entirely on the quality of information it receives and the structure of its prompts.

AI systems depend on patterns; disruption confuses those patterns. During a crisis, teams rely on AI to interpret regulatory guidance or analyze operational updates. When that information is incomplete or contradictory, the model may still generate what looks to be a coherent answer; however, that answer is based on limited context. Supply chain shocks, cyber incidents, and even regulatory changes alter data inputs in ways the AI training data didn't expect. With more changes, the model becomes less accurate.

A disruption could occur where new regulatory guidance affects vendor operations. A team may use generative AI to interpret the update and summarize its implications for their suppliers. If the model receives incomplete documentation or outdated policy language, it could produce a confident interpretation that misrepresents the requirements. The analysis looks reasonable, but with a closer look, it shows gaps in the data provided.

Inaccurate interpretations during a crisis compound the impact. A misleading summary of regulatory obligations might delay mitigation. An incorrect interpretation of exposure might shift response priorities. Few continuity programs treat AI failures like these as disruption scenarios, but flawed outputs can intensify losses, even when systems are still online.

HOW AI HELPS

Integrates Model Performance Into Continuity Planning

Generative AI can also strengthen accuracy when used deliberately. It can compare internal assumptions against benchmarks and identify logical gaps in planning. When paired with structured prompts and validation, it can challenge rather than reinforce reasoning.

AI can surface contradictions in recovery strategies and evaluate whether risk statements align with available data. Used this way, AI models can sharpen judgment.

With this framework, AI accuracy grows on the same slope. Instead of relying on static recovery assumptions, you can use live operational data to quickly reassess criticality. That allows your BIA to evolve constantly as conditions change, bolstering your response planning.

RISK FOUR

AI Innovation Moves Faster Than Your Controls

AI regulation evolves quickly, especially in highly regulated industries, while internal controls normally lag innovation. Without comprehensive governance, you might struggle to document usage, validate logic, and define accountability for AI.

After an incident, regulators and auditors scrutinize oversight as closely as they scrutinize operational failures. Inconsistent documentation and fragmented reporting increase that exposure. Even when teams manage models effectively, leadership may lack clear evidence of governance.

HOW AI HELPS

Embeds AI Governance Into Resilience Frameworks

Closing governance gaps requires more than assigning oversight to one function. AI governance becomes stronger when risk teams operate under one framework, with clearly defined ownership over AI risk decisions. When model usage, dependencies, and impacts are documented, oversight becomes defensible and consistent.

AI can support stronger governance when you embed it into monitoring and documentation workflows. Automated logging, traceability, and anomaly detection reduce manual oversight and create clear audit trails. Governance becomes continuous, not periodic, and allows for AI expansion without sacrificing control.

RISK FIVE

AI Oversight Is Still Siloed

AI touches nearly every function in your business. When each team evaluates exposure independently, blind spots multiply. One function may understand model logic, another may track vendor contracts, and another may own recovery planning. In that scenario, no single team sees the complete picture.

During disruption, fragmented oversight interrupts decision-making. Leadership may lack consolidated insight into AI dependencies or cross-functional exposure. That misalignment creates hesitation when clarity matters most.

HOW AI HELPS

Unifies Risk Domains Around Shared Intelligence

When risk functions operate from a shared AI framework, fragmentation decreases. That common structure makes consolidated dashboards possible, giving everyone a clearer view of AI-related dependencies and performance. Cross-functional scenario planning then reinforces that alignment.

AI also allows even further integration across risk domains. Shared dashboards and automated data aggregation provide leadership with a consolidated view of exposure. Instead of reconciling separate reports, executives can see interconnected risk in one place.

Designing Resilience for AI-Driven Risk

AI-related disruption won't wait for your governance model to mature. By the time weaknesses surface, the structural shift has already occurred. AI now influences how vendors operate, how decisions are made, and how quickly an impact can spread. Treating it as a side initiative within IT or innovation leaves resilience exposed.

A more durable approach recognizes AI as a structural change across all risk functions. Alignment becomes part of the operating model, not a reaction to failure.

AI can increase fragility when it creates more dependencies without visibility or automates decisions without guardrails. However, that same technology also has many benefits:

- **Real-Time Risk Awareness:** Revealing hidden vendor dependencies and anomalies.
- **Smarter BIA:** Stress-testing decision systems and recovery plans.
- **Faster Incident Decisions:** Quickly challenging assumptions and exposing gaps in logic.
- **Stronger Governance:** Monitoring model performance and validating outputs.
- **Integrated Enterprise Resilience:** Providing a unified view of risk exposure.

The difference is whether governance keeps pace with adoption.

The issue isn't whether AI introduces risk; it does. The issue is whether your resilience framework merely contains the risk or uses it to your advantage.



Is your resilience framework prepared for the AI risk shift? Evaluate your readiness with Riskonnect's AI Risk and Resilience Readiness Assessment.

About Riskonnect

Riskonnect is the leading integrated risk management software solution provider. Our technology empowers organizations with the ability to anticipate, manage, and respond in real time to strategic and operational risks across the extended enterprise.

More than 2,700 customers across six continents partner with Riskonnect to gain previously unattainable insights that deliver better business outcomes. Riskonnect has more than 1,500 risk management experts in the Americas, Europe, and Asia-Pacific. To learn more, visit riskonnect.com.

CONNECT NOW →

Integrated Risk Management Solutions:

INSURABLE RISK
- Risk Management Information System
- Claims Management
- Billing
- Policy Administration
- Health & Safety

ACTIVE RISK MANAGER

HEALTHCARE RISK & PATIENT SAFETY

BUSINESS CONTINUITY & RESILIENCE
- Business Continuity Management
- Operational Resilience
- Emergency Notifications
- Crisis Management
- Threat Intelligence

GOVERNANCE, RISK & COMPLIANCE
- Enterprise Risk Management
- Third-party Risk Management
- Environmental, Social & Governance
- Compliance
- Internal Audit
- Internal Controls Management
- Policy Management
- Project Risk Management
- IT Risk Management
- AI Governance
- Business Strategy

04.26

Copyright © 2026 Riskonnect Inc. All rights reserved.