keepit

Key takeaways

How to future-proof your resilience strategy

Future-proof isn't a buzzword; it's a design choice.

Many companies are adopting AI because of pressure, hype, or fear of falling behind. Organizations tend to underestimate the cost of AI, the planning required, and the potential for unintended consequences when AI is allowed to act at scale. At the same time, the opposite challenge arises when people within the organization adopt AI whether the company is ready or not. If leadership is not intentional in providing approved tools, thinking through policies, and designing guardrails, shadow AI will fill the gap.

In a recent Keepit webinar, a panel of experts outlined critical risk areas IT and business leaders must address when developing AI capabilities. Read on for the key takeaways below.

Risks and challenges

Unintended consequences at scale

A person may make one mistake. An AI agent may make 20.000 mistakes in seconds, increasing your risk exponentially.

Vendor risk

Even if your own environment is well controlled, a vendor's AI usage may introduce compliance, privacy, or operational risk.

Shadow AI

When organizations do not provide sanctioned tools, employees will use consumer AI tools anyway, often without proper safeguards.

Data exposure and integrity risk

Because SaaS tools are highly connected, AI may access more data than intended, increasing to leakage or corruption risk.

Agentic AI risk

Autonomous agents can act across systems, creating major risk if permissions, oversight, or rollback controls are weak.

How to adopt AI capabilities with intentional control

A disciplined three-step approach to responsible AI

Step 1:
Define outcome

- Fall in love with the problem, not the solution
- Start with business outcomes, avoid AI for AI's sake

Step 2:
Control and build resilience

- Ensure observability and traceability
- Implement technical and behavioral guardrails (human and agentic)

Step 3:
Enable the organization

- Education and Human-in-the-loop
- Provide sanctioned tools as well as training to curb shadow AI

Resilience requirements

Given the discussed challenges and risks, the strong tie between AI adoption and resilience planning cannot be ignored. To prepare, organizations should be able to:

- [ ] Detect when AI has done something unexpected
- [ ] Observe and trace what changed, when, and where
- [ ] Identify a clean point in time to return to
- [ ] Roll back safely and confidently
- [ ] Rely on immutable records or backups that cannot be altered

Actionable next steps

Turning AI into real outcomes requires discipline, not just experimentation. The webinar offered actionable next steps focus on starting small, maintaining control, and ensuring you have the visibility and resilience needed to move forward with confidence.

1. Pick one small, high-value use case with a clear business outcome.
2. Map the data and systems involved before giving AI access.
3. Set guardrails around permissions, scope, and approved tools.
4. Create observability so you can monitor what AI is doing.
5. Ensure rollback capability with trusted backups and immutability.
6. Educate employees on approved use and critical thinking.
7. Review vendor AI practices before exposing sensitive data.
8. Start small, test often, and scale only when controls are proven.

Responsible AI adoption requires staying resilient as automation and complexity increase. Having a strong backup and recovery foundation becomes critical to detect issues, preserve trusted data, and recover quickly. The more you rely on AI, the more essential it is to have immutable, reliable recovery that keeps you in control.

Peer insights on AI and disaster recovery

Read our latest report based on insights from more than 300 senior IT decision-makers across the U.S., Europe and APAC, exploring how rapidly evolving AI environments are impacting disaster recovery (DR) strategies.

Download now

keepit® Your data. Here today. Here tomorrow.

Keepit provides a next-level SaaS data protection platform purpose-built for the cloud by securing data in a vendor-independent cloud to safeguard essential business applications, boost cyber resilience, and future-proof data protection. www.keepit.com

bsi ISO/IEC 27001 Information Security Management CERTIFIED