



A strategic approach to managing **AI risks**

Cybersecurity Awareness Month **2025**



A strategic approach to managing AI risks



Adam Ihlenfeldt
BDO Belgium



Supported by:
Sacha Blasiak-Priestley
Director, Cloud Security
BDO Canada

Artificial intelligence (AI) is reshaping business at an unprecedented pace. Generative AI, in particular, has accelerated far beyond expert predictions, compressing decades of anticipated progress into just a few years.

By 2028, 62% of business leaders expect AI to be embedded across all areas of their organisations ^[1]. But while 45% see AI as a significant opportunity, 56% are concerned with the cybersecurity and privacy risks that accompany this rapid adoption.

“

We're at a pivotal moment where AI is no longer theoretical. It's in everyone's hands. That accessibility is fueling innovation, but it's also creating blind spots.”

Kirstie Tiernan, AI Leader, BDO USA

[1] [BDO Tectonic States](#)



Generative AI amplifies many of the cybersecurity risks organisations have faced for years, including social engineering, data leakage, and governance gaps. Nearly half of surveyed leaders report that data security concerns are holding back further investment in AI ^[1]. The risks are tangible. For example, The Netherlands' childcare benefits scandal, driven by an early machine learning algorithm, led to thousands of innocent families being wrongly flagged as fraudulent. The consequences included financial hardship, public outrage, and even loss of life. This case highlights the reputational, legal, and ethical risks that can arise when AI systems lack proper oversight.

A group of four people are walking along a path under a large, white, arched metal structure. In the center, a man in a light-colored suit and blue tie holds a tablet. Above him, a cloud of red and black icons floats, representing various security threats such as viruses, locks, warnings, and data loss. To his left, a woman in a black coat and red scarf walks. To his right, a man in a black coat and sunglasses walks, and further right, a woman in a light-colored jacket and blue jeans walks. The background shows more of the white arches under a clear blue sky.

While risks around data, privacy, and model bias are real, we must also consider the broader impact on workforce dynamics, adoption, and potential overreliance on AI.

Thoughtful planning that integrates technology with human capital and change management can significantly accelerate ROI on AI investments.”

Rocco Galletto, National and Global
Cybersecurity Leader, BDO Canada

[1] [BDO Tectonic States](#)

Building a cohesive AI governance strategy

To keep pace with technological change and evolving legislation, organisations should establish AI governance committees with cross-functional representation.

A cohesive governance strategy includes:

- Mapping global regulations and standards to maintain compliance across jurisdictions (such as the EU AI Act, NIST AI 100-2, and ISO/IEC 42005:2025).
- Aligning AI initiatives with organisational priorities, such as customer experience, operational efficiency, and innovation.
- Understanding strategic alignment opportunities across the business. Organisations that embed AI into enterprise-wide strategies will typically achieve a better return on investment.

AI should be integrated into existing risk, compliance, and governance frameworks, with safeguards applied throughout its lifecycle.

“

We recommend having an AI strategy, someone who is accountable for AI, and an AI governance committee consisting of multiple stakeholders. This ensures it's not a single point of failure.”

Jason Gottschalk, Partner Cybersecurity, BDO UK



Practical steps to take today

Risk often stems from a lack of understanding. By fostering a culture of awareness, organisations can turn unknown risks into manageable challenges.

Nearly half of organisations are already providing employee training on secure and ethical AI use, and 46% are deploying AI-specific security tools^[2].

To address today's risks, organisations should:

- Build employee awareness and skills for secure, ethical AI usage.
- Invest in advanced tools to detect and mitigate AI-related threats, such as data leakage and unauthorised access.
- Limit exposure to sensitive information through stricter access controls and policies.
- Conduct AI impact assessments to identify and address potential risks.

AI is expected to have the greatest impact in cybersecurity (55%), compliance monitoring (52%), and supply chain management (50%)^[3].

The time to act is now.

[2] [IDC BDO Security Survey](#)

[3] [Global Landscape 2025](#)



Future-proofing AI Adoption

Organisations that embrace a 'fail fast, learn faster' mindset are better positioned for successful AI integration. AI adoption is not just about innovation - it's about building resilience and agility in a dynamic business environment.

As technology evolves, it's essential to set clear goals, continuously monitor AI performance, update key risk indicators, and champion regulatory changes. This approach enables organisations to build resilient governance that evolves with AI, rather than resisting change and risking exposure to emerging threats.

DOWNLOAD THE REPORT

REGISTER FOR OUR WEBINAR

EXPLORE THE CYBER RISK ANALYZER



References

- [1] [BDO Tectonic States](#)
- [2] [IDC BDO Security Survey](#)
- [3] [Global Landscape 2025](#)

'BDO', 'we', 'us', and 'our' refer to one or more of BDO International Limited, its network of independent member firms ('the BDO network'), and their related entities.

The BDO network is an international network of independent public accounting, tax and advisory firms which are members of BDO International Limited and perform professional services under the name and style of BDO (hereafter: 'BDO member firms'). BDO International Limited is a UK company limited by guarantee. It is the governing entity of the BDO network.

Service provision within the BDO network is coordinated by Brussels Worldwide Services BV, a limited liability company incorporated in Belgium.

Each of BDO International Limited, Brussels Worldwide Services BV and the BDO member firms is a separate legal entity and has no liability for another entity's acts or omissions. Nothing in the arrangements or rules of the BDO network shall constitute or imply an agency relationship or a partnership between BDO International Limited, Brussels Worldwide Services BV and/or the

BDO member firms. Neither BDO International Limited nor any other central entities of the BDO network provide services to clients.

BDO is the brand name for the BDO network and for each of the BDO member firms.

© Brussels Worldwide Services BV October 2025

