KPMG

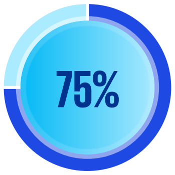
AI security framework

GenAI was utilized in the creation of this image

The sophistication of AI target-based cyber attacks and cyber incidents related to vulnerable AI systems are on the rise. These attacks and the larger attack surface present an urgent the need for a holistic approach to your organizations AI landscape, securing critical systems, and responding to adversarial AI attacks.

AI is being embedded into a wide array of business processes but…

…AI security remains a new frontier.



of surveyed companies will shift from piloting to operationalizing AI by 2024.

Source: Gartner Inc., U.K., June 22, 2020

of surveyed companies don't have tools in place to secure their ML systems.

Source: Microsoft, Redmond, March 19, 2021

$135B

Artificial Intelligence market size by 2025.

Source: Dragos 2020 ICS Cybersecurity Year in Review

Developing ethical AI remains an impending organizational responsibility

Core components of Trusted AI

Resilience

Technical robustness of your AI, its agility across platforms, and resistance against cyber threats.

Integrity

Checking the algorithm integrity and data validity, including lineage and appropriateness.

Fairness

Ensuring models are free from bias, free from prejudice, and that restricted protected attributes are not being used.

Explainability

The topic of understanding the decision-making process.

KPMG AI framework domains

The KPMG AI security framework is a set of controls that organizations can leverage to assess and manage the risks associated with the implementation and use of AI systems. The framework is based on both NIST CSF and ISO standards, and is organized in four domains that cover the critical aspects of securing AI. Monitoring these controls enables the responsible use of AI systems, and effective management of AI risk—by assessing the program, addressing secure processes, respecting personal data, and preparing to respond to potential incidents.

Assess (36 Controls)	Secure (52)	Respect (33)	Respond (29)
Asset management	Lifecycle security	Data risk management	Analysis
Pipeline governance	Resiliency	Data usage	Improvements
Security risk assessment	Supply chain security	Notice and consent	Mitigation
Security risk management	Anomaly and event detection	Privacy by design	Remediation
Training and awareness	Continuous ai monitoring	User rights	Response planning

KPMG services

KPMG AI security services is a leading suite of AI security service offerings that provide effective security approaches for AI systems and models. Our risk-based approach provides targeted prioritization to secure an organization's most critical systems.

	Services	Objectives
1	AI security coverage and maturity	Understand the current coverage and opportunities for better security over AI systems.
2	Peer benchmarking	Determine where Incyte sits in comparison to peers on AI security maturity.
3	Future state roadmap	Identify and prioritize key efforts in a future-state roadmap to evolve your current posture.

Top six reasons to secure AI

1 Ensure compliance with global AI regulations

Effectively enable our AI models to be compliant with the rapidly growing list of global regulations.

Explain to the customer (or regulator) so that they understand.

2 Empower innovation in AI systems while keeping them safe

Keep apace of innovation without compromising security.

Improve our AI rate of innovation and growth.

3 Drive cultural change for AI use

Ensure our workforce is using our AI systems properly.

Stop leakage of confidential or propriety data from AI models.

4 Secure our models from cyber attacks

Protect against adversarial attacks, insider threats, and nation states.

Align current security controls work for AI systems.

5 Monitor our AI performance

Measure effectiveness of AI systems.

Track key performance metrics.

Determine if our investment in AI was worth it.

6 Improve the use of AI systems at scale

Effectively use AI to automate processes across our organization.

Gain visibility into the growing number of AI models in our environment.

Misuse of AI and ungoverned AI

The exploitation of Artificial Intelligence systems can cause disruptions and have unprecedented consequences. Given the pervasive nature of AI and data, **C-suite and senior executives believe current issues associated with AI are problems of unregulated AI, which pose a challenge for organizations to keep pace.**

Misuse of AI

Fueled by the large amounts of available data, AI-based attacks on privacy have become commonplace. Misuse of AI models can lead to stolen PII information, system access outages, and biased decision making—impacting an organization's ability to conduct business.

Ungoverned AI

Insider threats represent the most dangerous and costly risk to an organization's AI security. Therefore, guardrails must be established to ensure that AI systems are governed properly, used responsibly, and leveraged appropriately.

of data inputted into ChatGPT is confidential. Everyday small incidents of sensitive data leakage could lead to enormous financial implications and reputational damage.

Source: Cyberhaven, February 28th, 2023

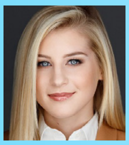
of surveyed executives believe that generative AI can have a negative impact on their organization's trust if the appropriate risk management tools are not implemented.

Source: KPMG, April 2023

To learn more about the KPMG AI Security Framework click here or get in touch below:

Matthew Miller
Principal,
AI Security
KPMG US
T: +1 212 954 4648
E: matthewpmiller@kpmg.com

Katie Boswell
Managing Director,
Cyber Security Services
KPMG US
T: +1 908 433 3417
E: katieboswell@kpmg.com



Kristy Hornland
Director,
Cyber Security Services
KPMG US
T: +1 425 281 5251
E: khornland@kpmg.com

Learn about us: in kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.