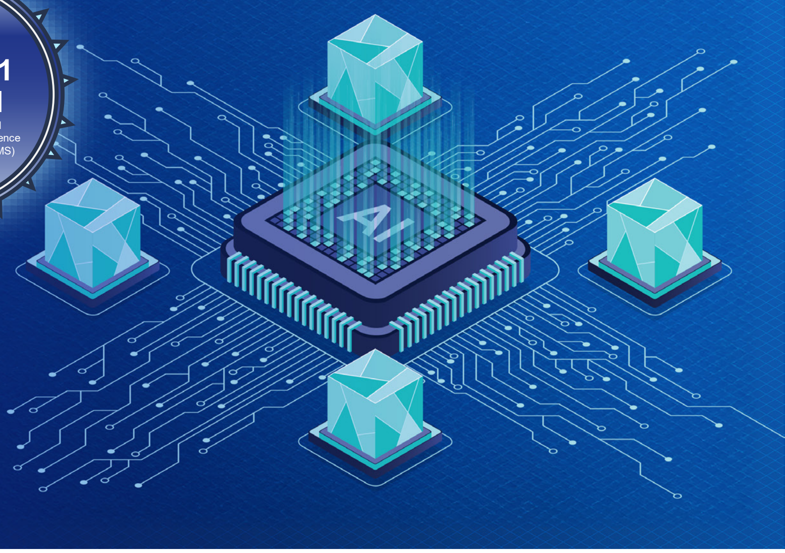
KPMG

ISO 42001 Certified

World's first international standard for Artificial Intelligence Management Systems (AIMS)

AI security testing by KPMG



AI systems and models protection

KPMG Cyber Managed Services

The challenge

AI systems present a broader attack surface than traditional applications, which renders them **even more** vulnerable. The significant increase in AI utilization within organizations, and proliferation of cyber attacks means that now, more than ever, **AI security matters.**

82%

CEOs rank cybercrime and cyber insecurity at the top of the near and long-term risk radar.

2025 KPMG US CEO Outlook

Four key pressures are driving the need for change:

AI adoption:
Rapid AI integration introduces new vulnerabilities without oversight.

Development:
App developers are tasked to innovate faster, adding complexity.

Talent:
Organizations struggle to find talent needed for testing at scale.

Remediation:
Organizations still fail to meet remediation SLAs, increasing risk exposure.

67%

Two out of three organizations report a lack of essential talent and skills to meet their security requirements.

World Economic Forum Global Cybersecurity Outlook 2025

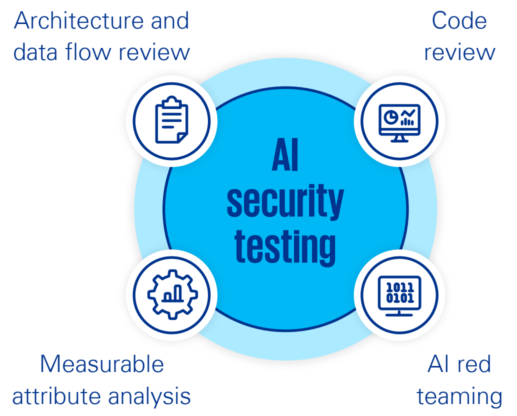
The KPMG solution

AI security testing by KPMG LLP empowers organizations to confidently protect their AI systems and models from vulnerabilities.

Our comprehensive approach, based on MITRE Atlas and OWASP Top 10 for LLMs, provides targeted testing of your AI systems, with a range of options that span the entirety of your AI ecosystem.

Key features

- Prioritized approach enables you to focus on the most critical risks and remediation actions.
- Repeatable testing methodology establishes standardized, scalable processes for ongoing AI security assessments.
- Upskilled and augmented resources empower client teams with advanced skills and knowledge for future AI testing.
- Reporting with actionable findings provide clear, actionable insights to drive security improvements.



Architecture and data flow review
Code review
AI security testing
Measurable attribute analysis
AI red teaming

AI security testing by KPMG capabilities

Architecture and data flow review
Thorough review of where the AI system sits in the environment and the various network connections.

Code review
Informed by software composition analysis (SCA) results, KPMG personnel perform line-by-line code review of applications to find security and logic flaws.

Measurable attribute analysis
KPMG will help define and score various categories of prompt injections and LLM decisions related to our proprietary Trusted AI measurable attributes.

AI red teaming
KPMG streamlines manual penetration testing to expose vulnerabilities throughout AI systems.

AI deployment lifecycle

1 | Data ingestion
Collect and process data from various sources. Secure and validate AI model sources and content.

2 | Data storage
Securely store raw and processed data for model use. Implement strict access controls to training data.

3 | Data preprocessing
Clean, structure, and validate data to ensure quality. Protect the model from malicious data input.

4 | Model training
Develop and train AI models using prepared datasets. Prevent tampering or theft of the model.

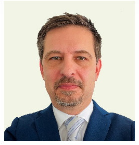
5 | Model serving
Deploy models to production environments, typically via APIs. Secure the surrounding environment.

6 | User interface
Enable end users to interact with outputs through applications or dashboards. Validate user inputs and prevent data leakage.

AI security testing by KPMG is part of a broad suite of Cyber Managed Services.
These fully managed offerings — powered by AI, automation, and leading technologies, and backed by our skilled teams — provide the security, confidence, insight, and visibility you need to help fortify your enterprise digital defenses.

- Managed Identity Services
- Managed Cyber Risk
- Managed Security Testing
- Cyber Threat Management

To learn how you can benefit from AI security testing by KPMG or any of our other Cyber Managed Services offerings, get in touch.



Evan Rowell
Managing Director, Advisory,
Cyber Managed Services
KPMG LLP
T: 704-219-8109
E: erowell@kpmg.com

Wes Cole
Director, Advisory,
Cyber Managed Services
KPMG LLP
T: 662-782-1811
E: westoncole@kpmg.com

Learn more about us: in | kpmg.com

Some or all of the services described herein may not bepermissible 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.