



Cyber risks with large language models





Security is a common feature across the evolving regulations

Core Governance Principle	Fairness Fairness	Explainability	Integrity of Data	Security & Resiliency	Accountability	Privacy	Risk Approach
Description of Principle	Fair and equitable outcomes across different groups	Ability to explain how Al outcomes were achieved	Leverage high- quality, appropriate data with lineage	Design AI to operate as intended with security	Human responsibility for AI decisions outcomes	Respect and protect privacy rights of consumer data	Targeted risk identification and assessment
Global Regulatory Guidance	7						
National Al Initiative Act	✓	✓	✓	✓		✓	✓
AI in Government	✓		✓	✓	✓		
The National Al Research Resource Task Force				✓	✓	✓	
	✓	✓	✓	✓	✓	✓	✓
NIST AI Risk Framework FHFA AB 2020-02	✓	✓	✓	✓	✓	✓	✓
NAIC Principles on AI	✓	✓		✓	✓	✓	✓
Federal Trade Commission	✓		✓		✓		
EU Artificial Intelligence Act	✓	✓	✓	✓	✓	✓	✓
EU Digital Services Act	✓			✓	✓	✓	✓
OECD Principles	✓	✓			✓	✓	✓
Social Principles of Human Centric Al	✓	✓		✓		✓	
AIST ML Quality Management Guideline	✓	✓		✓		✓	
Brazilian Al Strategy	✓	✓				✓	
Brazilian Al Bill		✓					
Al National Policy (Chile)		✓		✓		✓	
Al National Plan (Argentina)	✓			✓		✓	



Singapore has released it's own guidelines

Cyber Security Agency of Singapore:
Guidelines on Security Al Systems (Draft for Public Consultation, July 2024)



MAS/TCRS/2024/05: Cyber Risks Associated with Generative Artificial Intelligence (Information Paper, July 2024)



The KPMG AI Security framework can help you on your cybersecurity journey

Risk Indicators

Identifying incidents, vulnerabilities, risk considerations for AI systems (complex attack surface, etc.)

AI Ecosystem

Understanding your Al technologies, models in dev or production, third party models, and Al security tooling.

Regulations

Planning or addressing emerging/existing legislation or industry standards.

Public-Private Sector Initiatives

Leveraging knowledge from public/private/research led security initiatives to improve your organization's responsiveness to AI security.



Awareness

Enhance organization's security posture by empowering your workforce to understand emerging risks around AI.

Al Security Framework

Secure organization's Al landscape with a tailored framework providing governance and guidance on how to operationalize a robust Al security program.

Al Security Pipeline Management

Assess organization's current state of AI Security Pipelines, including technical components of an organization's AI pipeline and related vulnerabilities.

Al Security Uplift

Address organization's identified security issues and specifically address the issues and opportunities discovered within an organization's AI ecosystem.



Key Considerations



N1



Understand your Al footprint, including shadow Al





03





 $\mathbf{0}$



05

Understand the emerging AI cybersecurity requirements from laws and regulations

Set Al cybersecurity policy and promote awareness with cyber, data, tech and Al teams

Adopt a lifecycle and secure-by-design approach to Al cybersecurity

Conduct holistic Al program cybersecurity assessment and ongoing Al cybersecurity risk assessments to manage and monitor the risk



Contact us

Eddie Toh Partner

Cyber, Advisory KPMG in Singapore T: +65 6213 3028

E: eddietoh@kpmg.com.sg

Wendy HQ Lim

Partner

Cyber, Advisory KPMG in Singapore

T: +65 6411 8263

E: wlim@kpmg.com.sg

Paul Lothian

Director

Cyber, Advisory KPMG in Singapore

T: +65 9724 0297

E: plothian1@kpmg.com.sg

kpmg.com.sg



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 on such information without appropriate professional advice after a thorough examination of the particular situation.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

© 2024 KPMG Services Pte. Ltd. (Registration No: 200003956G), a Singapore incorporated company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are registered trademarks or trademarks of KPMG International.