

Emerging Tech Risk – AI Security










Why do we need **AI Security** on top of
traditional Cyber Security?

Targeted threats, expanded attack surface
and evolving regulations

Cyber risks with large language models



Security is a common feature across the evolving regulations

Core Governance Principle	 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 AI 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							
United States	National AI Initiative Act	✓	✓	✓	✓	✓	✓
	AI in Government	✓		✓	✓		
	The National AI Research Resource Task Force				✓	✓	
	NIST AI Risk Framework	✓	✓	✓	✓	✓	✓
	FHFA AB 2020-02	✓	✓	✓	✓	✓	✓
	NAIC Principles on AI	✓	✓		✓	✓	✓
	Federal Trade Commission	✓		✓		✓	
EU	EU Artificial Intelligence Act	✓	✓	✓	✓	✓	✓
	EU Digital Services Act	✓			✓	✓	✓
	OECD Principles	✓	✓			✓	✓
Japan	Social Principles of Human Centric AI	✓	✓		✓	✓	
	AIST ML Quality Management Guideline	✓	✓		✓	✓	
LATAM	Brazilian AI Strategy	✓	✓			✓	
	Brazilian AI Bill		✓				
	AI National Policy (Chile)		✓		✓	✓	
	AI National Plan (Argentina)	✓			✓	✓	

Singapore has released it's own guidelines



**Cyber Security Agency of Singapore:
Guidelines on Security AI 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



Key Considerations



01

Understand your AI footprint, including shadow AI



02

Understand the emerging AI cybersecurity requirements from laws and regulations



03

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



04

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



05

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



Contact us

Eddie Toh

Partner

Cyber, Advisory

KPMG in Singapore

T: +65 6213 3028

E: eddietch@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](https://www.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.