



Frontier AI Readiness Assessment

Turn cyber uncertainty
into informed decisions



What it is:

A readiness assessment to strengthen cyber controls against AI-accelerated attacks

CISOs



CROs



Enterprise Executives



Why it matters

Frontier AI accelerates vulnerability discovery, exploit chaining and attack scale, challenging whether existing controls can respond at attacker tempo. An independent assessment identifies where controls, assumptions and assurance no longer hold, helping leadership prioritise remediation, strengthen defensive use of AI and align findings with existing risk, audit and governance frameworks.

Assess whether existing controls remain effective against AI-accelerated threats, enabling informed security investment decisions.

What it does: **Know your current exposure. Set your direction.**

Establish the current state

Identify controls that may no longer be effective.

Understand exposure

Govern AI-accelerated cyber risk with confidence.

Set a clear direction

Prioritise the controls and investments that matter most.

Apply defensive AI

Enhance security operations responsibly.

Benefits

- Prioritised, board-ready improvement roadmap
- Clear domain-level visibility of control gaps
- Alignment with risk registers and audit plans



How it works: Translate readiness gaps into prioritised action

Input

Existing policies, standards, architectures, risk assessments, audit findings, operating procedures and stakeholder interviews across technology, security and risk teams.

Action

Review evidence, conduct workshops and interviews, and assess whether critical control domains remain effective against AI-accelerated attack scenarios.

Output

A clear view of control strengths, gaps, exposure areas and priority improvement opportunities.

Impact

Leadership gains the insights needed to make informed cyber investment decisions, set strategic priorities and strengthen resilience.



Explore your readiness for AI-accelerated cyber threats

Discover where existing controls require recalibration to remain effective against AI-accelerated attacks.

Consider an assessment if your organisation is:

- Revalidating existing cyber controls and accepted risks
- Prioritising remediation, strategy and investment initiatives
- Preparing board, senior management or regulatory assurance

Speak to us to translate readiness insights into a prioritised roadmap.



Sanjai Sivasankar

Associate Director, Cyber,
KPMG in Singapore

sanjaisivasankar@kpmg.com.sg

How KPMG supports you: Frontier AI Readiness Assessment

A targeted review of the established cyber control domains where AI-compressed attacker tempo changes whether a control still holds. Each domain is assessed for adequacy against the new threat landscape, resulting in a prioritised, board-ready roadmap.

What it is

An independent, outside-in assessment of whether existing controls, assumptions and assurance still hold at attacker tempo.

What it delivers

- Domain-level view of where controls no longer hold
- Prioritised, board-ready roadmap
- Board and senior management readout

Findings are expressed in standard control-domain language and mapped to NIST CSF 2.0, allowing direct alignment to existing frameworks, risk registers and audit plans.

8

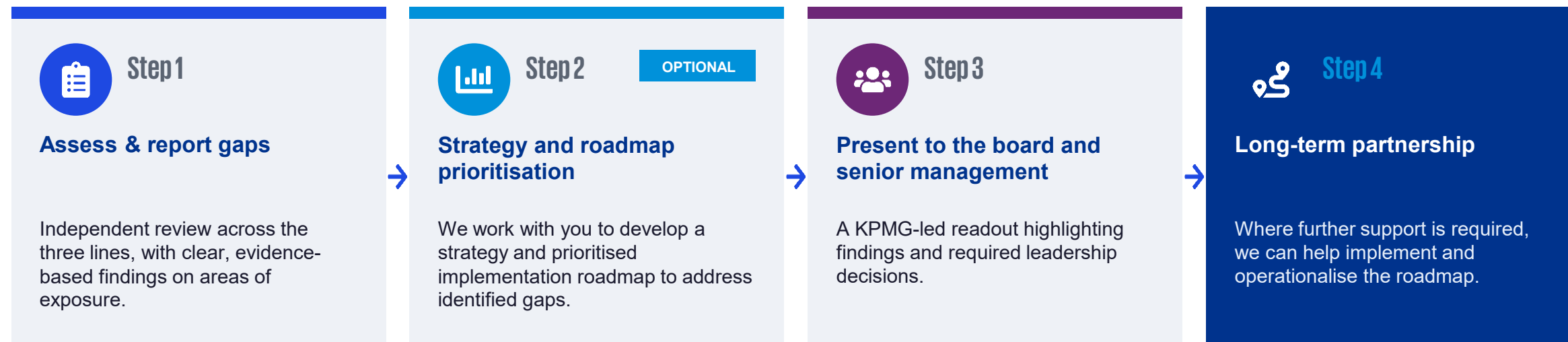
control domains in scope

Targeted scope — not a full-framework cyber review.

CONTROL DOMAIN	A FLAVOUR OF WHAT IS ASSESSED	READINESS QUESTION
 Asset & attack surface management IDENTIFY	<ul style="list-style-type: none">Internet-facing asset and EASM visibilityShadow exposure, APIs and ownership	<i>Is exposure known as it stands today?</i>
 Threat & vulnerability management PROTECT	<ul style="list-style-type: none">Exploitability-led triage (CVSS×EPSS×KEV)Patch-to-deploy velocity and compensating controls	<i>Can patching keep pace with AI-accelerated exploitation?</i>
 Identity & access management PROTECT	<ul style="list-style-type: none">Standing privilege and PAM coverageNon-human and agent identity governance	<i>Is blast radius contained through identity?</i>
 Security architecture & segmentation PROTECT	<ul style="list-style-type: none">Control placement mapped to ATT&CKSegmentation and assume-compromise design	<i>Are controls placed where AI-driven attacks are concentrated today?</i>
 Threat detection & response DETECT / RESPOND	<ul style="list-style-type: none">Detection coverage for multi-stage automated attacksTriage, escalation and response tempo	<i>Can intrusions be detected and contained in time?</i>
 Third-party & supply chain risk GOVERN	<ul style="list-style-type: none">Supplier and dependency blast-radius visibilityAI-provider and open-source exposure	<i>Is inherited exposure understood and managed?</i>
 Cyber resilience & recovery RECOVER	<ul style="list-style-type: none">Immutable backups and tested recoveryScalability of cyber operations under pressure	<i>Can critical services be restored if prevention fails?</i>
 Governance, risk & assurance GOVERN	<ul style="list-style-type: none">Risk appetite and accepted-risk revalidationAssurance scope and board reporting evidence	<i>Can readiness be independently evidenced to the board?</i>
<div><div>AI FOR OFFENCE<p>Frontier AI accelerates vulnerability discovery, exploit chaining and campaign scale against the existing estate.</p></div><div>READINESS ASSESSMENT<p>Each domain is reassessed against attacker tempo, identifying where AI can strengthen defence.</p></div><div>AI FOR DEFENCE<p>Prioritised AI use cases for security operations, such as SOC triage and detection, vulnerability triage and code review, with governed human oversight.</p></div></div>		

A starting point that takes you further

The prioritised report helps organisations define strategy and next steps to strengthen their security posture.



...Leading to a recalibrated, continuous control environment that thwarts AI-speed attacks



The next step: Begin with the readiness diagnostic, a board-level readout, and strategy definition to stay ahead of attacker tempo.



KPMG Services Pte. Ltd.

© 2026 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.

General disclaimer

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 endeavour 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 registered trademarks or trademarks of KPMG International.

Document Classification: KPMG Public