AI Regulation in Comparator Jurisdictions

Developments overseas and lessons for Australia

1 April 2026



GLOBAL SHIELD INSTITUTE



Anthropic raises $30 billion in Series G funding at $380 billion post-money valuation

Anthropic is a Public Benefit Corporation, whose purpose is the responsible development and maintenance of advanced AI for the long-term benefit of humanity. Our Board of Directors is elected by stockholders and our Long-Term Benefit Trust, as explained here.

ANTHROP\C

THE PENTAGON
WASHINGTON D.C.

Trump Can Keep America's AI Advantage

China is trying to catch up. The U.S. needs proactive development efforts and strong export controls.

By Dario Amodei and Matt Pottinger

Jan. 6, 2025 1:09 pm ET

AI Safety Index

	Anthropic
Overall Grade	C+
Overall Score	2.64

GSi
GLOBAL SHIELD INSTITUTE

Executive summary

No jurisdiction is fully addressing key AI risks.

Each country examined has gaps and is looking at reforms.

Two broad categories of AI policy approaches

Jurisdictions are either enacting **AI-specific legislation** (EU, Vietnam, South Korea) or pursuing **issue- and sector-specific reforms** (UK, Singapore).

Lessons for Australia

Australia is falling behind on either approach. Without an AI Act, urgent issue- and sector-specific reforms are needed, along with significant investment. We are at risk of entrenching dependence on foreign suppliers and regulators.

GSi
GLOBAL SHIELD INSTITUTE

Two Categories of Approaches

AI-specific legislation

The European Union

California & New York

Vietnam

Korea

Malaysia (under consideration)

Brazil (under consideration)

Issue/sector-specific approach

The United Kingdom

Singapore

Australia

Canada

Japan

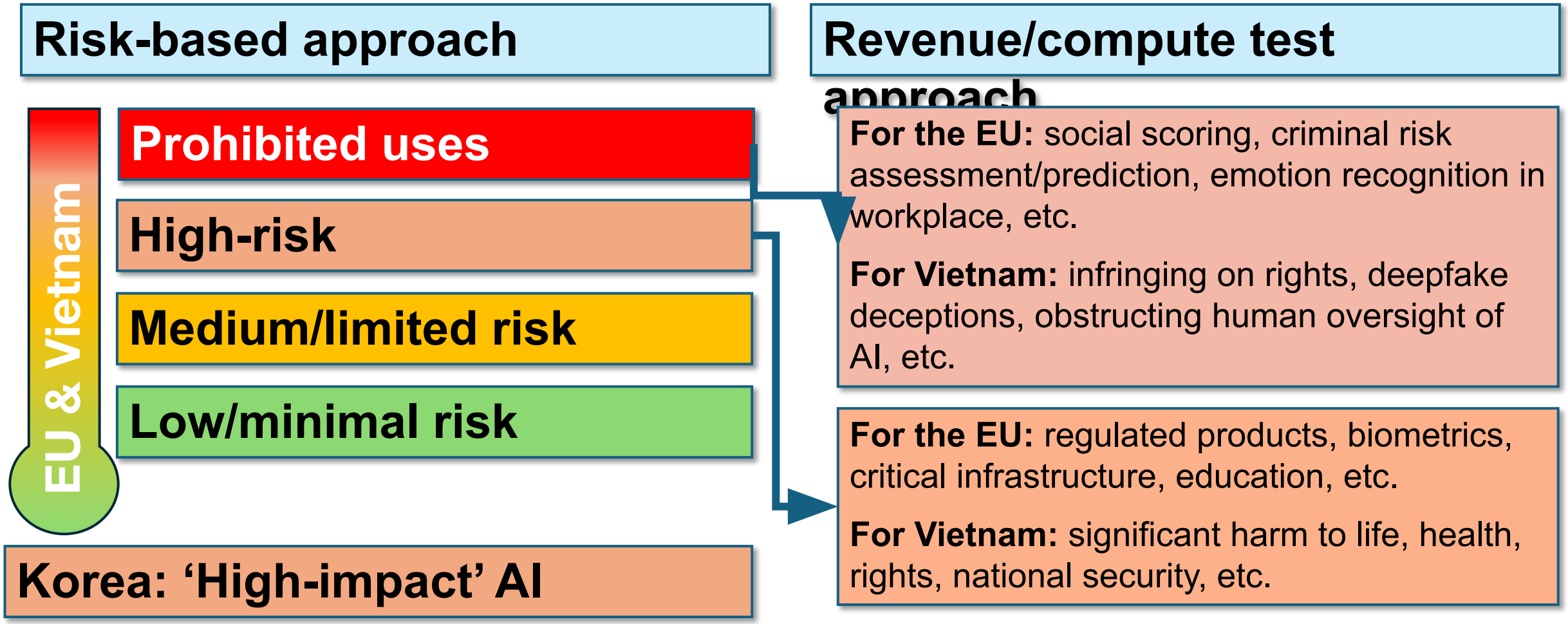
China

AI-specific legislation

Overview of AI-specific legislation

	European Union	California & New York	Vietnam	South Korea
Scope	Risk-based plus compute test	Compute and revenue test	Risk-based	Risk-based plus compute test
Risk management	Yes	Yes	Yes	Yes
Conformity assessment	Yes (high-risk)	No	Yes (high-risk)	No (but incentive for rights impact assessment)
Training data disclosure	Yes (GPAI models)	Yes (CA), No (NY)	No	Yes
AI must be disclosed	Yes	Yes (CA), No (NY)	Yes	Yes
Incident monitoring and reporting	Yes (serious incidents)	Yes (critical safety incidents)	Yes (serious incidents)	No (but must monitor and respond to safety incidents)
Penalties	Up to EUR35m or 7% of worldwide annual revenue	Up to US$1m per breach (US$3m in NY for subsequent breaches)	TBD	Up to AUD29,000

AI-specific legislation: Scope



AI-specific legislation: Scope

Risk-based approach

EU & Vietnam

- **Prohibited uses**
- **High-risk**
- **Medium/limited risk**
- **Low/minimal risk**

Korea: ‘High-impact’ AI

Revenue/compute test approach

Regulation of:

Frontier models	**Large developers**
AI models trained with more than 10^26 FLOPs of compute	Developers with more than USD500m revenue
California, New York, South Korea	**California & New York**

AI-specific legislation: Scope

Risk-based approach: General-Purpose AI (EU)

AI models can be:

Narrow, specific or specialised, such as for:

- **Medical imaging (Harrison.ai)**
- **Legal document analysis (Harvey)**
- **Fraud detection (Feedzai)**
- **Energy grid monitoring**
- **Game playing (Stockfish chess engine)**
- **Scientific research (AlphaFold)**

Harvey.

feedzai

AlphaFold

harrison.ai

General-Purpose AI (GPAI) models. These are broadly capable and able to perform a wide range of tasks in a broad range of use cases. It includes all of the well-known frontier AI models and products.

Grok

Gemini

GSi GLOBAL SHIELD INSTITUTE

AI-specific legislation: Scope

Risk-based approach: General-Purpose AI (EU)

AI models can be:

Narrow, specific or specialised, such as for:

The EU **imposes additional obligations on GPAI models** given their specific risk profile.

It also imposes **further obligations on GPAI models that pose a 'systemic risk'.**

- ~~Energy grid monitoring~~

Systemic risk is the "*risk of significant impact on the EU*" and is presumed to exist where models are trained with more than 10^25 FLOPs of computing power.

Harvey.

feedzai

AlphaFold

harrison.ai

General-Purpose AI (GPAI) models. These are broadly capable and able to perform a wide range of tasks in a broad range of use cases. It includes all of the well-known frontier AI models and products.

Grok

Gemini

AI-specific legislation: Risk management

California / New York
Frontier developers must maintain and follow a **Frontier AI Safety Framework**, setting out how they **identify and mitigate catastrophic risks.**

Vietnam
Obligation to **assess conformity** of high-risk systems before deployment.

High-risk systems must undergo a **risk assessment** and have **human oversight**.

South Korea
High-performance developers must have a **risk management plan** in place.

European Union
Obligation to **assess conformity** of high-risk systems before deployment.

High-risk systems must have **risk management plan** in place.

GPAI models with systemic risk must undertake evaluations to **identify and mitigate systemic risks**.

GSi GLOBAL SHIELD INSTITUTE

AI-specific legislation: Transparency & D

1

Disclosure of when interacting with an AI system

Users must be told if they are interacting with an AI chatbot or system if it is not clear.

EU, Vietnam, South Korea

2

Labelling of AI content

AI output must contain machine-readable markings or watermarks or be detectable as AI generated.

EU, Vietnam, South Korea

3

Training data disclosure

Developers publish high-level summaries or overviews of training data used to train their models.

EU, California, South Korea

Anthropic CEO: "…the right place to start is with transparency legislation... if truly strong evidence of risks emerges, then rules should be proportionately strong."

GSi GLOBAL SHIELD INSTITUTE

AI-specific legislation: Monitoring and

	Trigger	Timeframe	Scope
EU	**Serious incidents**: death, serious harm, rights infringement, critical infrastructure disruption	15 days; 2 days if widespread issue	High-risk AI and GPAI models
California	**Critical safety incidents**: unauthorised access causing death/injury, catastrophic harm, loss of control causing death/injury	15 days; 24 hrs if imminent	Frontier models
New York	**Critical safety incidents**: unauthorised access causing death/injury, catastrophic harm, loss of control causing death/injury	72 hours; 24 hrs if imminent	Frontier models
Vietnam	**Serious incidents** causing significant damage to life, rights, cybersecurity	Unspecified	All AI systems
Korea	**Safety incidents** (undefined)	Unspecified	High performance AI

GSi GLOBAL SHIELD INSTITUTE

AI-specific legislation: Compliance?



Signatories include:

- Amazon
- Anthropic
- Cohere
- Google
- IBM
- Microsoft
- Mistral AI
- OpenAI
- xAI (Safety & Security only)

GSi GLOBAL SHIELD INSTITUTE

AI-specific legislation: US Federal Preemption

In 2025, over **1200 AI-related bills** were introduced across all 50 states in the U[illegible].

Thirty-eight states adopted or enacted around **100 AI-related measures**.

Three **failed** attempts by federal government to pre-empt state AI laws in 2025.

State measures cover issues such as deepfakes, elections, transparency, automated decision-making, high-risk AI, government use of AI, health, and education.

On 20 March 2026, the Administration released a **National Policy Framework for AI** calling on Congress to legislate on AI issues including to "***preempt state AI laws that impose undue burdens".***



GSi GLOBAL SHIELD INSTITUTE

Issue/sector-specific approaches

The United Kingdom

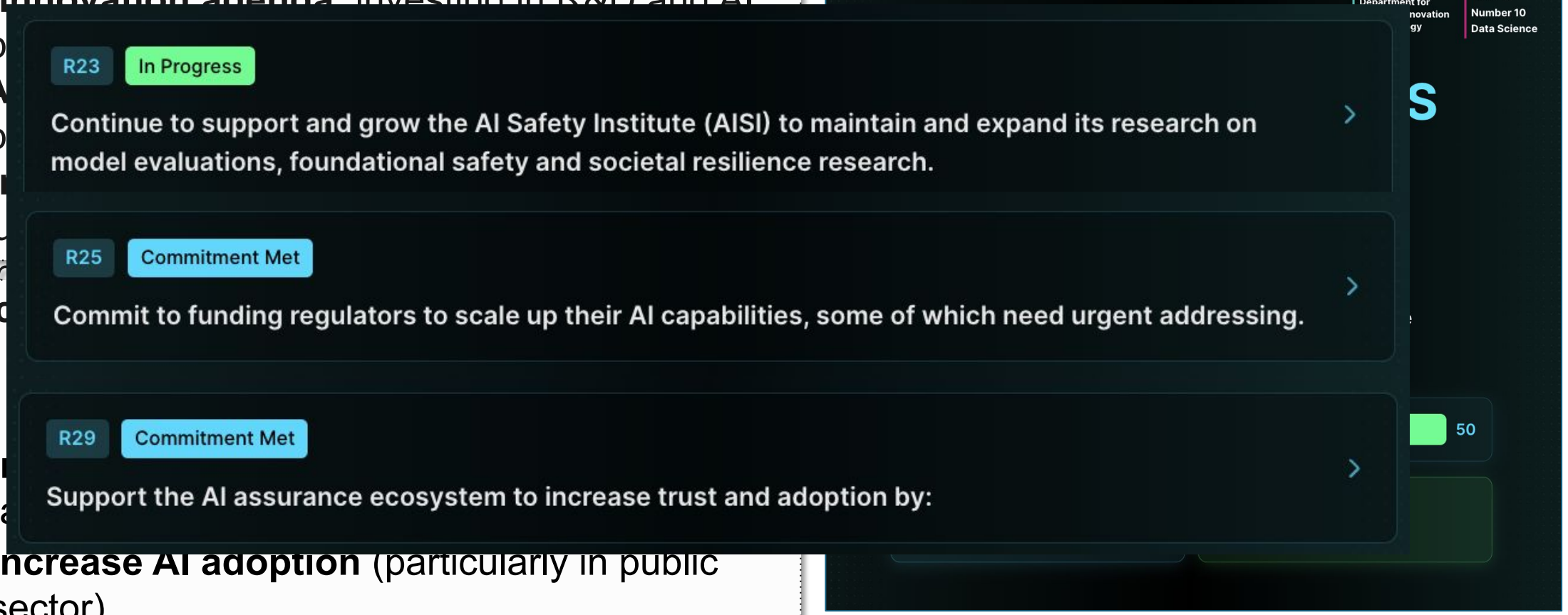
The context and approach

- **Pro-innovation agenda**, investing in R&D and AI enab
- **No A** adap
- **Stro** (inclu comm

Overarc Plan

- Fifty

1. **I** ta
2. **Increase AI adoption** (particularly in public sector)
3. **Aim to be an "AI maker, not an AI taker".**



The United Kingdom

Laws & regulations

- The United Kingdom deals with risks sector-by-sector rather than with horizontal legislation.
- The government has adopted a ‘harms based’ approach – reactive to incidents as they arise.
- Reforms likely in copyright, data protection, deepfakes, AI chatbots, and medical devices.

Representative government investments

£2 billion	Over next four years to develop public compute.
£500 million	In UK companies, AI assets and AI enablers.
£240 million	To establish and run world first AI Security Institute.
£187 million	In digital and AI skills development.
£100 million	For the National Data Library.
£11 million	In an AI Assurance Innovation Fund



Other initiatives

- Hosted first international AI Safety Summit in 2023.
- MoUs with DeepMind, Anthropic, OpenAI, NVIDIA and more.
- MoUs with Canada and the US on compute, safety partnerships, and R&D.

GSi GLOBAL SHIELD INSTITUTE

The United Kingdom

Sector regulation in the UK

Feature	Aviation	Financial Services	Pharma	Food Safety	Foundation models / general-purpose AI
Proactive risk monitoring	Yes	Yes	Somewhat	Somewhat	Voluntary
Safety standards	Yes	Yes	Yes	Yes	Voluntarily and only for some risks
Independent standards	Yes	Yes	Yes	Yes	No
Market entry authorisation	Yes	Yes	Yes	Somewhat	Existing safety-case domains only
Post-market monitoring	Yes	Yes	Yes	Somewhat	Voluntary
Independent regulator	Yes	Yes	Yes	Yes	No regulator for general-purpose AI
Enforcement powers	Yes	Yes	Yes	Yes	No general government or regulator powers
Accountability measures	Yes	Yes	Somewhat	Yes	No
Transparency/reporting requirements	Yes	Yes	Yes	Yes	No
Routes for redress	Yes	Yes	Somewhat	Yes	Not in practice

Commentary

Lack of regulatory capacity limiting AI innovation.

Unclear liability rules means AI risk not managed effectively.

Strong public support for **independent AI regulator**.

More than 100 UK parliamentarians calling for **binding AI regulations**.

Government **cautious on copyright reform**.

GSi GLOBAL SHIELD INSTITUTE

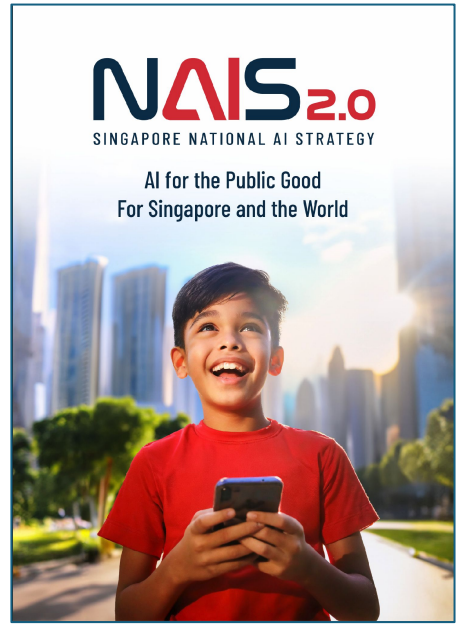
Singapore

The context and approach

- Priority on investment and innovation, **AI risk will be managed through *technical solutions* noting binding government regulations**.
- Focus on producing voluntary frameworks, guidelines, and practical tools for industry.
- Direct state influence in and engagement with corporate sector, including through SOE investments and research bodies.

Overarching strategy: National AI Strategy

- Frames AI as a national necessity, not just economic opportunity.
- **Focus across three 'systems'**
  - **System 1:** Coordinated industry, government and research around meaningful use cases.
  - **System 2:** Attracting and developing capabilities, including talented researchers and engineers to Singapore.
  - **System 3:** Ensure Singapore has the infrastructure and trusted environment for AI innovation

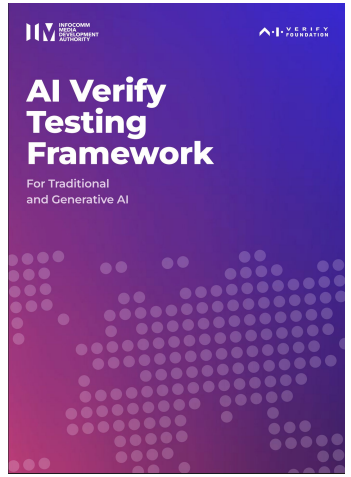


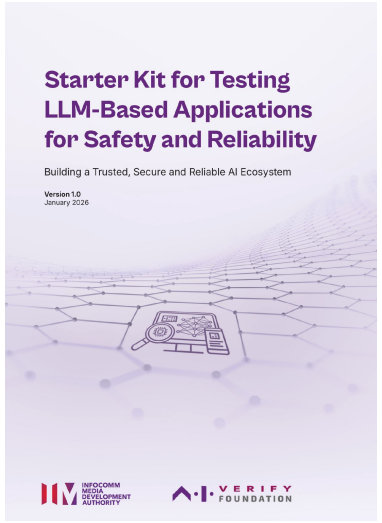
Singapore

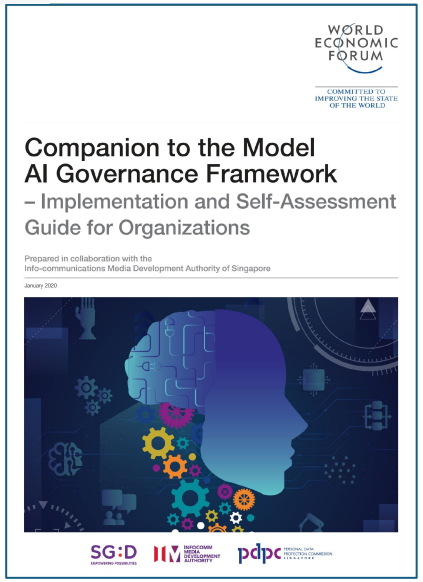
Laws & regulations

- Singapore has no AI-specific legislation. However, it has enacted **targeted legislative measures** addressing specific AI-related risks. This includes on:
  - Election deepfakes
  - AI-generated intimate images
  - Corporate deepfakes
  - Online safety
- **Extensive production of guidelines, frameworks, and tools.**



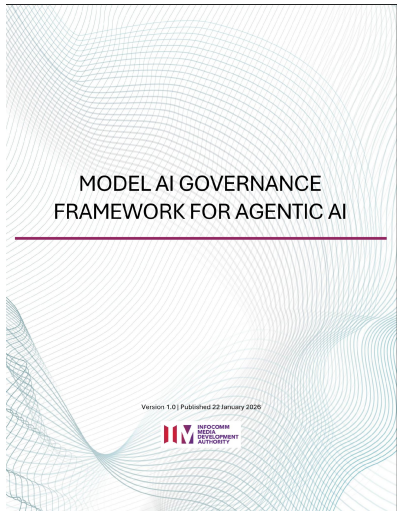


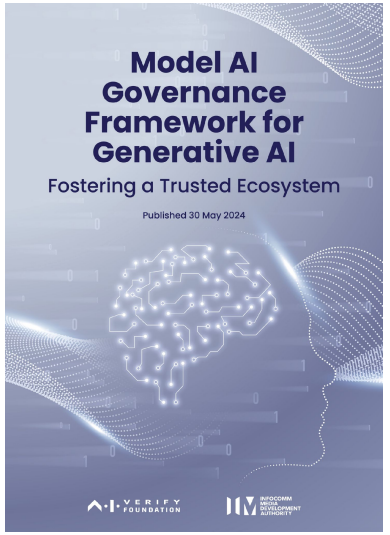












GLOBAL SHIELD INSTITUTE

Singapore

Investments

- **Singapore AISI** (2024), **established with USD37 million.**
- **National AI Research and Development Plan** with **committed S$1 billion investment** between 2025 and 2030 for AI research capabilities. **Follows over S$500 million investment from 2019 to 2023**.
- **S$150 million to an Enterprise Compute Initiative** to enable greater access to AI compute resources.
- **Two open-source AI model families developed under the S$70 million National Multimodal LLM Programme**:
  - **SEA-LION** — developed by AI Singapore. Multilingual LLMs supporting 13+ Southeast Asian languages including regional dialects.
  - **MERaLiON** — led by A*STAR's Institute for Infocomm Research (I²R), supported by IMDA. Multimodal AI model focused on empathetic, culturally attuned interactions for Singapore.

AISI SINGAPORE AI SAFETY INSTITUTE

SEA-LION.AI
Southeast Asian Languages in One Network

MERaLiON

Singapore

Commentary

- Approach depends on (a) **trust from populace**, (b) **close engagement with industry**, (c) **technical solutions being found for risk**, and (d) following and **relying on overseas regulators**.
- Key will be **extent to which voluntary instruments are adopted**.
- Some **indication of future changes coming**, in particular around high-risk AI model transparency and reporting obligations.
- Reactive approach means **incidents and scandals likely to trigger swift and substantial regulatory response**.

Conclusion and lessons for Australia

Conclusion

Australia does not need to start from scratch

There is a trending convergence towards core elements of best practice AI regulation, particularly in relation to risk management and transparency.

Issue/sector specific approaches work best with clear strategy

This includes investment, coherent regulatory settings to encourage investment, targeted reforms, and building regulator capability.

Inaction has a cost

This is an opportunity to lead and shape emerging global norms. However, at present, Australia risks entrenching dependence on foreign AI companies and regulators.

GSi GLOBAL SHIELD INSTITUTE

devon.whittle@globalshieldpolicy.org
max.evans@globalshieldpolicy.org