Published on e-First 24 March 2025

THE NEW FRONTIER: REGULATING ARTIFICIAL INTELLIGENCE IN SINGAPORE

Artificial intelligence ("AI") is advancing rapidly, transforming industries and societies. As a jurisdiction at the forefront of AI development, Singapore stands at the crossroads of this nascent but fast-evolving sector, where the need for a thoughtful, robust regulatory framework is apparent. This article considers the risk-based approach within Singapore's regulatory landscape, exploring in detail the principle of accountability embedded therein. It goes on to posit the future direction of AI regulation and governance in Singapore, highlighting key considerations that must be taken into account in developing and refining any formal regulatory regime.

LIM Fang-Zhou, Noah[1]
LLB (National University of Singapore); Advocate and Solicitor (Singapore); Trainee Associate (Clifford Chance Pte Ltd).

TAN Kay Shin
LLB (National University of Singapore); Advocate and Solicitor (Singapore); Associate (Rajah & Tann Singapore LLP).

I. Introduction

1 Artificial intelligence ("AI") is advancing at an unprecedented pace, transforming industries and societies worldwide.[2] By some metrics, Singapore is a leading country in the adoption and development of AI.[3]

1 The authors are immensely grateful to Senior Research Fellow Juliana Cardinale (Faculty of Law, National University of Singapore) for her invaluable guidance and comments on an earlier version of this article. The authors are also grateful to the anonymous referee for their comments and suggestions. This article is written in the authors' personal capacity. All opinions expressed herein are entirely the authors' own, and all errors and mistakes remain the authors' alone.

2 Aurelio Gurrea-Martinez, "Financial Regulation" in *Law and Technology in Singapore* (Simon Chesterman, Goh Yihan & Andrew Phang Boon Leong eds) (Academy Publishing, 1st Ed, 2021) ch 15, at para 15.011.

3 Alexi Mostrous, Joe White & Serena Cesareo, "The Global Artificial Intelligence Index 2024" *Tortoise Media* (19 September 2024) <https://www.tortoisemedia.com/2024/09/19/the-global-artificial-intelligence-index-2024/> (accessed 1 March 2025). See also Osmond Chia, "Singapore Ranked 3rd Globally in Digital Competitiveness" *The Straits Times* (1 December 2024) <https://www.straitstimes.com/tech/singapore-ranked-3rd-globally-in-digital-competitiveness> (accessed 1 March 2025).

Yet, as these technologies continue to evolve rapidly, the need for robust regulatory frameworks capable of keeping up with such developments becomes increasingly critical. To this end, this article argues that accountability represents the next frontier of AI regulatory development in Singapore, particularly within a risk-based regulatory framework.

2 At the outset, it should be stressed that this article does not seek to provide an overarching framework in relation to *all* types of AI. Given the rapid pace of development, it would certainly be a disservice to the field to attempt spelling out universal principles within the limited remit of this article. Rather, this article merely seeks to lay out some general considerations which might be helpful in conceptualising an appropriate regulatory regime for AI, while contextualising this to the existing state of play within Singapore.

3 Following this introduction, Part II defines key terms for the purposes of this article and provides an overview of Singapore's AI regulatory landscape. Part III goes on to consider the concept of risk and discusses the conceptual basis for risk-based regulation, drawing from an extensive body of literature relating to regulatory theory. Thereafter, Part IV hones in on the principle of accountability, exploring its theoretical basis, the extent to which this principle appears to be embedded within Singapore's existing regulatory regime and the practical implications of this.

4 Building upon this, Part V gazes into the crystal ball, sketching out the possible future of AI regulation in Singapore and highlighting key considerations that must be taken into account in conceptualising any formal regulatory framework. It argues that the future of AI development in Singapore would be best served by adopting a three-pronged approach, namely: (a) striking the right balance between competing policy considerations within this regulatory structure; (b) identifying and implementing the correct structure to serve the intended regulatory purpose; and (c) acknowledging and recognising a plurality of perspectives. Finally, Part VI offers a few parting reflections and concludes.

II. Defining key terms and an overview of the regulatory landscape

A. AI

5 It has been noted that there is presently no universal consensus on the scope of the term "AI",[4] and that defining such a term poses both conceptual and regulatory challenges.[5] For the purposes of consistency, and given the limited remit of this article, the definition of AI as proffered in Singapore's National Artificial Intelligence Strategy Paper is adopted. Thus, AI for the purposes of this article refers to:[6]

> … a set of capabilities through which computer systems can demonstrate humanlike behaviour and complete tasks which typically require human intelligence. It is considered a general-purpose technology which can be applied across a wide range of sectors. Some of its varied applications include advanced web search, recommendation and decision systems, advanced problem-solving, understanding speech and natural language, perception (for applications like facial recognition, image labelling, or autonomous vehicles), and Generative AI tools (including Large Language Models) that can produce various types of content, including text, images, audio, and synthetic data.

B. Regulation

6 Likewise, there is no single definition of regulation. As Moses observes, regulation can mean simply the promulgation of a binding set of rules, it can refer to any deliberate state influence, or it can include all forms of social or economic influence.[7] However, regulation can be clearly differentiated from "law" given that the former has a narrower application, and "operate[s] by defining a set of obligations and responsibilities expected from organisations or individuals that occupy

4 Daniel Seng, Jerrold Soh Tsin Howe & Lim How Khang, "An Introduction to the Relevant Technologies" in *Law and Technology in Singapore* (Simon Chesterman, Goh Yihan & Andrew Phang Boon Leong eds) (Academy Publishing, 1st Ed, 2021) ch 2, at para 02.016.

5 John Zerilli & Adrian Weller, "The Technology" in *The Law of Artificial Intelligence* (Matt Hervey & Matthew Lavy KC eds) (Sweet & Maxwell, 2nd Ed, 2024) ch 2, at para 2-010.

6 Smart Nation Singapore, "NAIS 2.0: Singapore National AI Strategy" (2023) at p 5 <https://file.go.gov.sg/nais2023.pdf> (accessed 1 March 2025). See also Navneet Kaur, "Unravelling the Legal Nexus: Artificial Intelligence and the Path to Responsible Innovation" (2023) 6 Intl J L Mgmt & Human 1106 at 1107–1108 for an overview of possible definitions for artificial intelligence.

7 Lyria Bennett Moses, "How to Think About Law, Regulation and Technology: Problems with Technology as a Regulatory Target" (2013) 5 Law Innovation & Tech 1 at 4.

such roles".[8] Indeed, as compared to "law", regulations are able to capture soft law that may be ignored by traditional definitions of law, as well as more distributed means of control.[9]

7 For the purposes of this article, Black's definition of regulation – as "the sustained and focused attempt to alter the behaviour of others according to standards or goals with the intention of producing a broadly identified outcome or outcomes, which may involve mechanisms of standard-setting, information-gathering and behaviour modification"[10] – is gratefully adopted.

C. AI regulation in Singapore

8 Jurisdictions across the world have taken different approaches to the regulation of AI.[11] In Singapore, there is no specific AI regulator or omnibus AI legislation, and oversight of AI deployment across various industries hinges primarily on the various sectoral laws and guidelines.[12] In this context, the Infocomm Media Development Authority ("IMDA") and Personal Data Protection Commission ("PDPC") are key regulatory bodies playing significant roles in AI governance. Together, these bodies are responsible for the key pieces of AI-related governance measures effected in Singapore – the PDPC released its first edition of the Model AI Governance Framework in 2019, before publishing the second edition of the Model Framework in 2020, while the IMDA published its Model AI Governance Framework for Generative AI in 2024[13] (collectively, the "Model Frameworks").

---

8 Yeong Zee Kin, "Regulation of Technology" in *Law and Technology in Singapore* (Simon Chesterman, Goh Yihan & Andrew Phang Boon Leong eds) (Academy Publishing, 1st Ed, 2021) ch 4, at para 04.007.

9 Lyria Bennett Moses, "How to Think About Law, Regulation and Technology: Problems with Technology as a Regulatory Target" (2013) 5 Law Innovation & Tech 1 at 4.

10 Lyria Bennett Moses, "How to Think About Law, Regulation and Technology: Problems with Technology as a Regulatory Target" (2013) 5 Law Innovation & Tech 1 at 4; Julia Black, "Critical Reflections on Regulation" (2002) 27 *Australian Journal of Legal Philosophy* 1.

11 Claire Bennett, "Artificial Intelligence and Autonomous Vehicles" in *The Law of Artificial Intelligence* (Matt Hervey & Matthew Lavy KC eds) (Sweet & Maxwell, 2nd Ed, 2024) ch 17, at para 17-023.

12 See, *eg*, Monetary Authority of Singapore, "Principles to Promote Fairness, Ethics, Accountability and Transparency (FEAT) in the Use of Artificial Intelligence and Data Analytics in Singapore's Financial Sector" (12 November 2018) <https://www.mas.gov.sg/publications/monographs-or-information-paper/2018/feat> (accessed 1 March 2025).

13 Infocomm Media Development Authority & AI Verify Foundation, "Model AI Governance Framework for Generative AI: Fostering a Trusted Ecosystem" (30 May 2024) <https://aiverifyfoundation.sg/wp-content/uploads/2024/05/

(cont'd on the next page)

9 Industry regulators in Singapore have also contributed by offering sector-specific guidance on AI governance measures. For example, in 2018, the Monetary Authority of Singapore ("MAS") released a set of principles known as the FEAT Principles to promote fairness, ethics, accountability and transparency in the use of AI within the financial sector.[14] The MAS has been very active in relation to AI. Most recently, on 5 December 2024, it released an information paper on AI Model Risk Management,[15] outlining the best practices for AI governance, oversight and risk management in relation to the development and deployment of AI systems. It is key to note, however, that all the existing regulatory guidance in relation to AI are not legally binding and are voluntary in nature – they merely spell out best practices to enable organisations deploying AI solutions to do so in a responsible manner, and do not prescribe any legally binding obligations on the part of organisations.

10 In tandem with its push to accelerate AI innovation, Singapore launched its second National AI Strategy (the "NAIS 2.0") in December 2023.[16] The NAIS 2.0 "outlines 15 Actions that Singapore will undertake … to support [its] ambitions in AI over the next three to five years",[17] including initiatives to strengthen Singapore's AI startup ecosystem and upskill the workforce through sector-specific AI training programmes,[18] which reflect Singapore's stated ambition to be a pace-setter in the development of AI.[19] This is in no small part fuelled by Singapore's desire to promote investment in AI to drive economic growth and security.[20]

Model-AI-Governance-Framework-for-Generative-AI-May-2024-1-1.pdf> (accessed 1 March 2025).

14 Monetary Authority of Singapore, "Principles to Promote Fairness, Ethics, Accountability and Transparency (FEAT) in the Use of Artificial Intelligence and Data Analytics in Singapore's Financial Sector" (12 November 2018) <https://www.mas.gov.sg/publications/monographs-or-information-paper/2018/feat>(accessed 1 March 2025).

15 Monetary Authority of Singapore, "Artificial Intelligence (AI) Model Risk Management" (5 December 2024) <https://www.mas.gov.sg/publications/monographs-or-information-paper/2024/artificial-intelligence-model-risk-management> (accessed 1 March 2025).

16 Smart Nation Singapore, "NAIS 2.0: Singapore National AI Strategy" (2023) <https://file.go.gov.sg/nais2023.pdf> (accessed 1 March 2025).

17 Smart Nation Singapore, "National Artificial Intelligence Strategy 2 to Uplift Singapore's Social and Economic Potential" *Smartnation.gov* <https://www.smartnation.gov.sg/media-hub/press-releases/04122023/> (accessed 1 March 2025).

18 Smart Nation Singapore, "NAIS 2.0: Singapore National AI Strategy" (2023) at pp 23 and 40 <https://file.go.gov.sg/nais2023.pdf> (accessed 1 March 2025).

19 Smart Nation Singapore, "NAIS 2.0: Singapore National AI Strategy" (2023) at p 9 <https://file.go.gov.sg/nais2023.pdf> (accessed 1 March 2025).

20 Matt Hervey & Matthew Lavy KC, "Introduction" in *The Law of Artificial Intelligence* (Matt Hervey & Matthew Lavy KC eds) (Sweet & Maxwell, 2nd Ed, 2024) ch 1, at para 1-003.

III. Risk and regulation of risk

11 Even as Singapore seeks to embrace AI, this technology does not come without its own challenges. Risk is inherent in AI – as machines designed to produce effective solutions which may defy human understanding, AI may fail in unpredictable ways[21] which may not be capable of human rationalisation. This is even before taking into account the existence of malicious actors seeking to utilise and exploit AI for nefarious purposes. Indeed, it was noted in the NAIS 2.0 that a renewed focus on refining Singapore's national strategy for AI was necessitated by "growing concerns over the safety and security risks of AI".[22]

12 However, what is clear is that Singapore has adopted a more pragmatic approach, recognising that such risk and danger might exist, but that on balance, the benefits presented by AI outweigh the possible downsides of this technology. As acknowledged by President Tharman Shanmugaratnam:[23]

> … regulating AI must be the art of the possible, the attainable, the art of the next best. We must go for the next best, which is to get the most good out of AI and avoid the worst … We must also seek to minimise the risks and deal with unwanted outcomes. But *we must know that we cannot avoid the risks altogether* … So *that has to be our frame of mind. Try to get the most good and avoid the worst outcomes, but accept that there's going to be a certain amount of bad in the system*. It's intrinsic to AI innovation. Seek to minimise harm but help people deal with the unwanted outcomes. [emphasis in original omitted; emphasis added in italics]

A. Defining risk

13 Risk is the chance (understood as a probabilistic notion) that a danger (*ie*, an event with harmful consequences) will happen.[24] It is intended to be an objective, measurable entity that combines the

21 Matt Hervey & Matthew Lavy KC, "Introduction" in *The Law of Artificial Intelligence* (Matt Hervey & Matthew Lavy KC eds) (Sweet & Maxwell, 2nd Ed, 2024) ch 1, at para 1-004.

22 Smart Nation Singapore, "NAIS 2.0: Singapore National AI Strategy" (2023) at p 9 <https://file.go.gov.sg/nais2023.pdf> (accessed 1 March 2025).

23 Tharman Shanmugaratnam, President of the Republic of Singapore, "Regulating AI: The Art of the Possible, the Attainable, the Next Best", speech at The Asia Tech X Summit Opening Gala (29 May 2024) <https://www.istana.gov.sg/Newsroom/Speeches/2024/05/29/Speech-By-President-Tharman-Shanmugaratnam-At-The-Asia-Tech-X-Summit-Opening-Gala> (accessed 1 March 2025).

24 Raphael Gellert, "Data Protection: A Risk Regulation? Between the Risk Management of Everything and the Precautionary Alternative" (2015) 5 Intl Data Priv L 3 at 7.

probability of an adverse event and the magnitude of its consequences,[25] and allows for the transformation of uncertain future dangers into certain future dangers through the use of statistics and probabilities.[26]

14 In this regard, the risk and unpredictability engendered by AI is ultimately the consequence of developments in science and industry.[27] It is due to society's inability to control and account for all the possible effects of AI that the process of decision-making is modified to account for this, by transforming these events (and the probability of their occurrence) into risks as a way of rationally managing the limits of regulation.[28]

B. Risk-based regulation

15 The regulation of risk is a logical consequence of the increasing place risks have played in modern, industrialised societies.[29] As concerns about risk have appeared on the radar of policymakers, this has led to a large number of initiatives from technology companies, governments and intergovernmental bodies across the world.[30] This, in turn, has engendered the promulgation of risk-based regulation, which recognises that the enforcers cannot control all processes and all data, and consequently places the focus on known risky or critical phases or elements rather than following all of the complete administrative processes.[31]

16 As May explains, the shift towards such alternative forms of regulation is undergirded by the understanding that it can be difficult to prescribe regulatory fixes given the complexity of organisations' systems, and that regulatory goals are more likely to be achieved by instituting

25 Jacqueline Peel, *Science and Risk Regulation in International Law* (Cambridge University Press, 2010) at pp 79–80.

26 Raphael Gellert, "Data Protection: A Risk Regulation? Between the Risk Management of Everything and the Precautionary Alternative" (2015) 5 Intl Data Priv L 3 at 13.

27 Marianne Ojo, "Beyond the Financial Crisis: Addressing Risk Challenges in a Changing Financial Environment" (2010) 2 Goettingen J Intl L 335 at 344.

28 Marianne Ojo, "Beyond the Financial Crisis: Addressing Risk Challenges in a Changing Financial Environment" (2010) 2 Goettingen J Intl L 335 at 342.

29 Raphael Gellert, "Data Protection: A Risk Regulation? Between the Risk Management of Everything and the Precautionary Alternative" (2015) 5 Intl Data Priv L 3 at 12.

30 Matt Hervey & Matthew Lavy KC, "Introduction" in *The Law of Artificial Intelligence* (Matt Hervey & Matthew Lavy KC eds) (Sweet & Maxwell, 2nd Ed, 2024) ch 1, at para 1-005.

31 Brigitte Unger & Frans van Waarden, "How to Dodge Drowning in Data: Rule- and Risk-based Anti-money Laundering Policies Compared" (2009) 5 Rev L & Econ 953 at 959.

the appropriate systems for monitoring organisations' processes.[32] Ultimately, risk-based regulation is an embodiment of the idea that regulatory failures are possible,[33] and represents controlled governmental interference with market or social processes so as to control potential adverse consequences.[34] It operates as a means of organising resource allocation, managing limited resources and concentrating those resources where they are needed most[35] – such an approach is "strategic and goal-oriented" at the same time, and seeks to ensure the optimum allocation of resources according to the impact and probability of (societal) risks as well as accounting and legitimising such use.[36] In this vein, just as regulation may be regarded as a response to risk,[37] the control of risks can be considered to be the main concern of regulation.[38]

17 Such a form of regulation has much to commend it. As Black and Baldwin argue, in its idealised form, risk-based regulation offers "an evidence-based means of targeting the use of resources and of prioritising attention to the highest risks in accordance with a transparent, systematic, and defensible framework".[39] Similarly, risk-based management offers the prospect of less obedience merely for the sake of obedience, less formalism, less administrative burdens both for the subjects of regulation and its enforcers, and less bureaucracy.[40]

---

32 Peter J May, "Regulatory Regimes and Accountability" (2007) 1 Regul & Gov 8 at 10.

33 Michael Power, *The Risk Management of Everything: Rethinking the Politics of Uncertainty* (Demos, 2004) at p 22. See also the Personal Data Protection Commission, "Model Artificial Intelligence Governance Framework: Second Edition" (21 January 2020) at p 54 <https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/resource-for-organisation/ai/sgmodelaigovframework2.pdf> (accessed 1 March 2025): "AI will continue to evolve, and no party has full sight of the risks that might emerge."

34 Christopher Hood, Henry Rothstein & Robert Baldwin, *The Government of Risk: Understanding Risk Regulation Regimes* (Oxford University Press, 2001) at p 3.

35 Marianne Ojo, "Beyond the Financial Crisis: Addressing Risk Challenges in a Changing Financial Environment" (2010) 2 Goettingen J Intl L 335 at 352.

36 Raphael Gellert, "Data Protection: A Risk Regulation? Between the Risk Management of Everything and the Precautionary Alternative" (2015) 5 Intl Data Priv L 3 at 13–14.

37 Marianne Ojo, "Beyond the Financial Crisis: Addressing Risk Challenges in a Changing Financial Environment" (2010) 2 Goettingen J Intl L 335 at 353.

38 Robert Baldwin, Martin Cave & Martin Lodge, *Understanding Regulation: Theory, Strategy and Practice* (Oxford University Press, 1999) at p 138.

39 Julia Black & Robert Baldwin, "Really Responsive Risk-Based Regulation" (2010) 32 *Law & Policy* 181 at 181.

40 Brigitte Unger & Frans van Waarden, "How to Dodge Drowning in Data: Rule- and Risk-based Anti-money Laundering Policies Compared" (2009) 5 Rev L & Econ 953 at 957.

IV. Shift toward accountability

A. Principle of accountability

18 The principle of accountability "ensures that AI actors are responsible and accountable for the proper functioning of AI systems and for the respect of AI ethics and principles, based on their roles, the context, and consistency with the state of art".[41] It is thus closely tied to the concept of responsibility, and is ultimately a multifaceted concept that requires collaboration between various stakeholders.[42] As May observes, there are at least three levels of accountability:[43]

> (a) the first level is that those who promulgate regulations must be accountable with respect to the content of the provisions ("First Level Accountability");
>
> (b) the second level is that those charged with the implementation of or compliance with regulatory regimes must be held accountable – this entails accountability by both the regulator as well as the regulated entities ("Second Level Accountability"); and
>
> (c) the third level of accountability is the responsiveness of elected officials to shortfalls in regulatory regimes – this encompasses the ability and willingness of elected officials to learn about shortfalls in the regulatory regime and to make necessary adjustments ("Third Level Accountability").

B. Accountability in Singapore's regulatory landscape

19 Ensuring accountability within Singapore's AI regime serves three distinct purposes: (a) it promotes the responsible development of AI systems in Singapore; (b) it provides assurance to users of such systems that their interests have been taken into account in the development and use of AI systems – thus facilitating the use of such systems, and in turn further development spurred by data gleaned from such use; and (c) more broadly, it fosters trust in Singapore's AI landscape.

---

41 Personal Data Protection Commission, "Model Artificial Intelligence Governance Framework: Second Edition" (21 January 2020) at Annex A <https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/resource-fororganisation/ai/sgmodelaigovframework2.pdf> (accessed 1 March 2025).

42 Navneet Kaur, "Unravelling the Legal Nexus: Artificial Intelligence and the Path to Responsible Innovation" (2023) 6 Intl J L Mgmt & Human 1106 at 1110.

43 Peter J May, "Regulatory Regimes and Accountability" (2007) 1 Regul & Gov 8 at 11–12.

20 The importance of embedding accountability within the local AI regime is made clear in the NAIS 2.0, where the existence of a "Trusted Environment" is identified as a key enabler of Singapore's AI aspirations, and where it is stated that "[t]he ultimate aim [of the Government] is to establish a trusted environment for AI, where people can have the confidence that their interests are protected when interacting with AI".[44] In this regard, it is clear that accountability forms a cornerstone of Singapore's AI Governance Framework – indeed, the terms "trust" and "accountability", which go hand-in-hand, appear more than 40 times throughout the Framework.

21 In the Singaporean context, the First and Third Levels of accountability, as laid out by May, place the onus on the regulator or the State, which is expected to shoulder responsibility for the content of the relevant regulatory guidance, as well as demonstrate responsiveness in curing deficiencies in the regulatory regime as and when they arise. This much appears to be recognised in the NAIS 2.0, where the Singapore Government expressly spells out its role in institutionalising "appropriate governance and security frameworks for AI systems".[45] The NAIS 2.0 further recognises that the Government needs "a deeper understanding of how AI works, what benchmarks to use, and what testing is appropriate";[46] where existing regulatory frameworks need to be updated, this will be done "thoughtfully and in concert with others, accounting for the global nature of AI".[47]

22 By elimination, the outstanding issue is in respect of Second Level Accountability – how are those charged with the implementation of regulatory regimes held accountable? Here, it is seen that the emphasis on accountability-based principles shifts the primary responsibility for ensuring compliance from the regulator to the regulated organisation, requiring the latter to take responsibility. Indeed, to the extent that accountability for compliance with existing regulatory guidance is concerned, it is suggested that greater emphasis has been placed on the role played by organisations in Singapore.

---

44 Personal Data Protection Commission, "Model Artificial Intelligence Governance Framework: Second Edition" (21 January 2020) at p 54 <https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/resource-for-organisation/ai/sgmodelaigovframework2.pdf> (accessed 1 March 2025).

45 Smart Nation Singapore, "NAIS 2.0: Singapore National AI Strategy" (2023) at p 54 <https://file.go.gov.sg/nais2023.pdf> (accessed 1 March 2025).

46 Smart Nation Singapore, "NAIS 2.0: Singapore National AI Strategy" (2023) at p 55 <https://file.go.gov.sg/nais2023.pdf> (accessed 1 March 2025).

47 Smart Nation Singapore, "NAIS 2.0: Singapore National AI Strategy" (2023) at p 54 <https://file.go.gov.sg/nais2023.pdf> (accessed 1 March 2025).

23 The AI Verify Foundation was launched by the IMDA in June 2023[48] as a not-for-profit entity that "aims to harness the collective power and contributions of the global open-source community to develop AI testing tools to enable responsible AI … [and promote] best practices and standards for AI".[49] While it is a wholly-owned subsidiary of the IMDA, its premier members at launch included various industry leaders such as Google, IBM and Microsoft, and its membership as of December 2024 includes more than 160 organisations across various industries and sectors.[50]

24 The co-opting of industry voices into the AI Verify Foundation, which arguably serves a quasi-regulatory role in setting standards regarding the use and deployment of AI, is emblematic of Singapore's consultative approach toward regulating AI, at least within this current phase of AI development. This is further highlighted by the fact that the Model Frameworks relied extensively on feedback from various individuals and organisations.[51]

25 Understandably, valid concerns may arise regarding the risk of regulatory capture. This would ostensibly occur where, by virtue of the collaboration with industry voices, any form of regulatory guidance which is released ultimately represents a "direct or indirect [deviation] from the regulatory aim of maximising public welfare"[52] in so far as it provides industry stakeholders with an opportunity to lobby or exert influence on regulators through relational means. This phenomenon has the potential to hinder effective AI regulation and compromise the protection of public interests, as industry goals may not always align with broader societal needs. While such concerns are certainly valid, this

48 Personal Data Protection Commission, "Launch of AI Verify Foundation to Shape the Future of AI Standards Through Collaboration" *PDPC.gov* (7 June 2023) <https://www.pdpc.gov.sg/news-and-events/announcements/2023/06/launch-of-ai-verify-foundation-to-shape-the-future-of-ai-standards-through-collaboration> (accessed 1 March 2025).

49 "AI Verify Foundation" *AI Verify Foundation* <https://aiverifyfoundation.sg/ai-verify-foundation/> (accessed 1 March 2025).

50 "Foundation members" *AI Verify Foundation* <https://aiverifyfoundation.sg/foundation-members/> (accessed 1 March 2025).

51 Personal Data Protection Commission, "Model Artificial Intelligence Governance Framework: Second Edition" (21 January 2020) at p 68 <https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/resource-for-organisation/ai/sgmodelaigovframework2.pdf> (accessed 1 March 2025); Infocomm Media Development Authority & AI Verify Foundation, "Model AI Governance Framework for Generative AI: Fostering a Trusted Ecosystem" (30 May 2024) at p 32 <https://aiverifyfoundation.sg/wp-content/uploads/2024/05/Model-AI-Governance-Framework-for-Generative-AI-May-2024-1-1.pdf> (accessed 1 March 2025).

52 Zeyi Ren, "Regulatory Capture in China's IPO Regulation and Proposed Solutions" (2021) 9 Peking U LJ 187 at 189.

article suggests that such concerns may be mitigated by adopting the best practices spelt out in Part V below.

26 To be sure, there are clear benefits to such a consultative approach, namely that any resulting guidance will be better tailored to suit the needs of organisations. However, it is further suggested that this approach encourages accountability, given that organisations are more likely to follow regulatory guidance where it suits their own interests. The Model Frameworks would thus encourage accountability in so far as it represents a set of standards which have been set by the organisations themselves. Any standards set would also be subject to a minimum standard given the involvement of the PDPC and the IMDA, while remaining realistic and grounded by virtue of the participation and input of industry participants. The resulting Model Frameworks developed from this consultative approach, accordingly, represent a set of practices which are more realistic, more achievable and more palatable to organisations, thus incentivising the adoption of these standards notwithstanding their voluntary nature. Moreover, by virtue of the membership within the AI Verify Foundation, the Model Frameworks arguably carry a degree of credibility within the various industries which they might not otherwise enjoy.

27 In this connection, the corpus of AI-related guidance highlights the role of organisational accountability within Singapore's existing regulatory regime. The Model AI Governance Framework stresses that organisations should develop appropriate internal governance structures that allow it to have appropriate oversight over how AI technologies are brought into their operations,[53] and suggests defining clear roles and responsibilities for ethical AI deployment as well as robust internal risk management controls.[54] Moreover, organisations are also encouraged to improve the auditability of their AI systems by keeping a comprehensive record of information across the systems' life cycle,[55] and using this

53 Personal Data Protection Commission, "Model Artificial Intelligence Governance Framework: Second Edition" (21 January 2020) at p 21 <https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/resource-for-organisation/ai/sgmodelaigovframework2.pdf> (accessed 1 March 2025).

54 Personal Data Protection Commission, "Model Artificial Intelligence Governance Framework: Second Edition" (21 January 2020) at pp 22–24 <https:// www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/resource-for-organisation/ai/sgmodelaigovframework2.pdf> (accessed 1 March 2025).

55 Personal Data Protection Commission, "Model Artificial Intelligence Governance Framework: Second Edition" (21 January 2020) at p 51 <https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/resource-for-organisation/ai/sgmodelaigovframework2.pdf> (accessed 1 March 2025).

audit trail to promote the traceability of such systems[56] – *ie*, the ability to document an AI system's decisions and processes in an easily-understandable manner.

28 Within the domain of Generative AI, the Model AI Governance Framework for Generative AI provides that accountability is key to fostering a trusted AI ecosystem.[57] To this end, the Framework emphasises the need to consider the allocation of responsibility both upfront, during the development process (*ex ante*) and after issues arise (*ex post*).[58] Ultimately, the Framework highlights the need for stakeholders along the AI development chain to be accountable towards end-users, and calls for the alignment of structural incentives to facilitate this.[59]

29 As the broad principles of accountability are mapped out across existing regulatory guidance and materials, various initiatives have kickstarted the process of operationalising the practice of accountability by organisations. In 2022, the IMDA launched the AI Verify initiative, an AI governance testing framework and software toolkit for organisations to validate their AI systems' performance against internationally-recognised principles.[60] The proliferation of such toolkits presents part of a global trend towards AI assurance tools, standards, certification and audit, which are used to help manage expectations between parties,[61] illustrating the importance placed on accountability across various jurisdictions.

---

56 Personal Data Protection Commission, "Model Artificial Intelligence Governance Framework: Second Edition" (21 January 2020) at p 48 <https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/resource-for-organisation/ai/sgmodelaigovframework2.pdf> (accessed 1 March 2025).

57 Infocomm Media Development Authority & AI Verify Foundation, "Model AI Governance Framework for Generative AI: Fostering a Trusted Ecosystem" (30 May 2024) at p 7 <https://aiverifyfoundation.sg/wp-content/uploads/2024/05/Model-AI-Governance-Framework-for-Generative-AI-May-2024-1-1.pdf> (accessed 1 March 2025).

58 Infocomm Media Development Authority & AI Verify Foundation, "Model AI Governance Framework for Generative AI: Fostering a Trusted Ecosystem" (30 May 2024) at pp 7–8 <https://aiverifyfoundation.sg/wp-content/uploads/2024/05/Model-AI-Governance-Framework-for-Generative-AI-May-2024-1-1.pdf> (accessed 1 March 2025).

59 Infocomm Media Development Authority & AI Verify Foundation, "Model AI Governance Framework for Generative AI: Fostering a Trusted Ecosystem" (30 May 2024) at p 7 <https://aiverifyfoundation.sg/wp-content/uploads/2024/05/Model-AI-Governance-Framework-for-Generative-AI-May-2024-1-1.pdf> (accessed 1 March 2025).

60 AI Verify Foundation, "What is AI Verify" <https://aiverifyfoundation.sg/what-is-ai-verify/> (accessed 1 March 2025).

61 David Leslie & Patricia Shaw, "Ethics: Context Really Matters for Responsible Innovation" in *The Law of Artificial Intelligence* (Matt Hervey & Matthew Lavy KC eds) (Sweet & Maxwell, 2nd Ed, 2024) ch 3, at para 3-001.

30 Separately, the IMDA launched the Generative AI Sandbox in February 2024 to facilitate local small and medium-sized enterprises' access to Generative AI, as part of efforts to strengthen AI development in Singapore[62] – this scheme proved so successful that a second iteration of the initiative was subsequently announced in October 2024.[63] Such schemes help to meaningfully facilitate accountability practices within organisations by embedding such practices at the outset of organisations' adoption of AI tools, entrenching such practices as the default through exposure.

31 In the face of AI's unpredictability and propensity to generate unexpected outcomes from any given set of data, the desire to see greater accountability within Singapore's regulatory framework has also manifested itself in the sustained effort to ensure that an appropriate level of human oversight is incorporated across the life cycle of AI systems. To this end, the Model Frameworks introduce a "Probability-Severity of Harm Matrix" to assist organisations in assessing the extent of human involvement required in AI-augmented decision-making.[64] This matrix entails computing the probability and severity of harm to an individual (or organisation) as a result of a decision made with the assistance of AI.

32 Where the resulting harm associated with a particular decision is high (whether because there is a high probability of harm, high severity of harm, or both), this would militate in favour of a greater degree of human involvement, which would accordingly scale up to a human-in-the-loop approach, where active and involved human oversight is introduced to AI processes, and where decisions cannot be exercised without affirmative action by a human.[65] Indeed, the PDPC has suggested that where human control is not possible for safety-critical systems, it would be prudent

62 "Singapore's First Generative AI Sandbox to Familiarise and Help SMEs Get Head Start in Capturing New AI Opportunities" *Infocomm Media Development Authority* (7 February 2024) <https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/press-releases/2024/sg-first-genai-sandbox-for-smes> (accessed 1 March 2025).

63 "Building on the Success of Singapore's First Generative AI Sandbox for SMEs, IMDA Launches Generative AI Sandbox for SMEs v2.0 to Help SMEs Adopt GenAI Solutions" *Infocomm Media Development Authority* (29 October 2024) <https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/factsheets/2024/gen-ai-sandbox-2-0> (accessed 1 March 2025).

64 Personal Data Protection Commission, "Model Artificial Intelligence Governance Framework: Second Edition" (21 January 2020) at p 31 <https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/resource-for-organisation/ai/sgmodelaigovframework2.pdf> (accessed 1 March 2025).

65 Personal Data Protection Commission, "Model Artificial Intelligence Governance Framework: Second Edition" (21 January 2020) at p 30 <https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/resource-for-organisation/ai/sgmodelaigovframework2.pdf> (accessed 1 March 2025).

for organisations to ensure that humans are minimally allowed to make meaningful decisions or to safely shut down the AI system.[66] The particular *type* of decision made, in addition to the *implications* of such a decision, thus plays a key role in determining the extent of human oversight necessary for organisations to discharge their accountability obligations in ensuring that AI is responsibly used and deployed. This is because such considerations would determine the relative severity of harm as a result of the decision, as well as the probability of that harm occurring.[67]

33 However, it bears iterating that the particular *type* of AI that is used would also be highly significant in determining the appropriate level of human oversight necessary for an organisation to discharge its accountability obligation. This is because certain types of AI are likely to present greater inherent risk, particularly where it operates autonomously or uses a "black box" system whereby it is impossible to fully verify how a particular decision was arrived at. In any case, it would be fanciful thinking to suggest that humans are capable of assessing and accounting for all risk, even at the relatively undeveloped existing state of AI. It was reported as recently as December 2024 that OpenAI's o1 AI model had "secretly pursued goals of its own even if they opposed a user's wishes".[68] Given that this was only uncovered through targeted and deliberate testing, there are doubtless further issues which remain undiscovered, some of which may not yet be capable of being discovered until knowledge regarding AI further evolves.

34 There are various other factors which may have a bearing of an organisation's assessment of the required level of human oversight, and this much is recognised in the Model Frameworks, which stress that the Probability-Severity of Harm Matrix "should not be taken to imply that the probability of harm and severity of harm are the only factors to be considered in determining the level of human oversight in an organisation's decision-making process involving AI".[69]

---

66 Personal Data Protection Commission, "Model Artificial Intelligence Governance Framework: Second Edition" (21 January 2020) at p 30 <https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/resource-for-organisation/ai/sgmodelaigovframework2.pdf> (accessed 1 March 2025).

67 Personal Data Protection Commission, "Model Artificial Intelligence Governance Framework: Second Edition" (21 January 2020) at p 31 <https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/resource-for-organisation/ai/sgmodelaigovframework2.pdf> (accessed 1 March 2025).

68 Maxwell Zeff, "OpenAI's o1 Model Sure Tries to Deceive Humans a Lot" *TechCrunch.com* (5 December 2024) <https://techcrunch.com/2024/12/05/openais-o1-model-sure-tries-to-deceive-humans-a-lot/> (accessed 1 March 2025).

69 Personal Data Protection Commission, "Model Artificial Intelligence Governance Framework: Second Edition" (21 January 2020) at p 31 <https://www.pdpc.gov.sg/-/

(cont'd on the next page)

35 The provision of such matrices through the Model Frameworks enables organisations to make informed decisions regarding the level of human involvement in AI decision-making, thus empowering them to take greater responsibility and accountability within this process. It supports the efficient deployment of manpower according to the particular needs of the situation, while mitigating risk by encouraging greater human oversight where necessary to ensure that AI outputs align not just with the inputs provided, but also with human and cultural values.[70]

36 In this regard, it bears emphasis that the concept of accountability is not new to the Singapore regulatory regime. Indeed, the concept of accountability is one that has very much been embedded in the heart of Singapore's approach to data protection by virtue of changes in the legislative stance in July 2017, when Singapore announced a pivot away from compliance and toward accountability.[71] It certainly cannot be a coincidence that the Model Frameworks are stated as being "intended to assist organisations to … *[d]emonstrate reasonable efforts to align internal policies, structures and processes with relevant accountability-based practices in data management and protection (e.g. the Personal Data Protection Act 2012)*"[72] [emphasis added].

37 Where it is accepted that the accountability principle under both the data protection domain and the AI domain are the same, or at least functionally equivalent, this has significant implications for how one ought to understand the regulation of AI in Singapore. First, the benefits of the accountability-based approach under Singapore's data protection regime are equally pertinent to the regulation of AI. In this respect, it is observed that the use of systematic assessments, as facilitated under the accountability-based approach, is better suited to risk-based domains,[73] such as the regulation of AI.

---

media/files/pdpc/pdf-files/resource-for-organisation/ai/sgmodelaigovframework2.pdf> (accessed 1 March 2025).

70 Smart Nation Singapore, "NAIS 2.0: Singapore National AI Strategy" (2023) at p 55 <https://file.go.gov.sg/nais2023.pdf> (accessed 1 March 2025).

71 Dr Yaacob Ibrahim, Minister for Communications & Information, "From Compliance to Accountability: A Robust and Progressive Data Protection Framework", speech at the Personal Data Protection Seminar 2017 (27 July 2017) <https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/speeches/2017/personaldata-protection-seminar-2017> (accessed 1 March 2025).

72 Personal Data Protection Commission, "Model Artificial Intelligence Governance Framework: Second Edition" (21 January 2020) at p 13 <https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/resource-for-organisation/ai/sgmodelaigovframework2.pdf> (accessed 1 March 2025).

73 Martin Lodge & Kai Wegrich, *Managing Regulation: Regulatory Analysis, Politics and Policy* (Palgrave Macmillan, 2012) at p 224.

38 Second, the inherent element of subjectivity that exists in the making of risk assessments[74] can be tempered by pegging the standard of such an assessment to the objective standard of reasonableness.[75] Modifying Chesterman's observations in the context of data protection, introducing such a standard of reasonableness would shift the onus onto organisations to justify the use of data in developing their AI systems, as well as the methodology for the systems' use and deployment.[76]

39 In practice, this ultimately means recognising that "accountability" within the context of AI development and deployment does *not* mean that organisations are responsible for mitigating *all* risk. Instead, organisations are merely responsible for mitigating risk where it would be reasonable to expect them to do so; whether an organisation can be said to have satisfied their obligation of accountability is thus a fact-sensitive query that considers what an organisation exercising the appropriate degree of care and judgment in the particular circumstance would do. This standard of reasonableness is a flexible standard that can be calibrated according to various factors including: (a) the relative resources of the organisation; (b) the relative cost of implementing the relevant accountability measures; and (c) the existing state of the art or available knowledge in relation to AI.

40 While it may certainly be argued that in this era of "unknown unknowns", limiting an organisation's obligation of accountability merely to what is "reasonable" might encourage irresponsible experimentation and reckless risk-taking, it is respectfully suggested that such concerns are overstated. The benefit of such a flexible standard lies in its ability to recognise that while it is important for organisations to mitigate the risk posed by AI, this may not always be possible, either because the risks posed by AI are beyond the level of human comprehension that exists at that particular period in time, thereby making it impossible to guard against such risk, or because it is in society's best interests to accept the risk as part and parcel of meaningful AI innovation. In fact, by virtue of the fact-sensitive nature of the "reasonableness" qualifier, the standards imposed on an organisation are ultimately pegged to the specific facts of the situation – if anything, such a standard arguably *reduces* the risk of undesirable behaviour, in so far as it is capable of scaling up the obligation of accountability to hold an organisation responsible not just

74 Robert Baldwin & Julia Black, "Driving Priorities in Risk-based Regulation: What's the Problem?" (2016) 43 J L & Socy 565 at 571.

75 Noah Lim, "Data Protection from a Regulatory Theory Perspective" (2024) 41 Sing L Rev 162 at 181.

76 Simon Chesterman, "Data Protection Law" in *Law and Technology in Singapore* (Simon Chesterman, Goh Yihan & Andrew Phang Boon Leong eds) (Academy Publishing, 1st Ed, 2021) ch 23, at para 23.046.

based on what it *in fact* knew, but also what it ought to have known, in any given scenario.

41 Given the nascent stage of AI development and regulation in Singapore, the concept of reasonableness is presently not a part of Singapore's formal AI regulatory regime – which as of yet does not exist. However, just as the concept of reasonableness underpins the PDPA's approach to data protection[77] – *ie*, a balancing approach that is based on economic considerations[78] – so too should Singapore's AI regulatory regime be underpinned by such an operating logic when a formal framework is ultimately put into place. Indeed, it is entirely consistent with Singapore's aspirations to be a leading AI hub in the world[79] that such a standard of reasonableness be introduced in the form of binding legislation or regulation. After all, neither the State nor any commercial-minded organisation would be willing to be the underwriter of all risks engendered by AI, nor should they be. The imposition of such an onerous obligation would be anathema to innovation, and would amount to mitigating risk by smothering all risk-taking behaviour, including positive risk-taking which is both necessary and beneficial for the meaningful development of technology and society.

42 The *true* role of accountability within any regulatory regime, accordingly, is simply to define organisations' responsibility to identify and sift out risks which are deemed "unacceptable" based on the standard of reasonableness, and to thereafter compel organisations to mitigate this particular category of risk. This much was recognised in the NAIS 2.0, where the Singapore Government acknowledged that it is "only through experimentation and exploration that the AI community can deepen its understanding of AI, and discover and address potential risks".[80]

43 To be clear, while risk-based approaches towards AI are not new, Singapore's risk-based approach to regulation arguably operates with greater fidelity to the concept of risk-based regulation. The EU's AI Act[81] is the first piece of legislation aimed at comprehensively regulating

77 Noah Lim, "Data Protection from a Regulatory Theory Perspective" (2024) 41 Sing L Rev 162 at 171; *Re Black Peony* [2017] PDP Digest 218 at para 8.

78 Noah Lim, "Data Protection from a Regulatory Theory Perspective" (2024) 41 Sing L Rev 162 at 165.

79 Smart Nation Singapore, "NAIS 2.0: Singapore National AI Strategy" (2023) at p 9 <https://file.go.gov.sg/nais2023.pdf> (accessed 1 March 2025).

80 Smart Nation Singapore, "NAIS 2.0: Singapore National AI Strategy" (2023) at p 54 <https://file.go.gov.sg/nais2023.pdf> (accessed 1 March 2025).

81 Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024, laying down harmonised rules on AI and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858,

(cont'd on the next page)

AI, where the choice and design of regulatory instruments is tailored based on the level of risk posed.[82] However, Ebers observes that the AI Act deviates from the traditional tenets of the risk-based approach in various ways, most notably through: (a) the choice to emphasise citizens' fundamental rights alongside health and safety; and (b) the absence of a risk-benefit analysis.[83]

44 In contrast, Singapore's approach does not appear to have any such specific emphasis on citizens' rights, focusing instead on the health and safety implications of AI development and deployment. Further, the use of the Probability-Severity of Harm Matrix within Singapore's various Model Frameworks is functionally equivalent to a risk-benefit analysis, in so far as it compels the individual making the assessment to determine the relative harm *in relation to* the benefits posed by the development or deployment of AI within that particular situation.

45 Given the above, Singapore's approach arguably seeks to strike a delicate balance in protecting the public's interests without imposing overly onerous obligations on organisations. While the principle of accountability, in itself, is not a panacea for all the risks posed by the adoption of AI, it serves a crucial role within Singapore's regulatory framework in embodying an approach that seeks to efficiently allocate resources in a way that best allows organisations to mitigate risk, while also ensuring that the rights of individuals remain untrammelled.

V. The way forward

46 Having established that accountability is a key component of the AI regulatory regime, the next issue is how such a regime can be further refined to encourage innovation in a way that is both responsible and sensitive to the needs of society, and in a manner that evolves with the state of the art. This is undoubtedly a difficult task for any regulator. As Yeong observes:[84]

(EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act).

82 Martin Ebers, "Truly Risk-based Regulation of Artificial Intelligence: How to Implement the EU's AI Act" (2024) at p 3 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4870387> (accessed 1 March 2025).

83 Martin Ebers, "Truly Risk-based Regulation of Artificial Intelligence: How to Implement the EU's AI Act" (2024) at p 11 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4870387> (accessed 1 March 2025).

84 Yeong Zee Kin, *Technology Regulation in the Digital Economy* (Academy Publishing, 2023) ch 2, at para 2.17.

> Regulation is often assumed to be the antithesis of innovation, and often associated with constructing markets and stifling innovation. This reputation is probably due to the phenomenon that regulation had hitherto lagged developments in technology, and were often introduced to correct social and market issues.

47 This article suggests that the future of AI is best served by: (a) striking the right balance between competing policy considerations within this regulatory structure; (b) identifying and implementing the correct structure to serve the intended regulatory purpose; and (c) acknowledging and recognising a plurality of perspectives.

A. Striking the right balance

48 The challenge for Singapore in regulating AI is to avoid under-regulation, which could put citizens at risk and undermine public trust, while also steering clear of over-regulation, which could scare away foreign partners and stifle innovation.[85] As already alluded to above, the challenge in refining Singapore's regulatory approach lies in striking the correct balance across a broad spectrum of considerations.

49 One crucial consideration is that regulators must remain clear-eyed about their priorities in identifying risks to be mitigated – an ideal balance must thus be struck between lower risks and higher risks. This is because while low risk, in the context of risk-based approaches, often means low priority,[86] not all low risks are the same, given that risks are ultimately the product of two dimensions: probability and impact. Different strategies may be appropriate for risks that are known and simple and the impacts of which are remediable or reversible than for those that are uncertain and/or highly contestable, the impacts of which are irremediable or irreversible.[87] Baldwin, Black and O'Leary persuasively argue that regulators cannot simply focus on their most important problems and fix them – they have a legal mandate to fulfil, and must accordingly also consider lower risks, which may well

85 Clay Chandler, "Singapore's AI Ambitions: How the City-State Is Keeping Up in an Arms Race Dominated by the U.S. and China" *Fortune* (30 July 2024) <https://fortune.com/2024/07/29/singapore-artificial-intelligence-travel-shipping-banks-languages/> (accessed 1 March 2025).

86 Robert Baldwin, Julia Black & Gerard O'Leary, "Risk Regulation and Transnationality: Institutional Accountability as a Driver of Innovation" (2014) 3 TEL 373 at 374.

87 Robert Baldwin, Julia Black & Gerard O'Leary, "Risk Regulation and Transnationality: Institutional Accountability as a Driver of Innovation" (2014) 3 TEL 373 at 379.

transform into high risks should the political context shift.[88] Ensuring an appropriate allocation of resources between lower risks and high risks is thus important.

50 Further, as observed by Gellert, governments have a limited capacity to manage risks, yet they must satisfy multiple and sometimes conflicting demands for risk management in addition to the expectations they created for zero-tolerance.[89] Any regulatory regime must therefore strive to identify the appropriate balance between how tight controls should be in seeking consistency, and how much discretion should be granted in promoting flexibility and innovation,[90] taking into account the myriad of policy considerations and stakeholder interests which may often come into conflict with one another. Such a mandate is a difficult but essential one that must surely remain the lodestar for any government or regulator. In this regard, Power warns against the situation where the whole risk management process may be perverted into a self-legitimation exercise that serves no other purpose than that of managing operational and reputational risks, and which, ultimately, is itself a risk to the management of (primary) risks.[91]

B. Identifying the correct structure

51 Equally important to finding the correct balance is finding the appropriate structure for Singapore's AI regulatory regime. Across the world, various jurisdictions have trended towards a high degree of convergence as to basic values to be incorporated into any AI governance framework,[92] such as explainability or transparency, robustness, the avoidance of unwanted bias, safety and human control.[93] Singapore

88 Robert Baldwin, Julia Black & Gerard O'Leary, "Risk Regulation and Transnationality: Institutional Accountability as a Driver of Innovation" (2014) 3 TEL 373 at 389–390.

89 Raphael Gellert, "Data Protection: A Risk Regulation? Between the Risk Management of Everything and the Precautionary Alternative" (2015) 5 Intl Data Priv L 3 at 14.

90 Peter J May, "Regulatory Regimes and Accountability" (2007) 1 Regul & Gov 8 at 23.

91 Raphael Gellert, "Data Protection: A Risk Regulation? Between the Risk Management of Everything and the Precautionary Alternative" (2015) 5 Intl Data Priv L 3 at 15; Michael Power, *The Risk Management of Everything: Rethinking the Politics of Uncertainty* (Demos, 2004) at pp 13–14.

92 Jacob Turner & Leah Gardner, "International Regulation of Artificial Intelligence" in *The Law of Artificial Intelligence* (Matt Hervey & Matthew Lavy KC eds) (Sweet & Maxwell, 2nd Ed, 2024) ch 5, at para 5-001.

93 Jacob Turner & Leah Gardner, "International Regulation of Artificial Intelligence" in *The Law of Artificial Intelligence* (Matt Hervey & Matthew Lavy KC eds) (Sweet & Maxwell, 2nd Ed, 2024) ch 5, at para 5-001.

is no exception. Indeed, the Model Frameworks are drafted in such a way as to be agnostic to algorithms, technology, sector, organisational scale and business models,[94] and are merely intended to address the implementation of "existing and common AI ethical principles".[95] Such an approach necessarily corresponds to the relative nascency of AI and AI regulation, and efforts across the world in this regard appear to have focused on establishing a universal set of principles. This approach entails parsing through jurisdictional- and industry-specific practices to identify core commonalities capable of consistent application across the board.

52 However, Turner and Gardner observe that as the field matures, it is likely that the relevance of some sources of non-binding "soft law" will diminish over time, while soft laws in the form of international technical standards for AI are likely to remain relevant as more AI-specific legislation is enacted.[96] This is consistent with the understanding that while the risk-based approach creates opportunities for the private sector to use its discretion, such an approach also generates significant uncertainty,[97] and *truly* risk-based regulation is likely to disappear over time in the interests of certainty as standards begin to converge. Such a convergence may occur either through mutual agreement among the relevant actors or through the courts,[98] but is ultimately fuelled by organisations' desire for commercial certainty – thus, precision, clarity, transparency and predictability eventually re-emerge over time as risk-based regulation regresses back to *de facto* rule-based regulation. Notably, Unger and van Waarden illustrate this with their observation that legal systems have many broad and vague principles – legality, opportunity, proportionality,

94 Personal Data Protection Commission, "Model Artificial Intelligence Governance Framework: Second Edition" (21 January 2020) at p 10 <https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/resource-for-organisation/ai/sgmodelaigovframework2.pdf> (accessed 1 March 2025).

95 Personal Data Protection Commission, "Model Artificial Intelligence Governance Framework: Second Edition" (21 January 2020) at p 10 <https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/resource-for-organisation/ai/sgmodelaigovframework2.pdf> (accessed 1 March 2025).

96 Jacob Turner & Leah Gardner, "International Regulation of Artificial Intelligence" in *The Law of Artificial Intelligence* (Matt Hervey & Matthew Lavy KC eds) (Sweet & Maxwell, 2nd Ed, 2024) ch 5, at para 5-001.

97 Brigitte Unger & Frans van Waarden, "How to Dodge Drowning in Data: Rule- and Risk-based Anti-money Laundering Policies Compared" (2009) 5 Rev L & Econ 953 at 977.

98 Brigitte Unger & Frans van Waarden, "How to Dodge Drowning in Data: Rule- and Risk-based Anti-money Laundering Policies Compared" (2009) 5 Rev L & Econ 953 at 980.

equality, legal certainty and discrimination – all of which have, over time, acquired precise meanings in legal discourse.[99]

53 As the field of AI advances and develops, with more binding legislation expected to be enacted in the coming years, it is possible that individual regimes will begin to diverge as to the implementation and application of these norms.[100] It is thus crucial that Singapore identifies an appropriate structure for framing its approach to AI regulation, so as to strike out on the right foot. This means finding the right fit between the relevant regulatory circumstances and the design of regulatory regimes, which would go a long way toward reducing confusion over regulatory requirements and the incentives for regulated entities to shirk their responsibilities.[101]

54 To this end, Ayres and Braithwaite propose that regulation be responsive to industry structure[102] – under this model, different structures would thus be conducive to different degrees and forms of regulation. Baldwin, Black and O'Leary also argue that the nature of the regulated organisations must also be taken into account.[103] This is because some low-risk intervention strategies work well with highly motivated regulatees who have a high capacity to comply (*eg*, self-certification systems), but would not prove successful where regulatees are less motivated to comply, or have a low capacity to comply because of limitations in areas such as information about regulatory requirements, resources, systems and personnel.[104] Moreover, the attitude and capacity of the regulatee is particularly critical in determining whether a higher risk can, in fact, be classified as a lower "net" risk and for the intervention strategy that should be used.[105]

---

99 Brigitte Unger & Frans van Waarden, "How to Dodge Drowning in Data: Rule- and Risk-based Anti-money Laundering Policies Compared" (2009) 5 Rev L & Econ 953 at 980.

100 Jacob Turner & Leah Gardner, "International Regulation of Artificial Intelligence" in *The Law of Artificial Intelligence* (Matt Hervey & Matthew Lavy KC eds) (Sweet & Maxwell, 2nd Ed, 2024) ch 5, at para 5-001.

101 Peter J May, "Regulatory Regimes and Accountability" (2007) 1 Regul & Gov 8 at 24.

102 Ian Ayres & John Braithwaite, *Responsive Regulation: Transcending the Deregulation Debate* (Oxford University Press, 1992) at p 4.

103 Robert Baldwin, Julia Black & Gerard O'Leary, "Risk Regulation and Transnationality: Institutional Accountability as a Driver of Innovation" (2014) 3 TEL 373.

104 Robert Baldwin, Julia Black & Gerard O'Leary, "Risk Regulation and Transnationality: Institutional Accountability as a Driver of Innovation" (2014) 3 TEL 373 at 380.

105 Robert Baldwin, Julia Black & Gerard O'Leary, "Risk Regulation and Transnationality: Institutional Accountability as a Driver of Innovation" (2014) 3 TEL 373 at 380.

55 To the extent that the accountability-based approach in Singapore would require self-reporting by organisations, such considerations will certainly need to be taken into account – it should not simply be assumed that more reporting means greater organisational accountability. As Unger and van Waarden observe, excessive reporting can be harmful, and can be spurred either by an overly-conscientious business's desire to play it safe by reporting as much as possible, or by the deliberate intention of a more calculating entity to dilute critical shortcomings through a deluge of information.[106] Moreover, leaving organisations some discretion to decide what to report entails the risk for the government that detection, assessment and reporting is done sloppily or arbitrarily, with the effect that the standards across different businesses may lack homogeneity and standardisation.[107]

56 The design of any future, formal system of AI regulation in Singapore, accordingly, must pay close heed to the nuances of the environment in which this system is intended to operate. Where increased regulatory flexibility is granted, there must necessarily still be sufficient accountability structures put in place,[108] with a minimum baseline standard put in place by legislative action.

C. Recognising and respecting diversity

57 Above and beyond the more practical aspects of regulatory design discussed above, the development of AI could stand to benefit greatly from a regulatory approach that seeks to recognise and respect diversity in AI, which this article now turns to consider.

(1) Value pluralism and social equity

58 As Moses observes, the study of technological regulation is not strictly the study of the regulation of technology, but rather the study of law or regulation *in the context* of a new or changing technology.[109] However, the context in which any regulatory system operates is one that

106 Brigitte Unger & Frans van Waarden, "How to Dodge Drowning in Data: Rule- and Risk-based Anti-money Laundering Policies Compared" (2009) 5 Rev L & Econ 953 at 960–961.

107 Brigitte Unger & Frans van Waarden, "How to Dodge Drowning in Data: Rule- and Risk-based Anti-money Laundering Policies Compared" (2009) 5 Rev L & Econ 953 at 960.

108 Peter J May, "Regulatory Regimes and Accountability" (2007) 1 Regul & Gov 8 at 24.

109 Lyria Bennett Moses, "How to Think About Law, Regulation and Technology: Problems with Technology as a Regulatory Target" (2013) 5 Law Innovation & Tech 1 at 7.

is ultimately shaped by its stakeholders and constituents. As noted by Baldwin, Black and O'Leary, risk-based regulation, in ranking risks on a scale from "low" to "high", assumes that risks are "self-presenting" and that clear-cut distinctions can be made between risk types.[110] This is, however, a flawed assumption – notwithstanding its claim to be an objectively measurable product of impact and probability, risk is ultimately a value-centric exercise.

59 Science and technology studies have long criticised the shortcomings of risk assessment techniques for, among other things: (a) the pretences to objectivity; (b) the hidden methodological choices, values and assumptions inherent to the process; and (c) the limits of scientific knowledge itself.[111] Indeed, how risks are selected, framed and categorised for attention is a complex process, involving a mosaic of technical, psychological, cultural, social, political, organisational and economic concerns.[112] Gellert similarly states that risk management embodies significant values and ideals, not least of accountability and responsibility.[113] But perhaps Fisher puts this best, with her striking statement that:[114]

> Different future threats are regulated in different ways due to a mixture of legal culture, socio-political catalysts, and sheer historical accident. Risk regulation is thus an impenetrable tangle of legislation, secondary legislation, policies, institutional structures, and processes.

60 The need to incorporate various lenses and for regulation to track the evolution of society is alluded to by Moses, who observes that "technology" may not just refer to changes of tools or process over time, but may include new forms of conduct becoming part of social practice.[115] Properly framed, Singapore's risk-based approach to AI regulation might be optimal for innovation and economic development. Nevertheless, this

---

110 Robert Baldwin, Julia Black & Gerard O'Leary, "Risk Regulation and Transnationality: Institutional Accountability as a Driver of Innovation" (2014) 3 TEL 373 at 379.

111 Andrew Stirling, "Risk, Precaution and Science: Towards a More Constructive Policy Debate" (2007) 8(4) *EMBO Reports* 309.

112 Robert Baldwin, Julia Black & Gerard O'Leary, "Risk Regulation and Transnationality: Institutional Accountability as a Driver of Innovation" (2014) 3 TEL 373 at 379.

113 Raphael Gellert, "Data Protection: A Risk Regulation? Between the Risk Management of Everything and the Precautionary Alternative" (2015) 5 Intl Data Priv L 3 at 14.

114 Elizabeth Fisher, "Framing Risk Regulation: A Critical Reflection" (2013) 4 Eur J Risk Reg 125 at 126.

115 Lyria Bennett Moses, "How to Think About Law, Regulation and Technology: Problems with Technology as a Regulatory Target" (2013) 5 Law Innovation & Tech 1 at 10.

should not detract from the reality that the frameworks developed for risk regulation are not just tools for decision-making, but they represent the world, and in so doing "tacitly define the horizons of possible and acceptable action".[116] This makes it imperative that any regulatory system be designed in such a way as to account for the different value systems within the society in which it operates, in so far as this determines the social distribution of a risk.[117]

61 This task of creating a culture of responsible AI innovation in a way that is sufficiently responsive to power asymmetries and value pluralism is far from straightforward,[118] and requires a buy-in from all stakeholders. Moreover, this is a multifaceted process involving both inward and outward-facing aspects, as observed by Leslie and Shaw:[119]

> While practices of inward-facing reflection on purposes, positionality and power can strengthen the reflexivity, objectivity and reasonableness of AI research and innovation activities, practices of outward-facing stakeholder engagement and community involvement can bolster an AI project's legitimacy, social licence and democratic governance as well as ensure that its outputs will possess an appropriate degree of public accountability and transparency.

62 Nevertheless, it is arguably only where this is done that Singapore can truly go about seeking to make AI the "great equaliser" that uplifts and empowers society within an AI-enabled future.[120]

(2) Different approaches and paradigms

63 Whichever way one looks at it, risk regulation is a highly interdisciplinary area that requires a range of expertise – in sciences, in law, in policy and in politics.[121] Indeed, the unique challenges of regulating technology and innovation such as AI are recognised in

116 Elizabeth Fisher, "Framing Risk Regulation: A Critical Reflection" (2013) 4 Eur J Risk Reg 125 at 125.

117 Raphael Gellert, "Data Protection: A Risk Regulation? Between the Risk Management of Everything and the Precautionary Alternative" (2015) 5 Intl Data Priv L 3 at 17.

118 David Leslie & Patricia Shaw, "Ethics: Context Really Matters for Responsible Innovation" in *The Law of Artificial Intelligence* (Matt Hervey & Matthew Lavy KC eds) (Sweet & Maxwell, 2nd Ed, 2024) ch 3, at para 3-006.

119 David Leslie & Patricia Shaw, "Ethics: Context Really Matters for Responsible Innovation" in *The Law of Artificial Intelligence* (Matt Hervey & Matthew Lavy KC eds) (Sweet & Maxwell, 2nd Ed, 2024) ch 3, at para 3-023.

120 Smart Nation Singapore, "NAIS 2.0: Singapore National AI Strategy" (2023) at p 13 <https://file.go.gov.sg/nais2023.pdf> (accessed 1 March 2025).

121 Elizabeth Fisher, "Framing Risk Regulation: A Critical Reflection" (2013) 4 Eur J Risk Reg 125 at 131.

the "Collingridge dilemma",[122] where regulators seeking to control the development of technology face a double-bind problem, where: (a) the impacts of technology cannot be easily predicted until it has been extensively developed and widely used; but (b) influencing or controlling the technology becomes difficult when it has already become entrenched in society by virtue of its extensive development and widespread use.

64 It is in this context that governance approaches targeting the *process* of innovation – rather than merely the product of said innovation – have garnered increased attention as a means of steering innovation in a way which "connects innovation and technologies with social goals and values".[123] Singapore's Model Frameworks thus appear inclined toward such an approach, as a means of proactively shaping the design and deployment of AI to mitigate the downstream risks that may otherwise be posed by these AI systems.

65 Ultimately, in designing an AI regulatory framework for the future, Singapore cannot afford to confine itself solely within the domain of law, but should go about with the understanding that the regulation of risk can be conceptualised, framed and understood in a variety of ways that produce pragmatic frameworks for regulatory decision-making.[124] It is only through the meaningful synthesis of these different paradigms that the regulatory regime can truly operate as a system serving the needs and interests of the broad swathe of society.

VI. Conclusion

66 In the final analysis, risk regulation is primarily framed as a linear process, and while this is understandable, it is not desirable.[125] As Fenwick, Kaal and Vermeulen observe, regulatory decisions should not be thought of as final events, but rather as measured decision-making – open-ended and highly contingent choices that form merely one stage in a longer process.[126] Regulators need to abandon a fixation on finality and

122 David Collingridge, *The Social Control of Technology* (Frances Pinter, 1980).

123 Siobhan O'Sullivan, "Models of Governance for Innovation in Medicine and Health Research" (2020) 27 Eur J Health L 324 at 326.

124 Elizabeth Fisher, "Framing Risk Regulation: A Critical Reflection" (2013) 4 Eur J Risk Reg 125 at 131.

125 Elizabeth Fisher, "Framing Risk Regulation: A Critical Reflection" (2013) 4 Eur J Risk Reg 125 at 125.

126 Mark Fenwick, Wulf A Kaal & Erik P M Vermeulen, "Regulation Tomorrow: What Happens When Technology Is Faster than the Law?" (2017) 6 Am U Bus L Rev 561 at 589–590.

legal certainty and embrace contingency, flexibility and an openness to new ideas.[127]

67 Crucially, there is a continuing mismatch between technology on one hand, and existing laws and regulatory approaches on the other – the latter is designed for the technological landscape of the past, and therefore requires constant "reconnection" with the former.[128] Accordingly, there is a need to ensure that the proper mechanisms are in place to make continuous adaptations as circumstances change.[129] It is not sufficient to simply regulate according to "singular one-at-a-time" technological frames – the focus should instead be on protecting values and minimising harm in light of a continuously evolving socio-technical landscape.[130] Even where risk-based regulation continues to remain in place, this should necessarily be complemented by appropriate mechanisms, including monitoring tools and engagement and incentive strategies.[131]

68 Ultimately, responsible Al development necessitates a collaborative effort on the part of policymakers, developers and stakeholders to develop robust regulatory frameworks that allow AI to serve as a powerful force for social transformation, allowing us to build a more just and sustainable world.[132] It is only through fostering a collective culture of responsible innovation that mankind can harness the full power of AI, and move toward an AI-enabled future capable of positively impacting society.

---

127 Mark Fenwick, Wulf A Kaal & Erik P M Vermeulen, "Regulation Tomorrow: What Happens When Technology Is Faster than the Law?" (2017) 6 Am U Bus L Rev 561 at 590.

128 Lyria Bennett Moses, "How to Think About Law, Regulation and Technology: Problems with Technology as a Regulatory Target" (2013) 5 Law Innovation & Tech 1 at 7; Roger Brownsword, *Rights, Regulation and the Technological Revolution* (Oxford University Press, 2008).

129 Lyria Bennett Moses, "How to Think About Law, Regulation and Technology: Problems with Technology as a Regulatory Target" (2013) 5 Law Innovation & Tech 1 at 19.

130 Lyria Bennett Moses, "How to Think About Law, Regulation and Technology: Problems with Technology as a Regulatory Target" (2013) 5 Law Innovation & Tech 1 at 19.

131 Julia Black & Robert Baldwin, "When Risk-based Regulation Aims Low: Approaches and Challenges" (2012) 6 Regul & Governance 2 at 14–17.

132 Navneet Kaur, "Unravelling the Legal Nexus: Artificial Intelligence and the Path to Responsible Innovation" (2023) 6 Intl J L Mgmt & Human 1106 at 1117.