New Zealand Banking Association
Te Rangapū Pēke

Submission

to the

Department of Prime Minister and Cabinet

on the

Discussion Document: *Enhancing the cyber security of New Zealand's critical infrastructure system*

19 April 2026

NEW ZEALAND BANKING ASSOCIATION – TE RANGAPŪ PĒKE
PO Box 3043, Wellington 6140, New Zealand
www.nzba.org.nz

About NZBA

1. The New Zealand Banking Association – Te Rangapū Pēke (**NZBA**) is the voice of the banking industry. We work with our member banks on non-competitive issues to tell the industry's story and develop and promote policy outcomes that deliver for New Zealanders.

2. The following seventeen registered banks in New Zealand are members of NZBA:

- ANZ Bank New Zealand Limited
- ASB Bank Limited
- Bank of China (NZ) Limited
- Bank of New Zealand
- China Construction Bank (New Zealand) Limited
- Citibank N.A.
- The Co-operative Bank Limited
- Heartland Bank Limited
- The Hongkong and Shanghai Banking Corporation Limited
- Industrial and Commercial Bank of China (New Zealand) Limited
- JPMorgan Chase Bank N.A.
- KB Kookmin Bank Auckland Branch
- Kiwibank Limited
- Rabobank New Zealand Limited
- SBS Bank
- TSB Bank Limited
- Westpac New Zealand Limited

Contact details

3. If you would like to discuss any aspect of this submission, please contact:

Antony Buick-Constable
Deputy Chief Executive & General Counsel
antony.buick-constable@nzba.org.nz

Sam Schuyt
Policy Director & Legal Counsel
sam.schuyt@nzba.org.nz

Introduction

4. NZBA welcomes the opportunity to provide feedback to the Department of Prime Minister and Cabinet (**DPMC**) on the Discussion Document: *Enhancing the cyber security of New Zealand's critical infrastructure system* (**Discussion Document**). NZBA commends the work that has gone into developing the Discussion Document.

5. Overall, we are supportive of the proposal's focus on lifting cyber resilience and providing clearer guidance across critical infrastructure and essential services.

6. Defending the New Zealand economy against cyber disruption is an important and worthwhile exercise; the intent to lift national capability is well understood and aligns with similar provisions internationally.

7. We consider cyber security should be treated as an enabler of innovation, particularly as banks continue digital transformation programmes and adopt technology. We support a principles- and risk-based approach, with clear thresholds and proportionality, rather than prescriptive requirements that may not scale appropriately across different entities.

8. Aligning any new standards with existing requirements (including but not limited to the Emergency Management Bill, Deposit Takers Act 2023 (**DTA**) and Australian provisions made by the Australian Prudential Regulation Authority that apply to a number of our members) will be an essential part of the reform, to enable efficiencies and avoid risk of duplication, inconsistent obligations, or misaligned reporting thresholds and timeframes.

9. As a general comment, we consider it would be helpful for DPMC to clarify the primary purpose of the proposed regime – i.e., is the focus on cyber protection of critical infrastructure, or more generally the national resilience and service continuity of critical infrastructure – as this would help to inform views on the appropriateness of proposed measures.

10. Our submission addresses the following key points:

    10.1. Clarification of the purpose of the regime is needed (including both the scope of 'cyber' and of 'critical infrastructure'.

    10.2. Director liability and criminal penalties are disproportionate to both existing regimes and the nature of breaches.

    10.3. Careful consideration must be given to avoid unnecessary duplication with existing regimes.

    10.4. We strongly support two-way information sharing, but submit that further safeguards will be needed to facilitate the exchange of information.

Scope of regime

11. As noted in the introduction to our submission, we consider it is important for DPMC to clarify the primary purpose of the regime, as this will inform how appropriate and proportionate the proposed measures are.

12. There is a lack of a clear distinction in the Discussion Document between "cyber security" / "cyber attacks" and the broader concept of "cyber resiliency". This distinction is well captured by the below submission from the Financial Security Information Exchange (**FSIE**):

> While "cyber security" is a well understood and widely accepted term referring to the protection of information systems, networks and data from malicious or unauthorised digital activity, the standalone use of "cyber" is frequently applied to describe a much broader set of matters.
>
> In practice, "cyber" is often used as a proxy for wider technology, digital, operational and systemic resilience considerations, which extend beyond the established and clearly understood scope of cyber security.

13. The Discussion Document takes the approach of defining "cyber resiliency" in broad terms, covering both attacks but also, under the definition of "cyber security incident", any events, whether intentional or not, that cause adverse consequences to an ICT system or its data.

14. In doing so, the strategy risks continuing the common approach of conflating cyber attacks and general digital / technology resiliency.

15. We support the submission of FSIE, copied below:

> FSIE members consider that this imprecise use of terminology risks creating ambiguity for regulated entities, supervisors and policymakers, particularly where cyber security, broader technology risk and operational resilience obligations intersect. This ambiguity increases the likelihood of confusion in regulatory interpretation, overlap with existing sector-led regimes (including those administered by the Reserve Bank of New Zealand and other regulators), and inconsistent or disproportionate application of future requirements. FSIE therefore encourages greater discipline and clarity in language, ensuring that broader resilience expectations are framed explicitly in technology or digital terms, and that the term "cyber" is used only where its meaning is clearly defined and intended.

16. We further submit, in relation to the scope of the regime, that the definition of critical infrastructure should take into account other, potentially critical financial services beyond the current limit of domestically systemically important banks (as identified by Reserve Bank of New Zealand (**RBNZ**)).

17. For example, this definition excludes other, potentially critical financial services such as point of sale payment providers, that play an important role in the economy by linking customers, merchants and banks, and RBNZ's exchange settlement account system.

18. It will be important for DPMC to consider the extent to which the aggregation of services provided by common service providers, either as part of the market or in support of multiple critical infrastructure entities, should be considered as within scope.

Director liability and criminal penalties

19. We consider the director liability and criminal penalties associated with critical or serious breaches appear to be disproportionately severe when viewed against comparable director liability provisions under existing financial sector regulatory regimes (including the DTA, Credit Contracts and Consumer Finance Act 2003, Customer and Product Data Act 2025 and Financial Markets Conduct Act 2013 (**FMCA**)). We submit that DPMC should reconsider these thresholds.

Appropriateness of director liability for cyber risk

20. The proposed penalties do not sufficiently reflect the nature of directors' governance role in relation to cyber risk, where adverse outcomes may arise despite appropriate oversight, resourcing and governance. Given the technical complexity of cyber security, reliance on third-party providers and the evolving threat landscape, cyber outcomes alone are a weak proxy for director governance failure.

21. The Cyber Security Strategy and Cyber Security Action Plan are framed around four key objectives: understand; prevent and prepare; respond; and partner. Imposing director personal liability is not necessary to achieve the proposed objectives and may be counterproductive by distorting governance behaviours. For example, it may be more difficult to attract and retain appropriately qualified directors with the required expertise on the boards of critical infrastructure entities where liability exposure is unduly severe.

22. To the extent it may be introduced (noting our comments above), any director liability should be explicitly structured around a due-diligence based obligation. This is consistent with the approach adopted in the DTA. While the Discussion Document contemplates certain defences to liability in specified circumstances, these do not act as a substitute for the need to anchor director accountability within an appropriate due diligence framework.

23. Where director liability arises from non-compliance with minimum cyber requirements, specified rules, or submitting false or misleading information, liability should be clearly channelled through an assessment of whether directors took reasonable and appropriate steps, having regard to the information available to them at the time, their governance role, and the technical and third-party-dependent nature of the cyber risk.

24. Absent a due diligence standard, directors risk being held liable for cyber incidents or compliance failures despite reasonable governance and oversight, which is inconsistent with established approaches to director accountability.

25. Lastly, we submit that where cyber security standards or specified rules operate as the trigger for director liability offences, it is important that those instruments are not overly prescriptive or operational in nature. If detailed or technical standards or rules are used as the basis for personal liability, there is a risk that directors' exposure extends beyond a governance level role into matters of implementation and execution, blurring the boundary between governance and management.

Comparison to existing criminal liability thresholds

26. The cyber security proposals represent a material shift from established approaches in New Zealand's financial sector regulation. They extend criminal liability beyond deliberate or reckless misconduct to negligent or judgment-based failures in cyber risk governance and operational resilience.

27. By contrast, the FMCA reserves criminal sanctions for intentional or reckless market misconduct, while the DTA confines criminal liability to knowing non-compliance and defiance of regulatory directions, despite addressing systemic risk. Further, deemed director liability was removed for certain breaches under the climate-related disclosures regime in 2025.

28. Under the Discussion Document, cyber resilience failures arising from complex, evolving and adversarial risk environments could therefore attract criminal liability even where conduct amounts to negligence rather than conscious misconduct.

Proportionality of penalties for entities

29. The Discussion Document makes clear that the proposed compliance mechanisms are intended to be "fair, consistent and proportionate to the severity of the breach and degree of harm caused".

30. The proposed formula to calculate criminal penalties may give rise to a perverse outcome, where a different critical infrastructure entity may face a lower potential penalty because of a lower annual turnover, rather than the penalty being linked to the severity of the breach.

31. Further, the Discussion Document acknowledges that Australia's Security of Critical Infrastructure Act 2018 (**SOCI Act**) has been a primary reference point for the proposed New Zealand regime. However, the proposed New Zealand penalties appear to be much higher than those included in the SOCI Act.

32. We encourage DPMC to give due consideration to comparable penalty regimes while also having regard to New Zealand's economic scale.

Additional comments on liability

33. Clear definitions relevant to the proposed offending are also recommended so directors are clear on obligations and appropriate governance and reporting measures

can be put in place. In our view, any changes to director accountability should align with existing governance frameworks, and directors' duties and definitions.

34. Given the severity of some of the penalties as currently proposed (subject to DPMC's consideration of our submissions above), and considering the processes and controls that may be needed to meet new obligations, we further submit that a longer grace period should be contemplated. Twelve months is unlikely to be sufficient for the required uplift.

35. Finally, we note that the New Zealand Cyber Security Strategy 2026 – 2030 calls for a whole of society approach, but the current proposals appear to create an asymmetry between private and public sector compliance tools.

Duplication with existing regimes

36. NZBA submits that careful consideration needs to be given to ensuring any new requirements are well coordinated with existing frameworks. Without clear alignment, there is a risk that organisations may be required to meet substantively similar requirements through parallel regimes, with differing thresholds, timeframes or assurance mechanisms.

37. Our members are already required to comply with a number of security frameworks. In addition to those listed at paragraph 8 above (namely, the DTA and Emergency Management Bill), there is a risk that the proposal in the Discussion Document creates duplication with existing government security frameworks, particularly the Protective Security Requirements, the New Zealand Information Security Manual, National Cyber Security Centre (**NCSC**) guidance, and sector-specific prudential and incident reporting regimes (including, for example, condition 5 of the Conduct of Financial Institutions licensing conditions as it relates to operational resilience).

38. Where new regimes are introduced that have duplicative, but slightly different, requirements, the cost of compliance for regulated entities typically increases. The cost of complying with new requirements will depend in great extent on the differences between obligations set by the DPMC and other regimes, such as those listed above.

39. Many of the proposed expectations, such as board-level accountability, risk-based cyber controls, preparedness, and incident response are already embedded within these frameworks and, in practice, are applied across government and regulated sectors.

40. For example, we note that the proposed regime does not appear to replace banks' existing and upcoming obligations set by RBNZ, but instead layer further standards on top of them. From a practical perspective, it is helpful to have clear guidance in place where different regulatory bodies require reporting or information, and alignment between reporting timeframes, key definitions (for example "significant cyber incident"), and related requirements.

41. We encourage a coordinated approach that recognises equivalence with existing frameworks and avoids duplication or inconsistent obligations, particularly for entities operating across multiple regulatory regimes. For example, DPMC may consider establishing an empowered central incident response capability, aligning with the Australian National Cyber Co-ordinator function. This central function could coordinate with sector specific regulators (e.g., RBNZ for the banking industry) to ensure regulatory alignment and reduce reporting duplication.

Incident reporting and information sharing

42. NZBA strongly supports improved two-way information sharing and coordination between government and industry. This already takes place between financial institutions to some extent, but not more widely between other, non-financial institution critical infrastructure entities and government.

43. Infiltration by advanced, persistent threat groups like Volt Typhoon are designed to go undetected. It is not immediately clear which of the proposed measures (measures 1 to 4) would necessarily prevent or detect Volt Typhoon style activity. To help close this gap, greater coordination by Government is needed so that there are not just minimum standards and incident reporting, but Government to critical infrastructure entity threat intelligence sharing.

44. Further, in relation to the government's central role in information sharing, it is important that the government considers the funding and resourcing of NCSC to ensure it can effectively step in and support critical infrastructure. Further consideration should be given to the potential of nominating a national cyber coordination function, in line with that in place in Australia, to help navigate the wider system ramifications of cyber activities.

45. However, it will be important to ensure there are strong safeguards around sensitive customer and commercially sensitive information. The Discussion Document does not address whether entities would be afforded legal protection for the act of sharing information, for example against risks such as breach of confidence, exposure under the Privacy Act 2020, contractual confidentiality obligations, or potential conflicts with overseas legal requirements. We submit that the proposed reform must give due consideration to other, potentially opposing obligations given their importance to practical implementation.

46. We submit that any information to be shared needs to have a clear purpose for exactly why it is necessary to provide; as such, we caution against a blanket information-gathering approach.

47. In response to the questions of:

    47.1. Whether essential infrastructure should also be able to attend briefings / receive information, we think this is an appropriate uplift. However, we would

not expect that the required information sharing would sit with essential infrastructure entities and would instead be managed by the central agency responsible for the system.

47.2. The frequency of cyber incident reporting (if introduced), we submit this should align with the RBNZ material cyber incident notification reporting requirements. We would also encourage due consideration be given to the threshold of reporting.

Introducing minimum cyber risk management requirements

48. The Discussion Document provides that good risk management is key to enhancing the cyber security of New Zealand's critical infrastructure system, and that minimum requirements are set consistently. In relation to the particular questions posed by the Discussion Document on this topic, we submit:

48.1. The requirement to have third party vendors with operational control over critical components to support compliance is important – however, further clarity would be helpful to understand how this would operate in practice.

48.2. Whether or not the concept of a risk that is material can be given effect within existing enterprise risk management requires further definitional guidance on cyber risk materiality.

48.3. We agree that the Government should not prescribe the internationally recognised cyber security frameworks that are acceptable. Rather, we propose guidance is provided on relevant requirements.

48.4. With regard to demonstrating compliance with minimum cyber risk management requirements, we encourage DPMC to consider self-attestation, similar to the cyber periodic capability survey process under the Reserve Bank of New Zealand Act 1989 s 93 cyber reporting notice.

Additional comments

49. Measure 6 would give the Minister responsible the power to require critical infrastructure providers to do / not do certain actions, as a last resort.

50. It is a significant action for a Minister to take control of actions of a private entity, albeit for a specific purpose. It is difficult to determine whether this is needed, given no proposed criteria or thresholds have been provided, short of some high-level protections signalled in the Discussion Document.

51. Further, while the Discussion Document contemplates broad Ministerial direction powers, it does not expressly address whether entities would be protected from liability

arising from actions taken in compliance with such directions (for example, customer losses, contractual breaches, or downstream legal claims).

52. To assist with certainty we submit this power should only apply in clearly defined circumstances where other mechanisms are insufficient. Our preference is for a model focused on government support, coordination and surge capability rather than direct operational direction. We would encourage DPMC to consult further on an exposure draft of any legislation that is drafted to give effect to this power.

53. We also submit that public identification of designated entities may create unintended security risks for non-designated ones; we query whether smaller entities may become a target if they aren't seen to have to comply with the minimum standards.