NEW ZEALAND BANKERS ASSOCIATION

Submission

to the

Reserve Bank of New Zealand

on the

Consultation document: Risk management guidance on cyber resilience and views on information gathering and sharing

23 December 2020

NEW ZEALAND BANKERS ASSOCIATION
Level 15, 80 The Terrace, PO Box 3043, Wellington 6140, New Zealand
TELEPHONE +64 4 802 3358 EMAIL nzba@nzba.org.nz WEB www.nzba.org.nz

About NZBA

1. The New Zealand Bankers' Association (**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
   - 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.
   - Kiwibank Limited
   - MUFG Bank Ltd
   - Rabobank New Zealand Limited
   - SBS Bank
   - TSB Bank Limited
   - Westpac New Zealand Limited

Introduction

3. NZBA welcomes the opportunity to provide feedback to the Reserve Bank of New Zealand (**RBNZ**) on the consultation document: *Risk management guidance on cyber resilience and views on information gathering and sharing* (**Consultation Document**). NZBA commends the work that has gone into developing the Consultation Document and appreciates the opportunity RBNZ's workshop provided to discuss this material.

4. We acknowledge the importance of cyber resilience to the financial system and to New Zealand more broadly. As noted in the Consultation Document, regulated entities have a clear interest in maintaining cyber resilience, but we agree that financial sector regulators can play a useful role in this area. We support RBNZ's intention to create high-level and principles-based guidelines. However, we believe that the draft guidelines are currently too prescriptive in some areas. We prefer a more outcomes-based approach which entities can tailor to their own business. That is discussed in more detail below.

Responses to questions in Consultation Document

5. NZBA's responses to the questions in the Consultation Document are as follows:

Question	NZBA response
Q1 In light of the nature of cyber risk and the range of observed international practices discussed in the previous section, do you support RBNZ's policy stance of being 'moderately active' in promoting cyber resilience within the financial sector?	We support the proposal that RBNZ be 'moderately active' in promoting cyber resilience. In our view, the approach described as 'high activity' could drive a reactive approach in organisations, with a focus on reacting individually to regulatory findings rather than responding collectively to changing threats.
Q2 Do you agree with RBNZ's general approach of sticking closely to international best practice? Do you have any specific feedback on the draft guidance on cyber resilience?	<u>General feedback on draft guidance</u> We agree that the guidance should be high-level and principles-based. However, as discussed above, in our view the draft guidance does not currently achieve this approach. In some parts it has become a detailed, technical set of instructions (which we understand is not RBNZ's intention). Examples of this include where the draft guidance suggests a specific operating structure, or requiring that a cyber resilience strategy "should" outline specific topics. We prefer a more outcomes-based approach, which entities can tailor to their own specific needs and technologies. That is consistent with the approach taken by APRA in CPS 234, which some of our members are familiar with. The draft guidance's Governance commentary appears to confuse the roles of the board and management in some respects. In contrast, APRA's CPS 234 requires the board to ensure that information security is managed appropriately but other obligations are those of the regulated entity. If an entity has clearly defined the roles and responsibilities of the various parties involved in managing cyber risk, the board should be able to fulfil its ultimate responsibility for the cyber resilience of the entity without being directly involved to the degree contemplated by the draft guidance. We discuss this further in our detailed comments on Part A.

	Given the overlap with standards already in place, notably CPS 234 (for some members) and BS11 – outsourcing, we are pleased to see that the draft guidance appears to broadly replicate these. In relation to the enhanced-level practices outlined in the draft guidance, it is unclear when these are expected to be implemented. While we understand the guidance is intended to take a risk-based approach, it would be helpful to clarify expectations in this respect. For example, is there an expectation that highly prudentially regulated, and more mature financial institutions, such as registered banks, meet the enhanced principles? Clarity will be useful when working to operationalise the guidance, and to guide board understanding of RBNZ's expectations. Further detailed comments on the draft guidance are set out in the table below at paragraph 6. <u>International best practice</u> We agree with RBNZ's general approach of closely following international practice as this is well accepted and is already taken into account by many banks in managing cyber risk. In addition to referencing the National Institute of Standards and Technology – U.S Department of Standards and Technology Cybersecurity Framework (**NIST Cybersecurity Framework**) as a reference tool, we encourage RBNZ to look also to other international best practice, such as the Financial Services Sector Cybersecurity Profile (**FSSCP**). The FSSCP is based on the NIST Cybersecurity Framework and tailors the controls specifically to the financial sector. It has seven elements: 1) governance, 2) identify, 3) protect, 4) detect, 5) respond, 6) recover and 7) supply chain/dependency management. These are in close alignment with the elements set out in the draft guidance. As IOSCO pointed out in its June 2019 Cyber Task Force Report, the FSSCP "…..is a customization of the NIST Cybersecurity Framework that financial institutions can use for internal and external cyber risk management assessment and as evidence for compliance, encompassing relations between Cyber frameworks, including Core Standards. Further, the tool encompasses all three of the Core Standards of this report, as well as others….." (page 18).

Q3 Do you agree that the guidance should be a set of high-level principle-based recommendations?	We agree the guidance should be a set of high-level principle-based recommendations, rather than prescriptive/detailed rules. However, as discussed above, at present a number of the principles are very granular, and we consider that RBNZ should reflect on the degree of detail provided in the guidance.
Q4 What's your view on the principle of proportionality and a risk-based approach adopted by the Guidance?	We are supportive of the guidance adopting the principle of proportionality and a risk-based approach.
Q5 Do you agree that the guidance should apply to all regulated entities of the RBNZ?	Agree.
Q6 What's your view on RBNZ's collaborative and coordinated approach to information gathering and sharing?	We are supportive of a collaborative and coordinated approach to information gathering and sharing subject to an appropriate confidentiality overlay.
Q7 Do you support RBNZ's intention to broadly follow the international practices and establish a cyber data collection for all prudentially regulated entities? Do you have any particular concerns or issues that you would like RBNZ to take into account when further developing its plan?	We are supportive of the intention to broadly follow international practices and establish a cyber data collection for all prudentially regulated entities. In relation to reporting cyber incidents, we note that informal reporting of cyber incidents to RBNZ is already happening. RBNZ has indicated it is planning to consult on the data collection requirements once the guidance is finalised and we look forward to participating in that process. Any RBNZ developed information gathering and sharing resource, while it may be useful, would need to be carefully designed and: • Should not be at the expense of existing voluntary forums in which banks already participate. There is value in these being sector focused, and for admission/participants to be vetted, as it allows for free and frank discussion and information sharing

	without concern in respect of confidentiality or reprisals. • Should not impose significant reporting burdens which redirect expertise/resource on/from financial institutions at a time when they may be responding to cyber incidents (which can be complex and fast-moving). For example, RBNZ should consider if information gathering could in certain cases be achieved by information sharing between regulators (eg a notifiable privacy breach reported to the Privacy Commissioner may be as the result of a cyber incident such as a ransomware attack, meaning personal information is temporarily or permanently unavailable causing serious harm to affected individuals). We are also concerned that this may lead to an aggregate of information that could be used against regulated entities. This could be addressed through a level of data sanitisation and collaborating on how the aggregate of data would be best protected and used. Our understanding from the recent workshop is that RBNZ's intention is that data collection of periodic survey information will be done infrequently. We consider that appropriate and would support that approach.

Detailed comments on draft guidance

6. NZBA's detailed comments on the draft guidance are as follows:

Part A: Governance	• A1.4: This provision contemplates both the board and senior management's involvement in ensuring that staff with cyber resilience related roles and responsibilities are qualified to perform their roles and are informed and empowered to act in a timely manner. While it is not clear what RBNZ's expectation is in terms of the board's involvement, this is an area where we would expect management to have responsibility generally. • A1.6: Similar to our comment above, we would not expect a board to approve all the matters set out in this section. Matters such as the procedures and controls necessary to support the strategy and framework are matters of detail that would normally be left to management.

	• A1.7.1: Remove the word “budgeting”, the focus should be on the plan. • A1.8: This principle should be future proofed to allow for developments, eg if there is an increase in virtual CISO support being provided to CTOs. Similar to our comments in A1.4, management should be able to appoint the CISO rather than this being a joint responsibility with the board. We reiterate our earlier comment that each bank should be able to determine appropriate governance based on its own business context. • A1.8.1: It is unclear what “act independently from the IT/operations department” means, ie whether this is a skills/expertise expectation. Rather than focusing on matters of structure, we consider the draft guidance should focus on the outcomes that RBNZ wants to achieve, ie, that there is a clear line of communication through to the board for cyber resilience issues. We note that it is not unusual in New Zealand for the CISO to be a member of the IT/operations department. We consider this an appropriate and effective model for the CISO role. It ensures that they are across the issues and are part of the solution. • A1.8.2: Again, we consider that this level of detail (ie matters of structure) is not required in principles-based guidance. • A2.1.1: In line with our feedback that the draft guidance could be more high-level and principles-based, we consider this bullet point list is too prescriptive, and “could” should replace “should”. It should be up to entities, with the oversight of their boards, to develop a strategy and framework which meets the requirement of A2.1 • A2.5: “Internal audit” should be replaced with “independent assurance” as there may be the need for external expertise if that skillset cannot be sourced internally (especially for smaller banks). • A3.1.1: We consider that it is more appropriate to share relevant information about the cyber resilience strategy and framework with staff, rather than the strategy and framework in its entirety. • A3.2.1: We suggest that this is amended to clarify that specific cyber threat intelligence can be shared with only key stakeholders and not business-wide. Although we agree that staff training, for example,

	should be informed by intelligence about cyber threats.
Part B: Capability building	• B2.2: Requiring segmentation is very specific and approaches to segmenting networks are varied. This is not consistent with the intention to provide principles-based requirements. Segmentation is one of the mitigants to cyber-attacks, but there are a number of others. Segmentation could be included, along with some other approaches, as examples of boundaries. • B2.3.2: We consider this should be amended with a focus on understanding the risk of these legacy systems and taking into account compensating controls. Banks should be empowered to make risk-based decisions regarding their approach to legacy systems, which may include retaining them within the organisation for a period of time. • B2.5: The reference to "life cyber" should be to "life cycle". • B2.6: We consider this requirement is too specific for principles-based guidance. • B4.7: This principle would be clearer if it read "The entity should have processes and procedures in place to conduct a post-incident analysis to identify the root cause of its cybersecurity incidents, and integrate its findings back into its response and recovery plans."
Part C: Information sharing	No specific comments.
Part D: Third-party management	• Most of Part D appears to be broadly consistent with BS11 policy, but the draft guidance looks to add an additional layer of 3rd party risk assessment. We query whether that is RBNZ's intention. • D4.1.1: We consider the intent of this principle would be clearer if it was amended to read "Clearly identify and document the cyber risk associated with using third ***party service providers*** and update this information on a regular basis." • D4.1.2: It would be helpful to understand the intention of this requirement and whether it is expected that banks will have proactive capabilities to monitor third party connections into their networks, or whether it is sufficient that they rely on the end-point security controls they already have within their organisation.

	• D4.1.3: It would be helpful to understand the intention of this requirement. Although it is possible to contractually obligate a third party to ensure it has appropriate identity controls in place, it is not common market practice for a bank to be "tracking actively" third party employee access. If this principle is to be maintained, we consider it should be enhanced, not baseline. • D4.1.4: We consider the involvement of third parties in response to testing should be an enhanced, rather than a baseline requirement. That is because banks will not necessarily always be able to contractually agree such participation with their third party service providers, or it may be able to be agreed only on the basis of a significant additional fee. • D4.2: We would welcome a definition or guidance in respect of the meaning of an "entity's critical functions". As a baseline standard, this would be problematic to implement/not pragmatically reasonable, as third-party service providers which provide systems critical to bank functions are not in many cases easily substitutable. It is especially unclear how banks should prepare for transitioning to alternative service providers, and it may not be possible for certain critical services to be performed in-house. Contracts with key third party service providers ordinary include SLAs in relation to system performance/availability, requirements for BCPs, obligations on the service provider in the event of termination, etc which seek to mitigate the impact of outages/performance failures. We consider this baseline standard should be reconsidered. • D5.1: This requirement could be understood in different ways, and leans towards being overly prescriptive. The wording "at least through the providers' self-assessment if not through conducting its own assessment" could be taken to cross over with the enhanced point covered at D5.2, and we ask that it be removed. • D6.1: It would be helpful for RBNZ to clarify what is meant by "interconnection with other entities". Is this referring to APIs, interconnectedness in the context of reliance, or something else? • D7.1: The termination/exit of third party service providers is ordinarily contractually provided for, including transition and service continuation

	provisions. It would therefore be helpful for RBNZ to clarify what is expected here. • D8 (cloud services) requires further clarification. For example, regarding D8.1 – will banks be required to obtain formal approval from RBNZ for usage of cloud-based services or is the intent that they provide notification? If it is the former, what process and timelines will be in place at RBNZ? What is the process in respect of existing cloud storage providers? What does RBNZ intend to do with the information provided to it, ie what is the purpose of the notification? NZBA welcomes further guidance on how members should approach cloud-based services.

Contact details

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

Antony Buick-Constable
Deputy Chief Executive & General Counsel
[redacted]

Olivia Bouchier
Policy Director & Legal Counsel
[redacted]