Financial Services Council.
Growing and protecting the wealth of New Zealanders

Financial Services Council of New Zealand
Level 33, ANZ Centre,
23-29 Albert St, Auckland 1010
P: +64 9 985 5762
E: fsc@fsc.org.nz
www.fsc.org.nz

Friday 29 January 2021

Dynamic Policy Team Financial System Policy and Analysis
Reserve Bank of New Zealand
PO Box 2498
Wellington 6140

By email: cyberresilience@rbnz.govt.nz

Reserve Bank of New Zealand Cyber Resilience

This submission on the Reserve Bank of New Zealand (RB) Consultation Document, Risk management guidance on cyber resilience and views on information gathering and sharing, 20 October 2020 (the Consultation) and the Guidance on Cyber Resilience (the Guidance), is from the Financial Services Council of New Zealand Incorporated (FSC).

The FSC is a non-profit member organisation and the voice of the financial services sector in New Zealand. Our 91 members comprise 95% of the life insurance market in New Zealand and manage funds of more than $83bn. Members include the major insurers in life, health, disability and income insurance, fund managers, KiwiSaver and workplace savings schemes (including restricted schemes), professional service providers, and technology providers to the financial services sector.

Our submission has been developed through consultation with FSC members and represents the views of our members and our industry. We acknowledge the time and input of our members in contributing to this submission.

The FSC's guiding vision is to be the voice of New Zealand's financial services industry and we strongly support initiatives that are designed to deliver:

- strong and sustainable customer outcomes
- sustainability of the financial services sector
- increasing professionalism and trust of the industry.

We welcome the opportunity to provide feedback on the Consultation and we would very much like to coordinate with the RB on a workshop to be held following the publication of the consultation. We do however note concerns with the timing of this Consultation and only one opportunity to provide feedback on the Guidance prior to its publication in March/April 2021. We therefore welcome and encourage continued discussions to ensure that the Guidance is suitable and well considered for the industry.

As frequently noted in FSC industry submissions, we encourage collaboration exercises between the Regulators, perhaps through the Council of Financial Regulators, to ensure consistency and to reduce duplication, confusion, and compliance burdens where there are multiple guides and requirements issued that deal with cyber resilience.

Financial Services Council.
Growing and protecting the wealth of New Zealanders

Financial Services Council of New Zealand
Level 33, ANZ Centre,
23-29 Albert St, Auckland 1010
P: +64 9 985 5762
E: fsc@fsc.org.nz
www.fsc.org.nz

I can be contacted on [redacted] to discuss any element of our submission.

Yours sincerely

Richard Klipin
Chief Executive Officer

Financial Services Council of New Zealand
Level 33, ANZ Centre,
23-29 Albert St, Auckland 1010
P: +64 9 985 5762
E: fsc@fsc.org.nz
www.fsc.org.nz

Q1. In light of the nature of cyber risk and the range of observed international practices discussed in the previous section, do you support the Reserve Bank's policy stance of being 'moderately active' in promoting cyber resilience within the financial sector?

We support the RB's stance of being moderately active. The publication of risk management guidance, as well as alignment with cyber security public sector bodies such as the National Cyber Security Centre and CERT NZ, is likely to raise awareness within the financial services sector of what strong cyber resilience entails. Along with improved information sharing practices, this will be beneficial to the New Zealand business and financial services sectors.

In contrast, low activity may not achieve the outcomes sought and high activity, including legally binding requirements, is not ideal for cyber security which is a technical and specialised area that needs to be tailored to individual entities. In addition, high activity would require significant additional resources and may drive a reactive approach in organisations, with a focus on reacting individually to regulatory findings rather than responding collectively.

Q2: Do you agree with the Reserve Bank's general approach of sticking closely to international practice?
Do you have any specific feedback on the draft Guidance on cyber resilience?

We agree that it is important to consider and align with international practice in the formulation of guidance and best practice for New Zealand where appropriate. In particular, with many of our members having Australian connections, consideration of the approach of Australian regulators is important. It will also assist a number of financial entities who currently look to international frameworks as best practice within their organisations to align more easily with the RB's Guidance. We also encourage review of other applicable and comparable cyber frameworks that are more advanced than New Zealand and have been tested and evolved.

As the legal status and enforceability of the Guidance is not yet clear, we suggest the status of the guidance should be advisory rather than enforceable, given the acknowledgment in the RB's consultation that "*a commonly agreed 'best practice' framework to address cyber risk has yet to emerge*".

Draft Guidance

We have the following specific feedback on the Guidance:

- **A1:** Whilst we support the aim of the Guidance to raise awareness of cyber resilience at the board level, this needs to be balanced with management's role in relation to the implementation of appropriate frameworks and standards to manage cyber risk. A board should be able to meet its responsibilities without being involved to the extent contemplated by the guidance.
- **A1.8:** Regarding the requirement that a senior executive be appointed to take care of cyber resilience issues, we expect that this would not necessarily have to be the senior executive's sole role but could be one aspect of it.
  A1.8.1: Whilst we support segregation of duties, we encourage further clarification on the term *act independently* and what this means in practice. Cyber resilience is an integral part of the IT/operations department and the executive responsible for IT/Operations would most often be responsible for cyber resilience issues. We encourage consideration as to whether matters of structure or the level of detail included in A1.8.1 and A1.8.2 are required for principles based guidance and recommend that the Guidance remain neutral on this detail.

Financial Services Council of New Zealand
Level 33, ANZ Centre,
23-29 Albert St, Auckland 1010
P: +64 9 985 5762
E: fsc@fsc.org.nz
www.fsc.org.nz

- **B2.2:** Approaches to segmenting networks are varied and we suggest further clarification on what the RB intends financial entities to consider.
- **B2.3.2:** Whilst we support the principle that removing legacy systems contributes to improved cyber resilience, the current wording could be interpreted that systems should be immediately removed. We recommend amendments so that there is focus on understanding the risk of these systems in an organisation's environment (taking into account compensating controls) and that financial entities are encouraged to make risk-based decisions on their approach to legacy systems. This may include retaining them within the organisation for a period of time or a phased approach to upgrades or replacements.
- **B2.6:** We query whether this level of detail is required for principles based guidance.
- **B4.1.6:** We support the intent of this statement and would like to understand if the RB expects financial entities to have documented scenarios? Cyber threats are evolving, and we consider it important to have a holistic cyber incident response process in place, rather than focusing solely on individual scenarios.
- **D4.1**: While this point states that the entity should consider the cyber risk associated with its third parties in each stage of its own capability building described in Part B, we consider that it would be more helpful to entities if relevant considerations were also included in Part B of the guidance. This would assist entities to understand how to build capabilities in respect of third party management, so that they will be well placed to manage this aspect.
- **D4.1.2:** We request clarification on the intent of this statement from the RB, as to whether there is an expectation that financial entities will have proactive capabilities to monitor third party connections into their networks or is it sufficient for financial entities to rely on the end-point security controls they may already have within their organisation?
- **D4.1.3:** We note that 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 financial entity to be *tracking actively* third party employee access. We request further clarification on this point.
- **D8.1:** Further clarification is sought as to whether financial entities will be required to obtain formal approval from the RB for usage of cloud based services or is the intent to provide notification? If it is the former, what process and timelines will be in place from the RB?

Q3: Do you agree that the guidance should be a set of high-level principle-based recommendations?

We agree that Guidance based on principles are preferable to prescribed recommendations. We encourage consideration of not only the range of entities that the Guidance will apply to but also the varying sizes of those entities, as having a one size fits all detailed and technical approach would not be suitable. We note that in places, the Guidance is more prescriptive, for example suggesting a specific operating structure as noted under A1.8 in this submission. We encourage the RB to consider a more outcomes based approach to meet the principles based aims of the Guidance.

Q4: What's your view on the principle of proportionality and a risk-based approach adopted by the Guidance?

We support the principle of proportionality and a risk-based approach being adopted for the Guidance. We consider it appropriate given the range of entities regulated by the RB both in terms of industry and scale. However, we consider it is important to emphasise that a risk-based approach must consider the potential harm of cyber events and incidents on New Zealand consumers.

A proportional approach to the Guidance means that for entities with an existing mature cyber resilience program, the Guidance is an opportunity to revisit and evaluate existing practices, while providing a roadmap and additional support for entities that are still in the process of implementing cyber resilience program.

Financial Services Council
of New Zealand
Level 33, ANZ Centre,
23-29 Albert St, Auckland 1010
P: +64 9 985 5762
E: fsc@fsc.org.nz
www.fsc.org.nz

In relation to the split between *baseline* and *enhanced* in the Guidance, we would like to understand if the RB expects all financial organisations to adopt the baseline requirements or whether the intent is adoption in accordance with a financial organisation's size and risk appetite?

Q5: Do you agree that the Guidance should apply to all regulated entities of the Reserve Bank?

We agree that the Guidance should apply to all regulated entities of the Reserve Bank given the importance of cyber risk and ensuring the financial stability of New Zealand, particularly if the Guidance is implemented as proposed in this Consultation, namely it is aligned to international practice, consists of high level principle based recommendations and a principle of proportionality applies.

Q6: What's your view on the Reserve Bank's collaborative and coordinated approach to information gathering and sharing?

We support in principle a collaborative and coordinated approach and would encourage information sharing as a key tool to combatting cyber attacks, however we have concerns relating to the security of the information once it has been provided. We would encourage the RB to consider providing entities with visibility over how the RB manages, stores and protects the information that is collected.

In addition, we are eager to understand the extent to which the RB proposes to share information with the public and within the industry, given the acknowledgment by the RB that certain cyber related information can be highly sensitive. We understand that the RB intends to consult more fully on this aspect this year and we welcome further discussion at that time.

We note that in considering data collection, information gathering and information sharing, along with coordinating with other public bodies, it is important that the goals and approach are carefully considered and specifically laid out. There is the potential for reduced value in a data collection exercise if it devolves to a pure information gathering activity. We encourage a focus on understanding current cyber threats and the effectiveness of varying approaches and security measures.

Q7: Do you support the Reserve Bank'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 the Reserve Bank to take into account when further developing its plan?

We support data collection for all prudentially regulated entities and as cyber capability develops, we encourage the RB to consider that depending on the nature of a cyber security incident, entities may not be able to provide the full impact of an incident right away. The information sharing processes will need to be reflective of this to ensure entities are not distracted in the early stages of a cyber security incident due to reporting requirements. We interpret section 4.4 of the Consultation as the RB's indication it understands the importance of this and will develop processes, which enable financial entities and the RB to execute their mutual responsibilities.

A concern in relation to cyber data collection is that this may lead to an aggregate of information that could be used for enforcement purposes in respect of 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.

Whilst we understand the need to establish cyber data collection, we strongly encourage the RB when further developing its plan to take into account what other regulators are doing in this space in New Zealand and to consider a coordinated approach or joint plan, such as through the Council of Financial

Financial Services Council of New Zealand
Level 33, ANZ Centre,
23-29 Albert St, Auckland 1010
P: +64 9 985 5762
E: fsc@fsc.org.nz
www.fsc.org.nz

Regulators or a single regulator. When multiple regulators require similar or even the same information, this comes at a cost to the industry in both time and resources and there is potential for confusion and duplication of compliance and reporting for regulated entities. Such duplication would be overly burdensome for regulated entities and ultimately provide no additional benefit for consumers (who may ultimately bear the costs). In addition, some entities have teams to enable the collation of data and smaller entities may struggle in this regard.

An example of the regulator overlap is between the RB and the Financial Markets Authority (FMA) in the oversight of cyber resilience particularly with the FMA as the regulator of proposed conduct legislation pursuant to the Financial Markets (Conduct of Institutions) Amendment Bill. There are and will be many entities that are regulated by both the RB and the FMA. We note that the FMA has already issued requirements for its regulated entities in respect of cyber resilience including the Cyber-resilience in FMA regulated financial services report issued in July 2019. This report sets out guidance and expectations and the Standard Conditions for Financial Advice Provider licences issued in November 2020 imposes cyber threat identification and reporting requirements on Financial Advice Providers. By way of further example, where cyber incidents involve a notifiable privacy breach under the Privacy Act 2020, entities may also be working with the Office of the Privacy Commissioner to respond to the incident.