ICNZ Insurance Council of New Zealand

Insurance Council of New Zealand
P.O. Box 474 Wellington 6140
Level 2, 139 The Terrace
Tel 64 4 472 5230
email icnz@icnz.org.nz
Fax 64 4 473 3011
www.icnz.org.nz

29 January 2021

Dynamic Policy Team
Financial System Policy and Analysis
Reserve Bank of New Zealand
Wellington

Emailed to: cyberresilience@rbnz.govt.nz

ICNZ submission on RBNZ Risk management guidance on cyber resilience and views on information gathering and sharing consultation document

Thank you for the opportunity to submit on the RBNZ Risk management guidance on cyber resilience and views on information gathering and sharing consultation document.

ICNZ represents general insurers that insure about 95 percent of the New Zealand general insurance market, including about a trillion dollars' worth of New Zealand property and liabilities. ICNZ members provide insurance products ranging from those usually purchased by individuals (such as home and contents insurance, travel insurance, motor vehicle insurance) to those purchased by small businesses and larger organisations (such as product and public liability insurance, professional indemnity insurance, cyber insurance, commercial property, and directors and officers insurance).

Please contact Jane Brown [redacted] if you have any questions on our submission or require further information.

This submission is in two parts:

- Overarching comments
- Responses to individual questions

Individual members may take differing views to ICNZ on some issues and those members will submit to you separately on them.

Overarching comments

ICNZ welcomes this consultation, as we believe that greater guidance on cyber resilience is a positive step for New Zealand's regulators to take, particularly for the financial sector which is frequently a target of cyberattacks and incidents. This consultation is also consistent with the approach being taken by regulators on the international stage. For example, in a recent announcement, APRA's Geoff Summerhayes told the financial sector that it will increase its supervision and scrutiny of regulated entities' cyber risk management in 2021[1].

[1] https://www.apra.gov.au/news-and-publications/executive-board-member-geoff-summerhayes-speech-to-financial-services.

We are also aware that there is increased interest in cyber resilience amongst New Zealand regulators, and not just the Reserve Bank, with the FMA also taking an interest in this space. For this reason, we support an integrated and collaborative approach to cyber security and cyber data collection by regulators and other entities like NCSC and CERT. There is a need, in relation to data collection in particular, to avoid a situation where entities are expected to report the same or similar information via multiple channels, which would be time-consuming and could potentially impact on an entity's ability to respond efficiently to a cyber incident. Duplicate reporting for multiple regulators would also mean added cost which would disproportionately impact smaller entities with less resources at their disposal. We go into further detail on these points in our responses to the questions below.

We would also like to point out the difficulty in providing in principle agreement to an information gathering and sharing scheme when the details of such a scheme are not yet known. The consultation document indicates that there will be further consultation on a detailed proposal for data collection later this year, but not until many months after the close of this consultation. This is an unhelpful timeframe given that submitters are asked to provide agreement and/or raise any concerns at this stage without the benefit of having seen what will be required.

The recent cyberattack on the Accellion FTA platform, with the full consequences as yet unknown, raises a number of questions for this consultation, which aims to ensure cyber resilience amongst regulated entities. We believe the findings of the review into the attack should be shared with the industry and that lessons learned from the breach used to better inform cyber risk management frameworks for the Reserve Bank and the entities it regulates. We encourage the Reserve Bank to continue being as transparent as possible in the interests of supporting a robust cyber security system, acknowledging that to date, it has made great efforts to be transparent about the extent of the breach and to communicate openly with the industry in this regard. As part of the communications, it would be helpful to know which cyber security framework the Bank itself currently adheres to, and whether there are alternate frameworks used by the likes of CERT and NCSC.

The attack also highlights the risk of the proposed information gathering and sharing outlined in the consultation document. If the Reserve Bank holds information about the cyber security arrangements of financial institutions, which could potentially reveal weaknesses and/or vulnerabilities in their systems, and this information was subject to a breach, it could make them an attractive target for future attacks. We await further details about the changes being made by the Reserve Bank to increase the security of any information being gathered, shared and stored in future.

Finally, we encourage the Reserve Bank to give thought to what implementation of the guidance will look like in practice once it has been finalised. In our view, most entities have a reasonable level of awareness around the importance of cyber security, but it is the putting the guidance into action where ongoing support will be required and collaboration between entities encouraged. It would also be useful to provide an overview of where the Reserve Bank currently believes the level of cyber security is amongst regulated entities and where they hope it will be in 5-10 years' time, perhaps using a similar framework to that included on page 7 of the Bank's Digital Services Consultation for Change proposal[2].

[2] https://www.rbnz.govt.nz/-/media/ReserveBank/Files/Publications/Information-releases/Digital-Services-Consultation-For-Change-Proposal.pdf?revision=0040d660-09b2-41ab-b59a-e73f20f8ab8c, pg 7.

Responses to individual questions

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?

ICNZ agrees that taking a moderately active policy stance is the most appropriate approach and is proportionally aligned to international and peer regulatory expectations for the financial industry regarding cyber resilience. We encourage the Reserve Bank to not necessarily limit itself to the definition of "moderately active" as outlined in the consultation document and consider, for example, ongoing discussions and workshops for regulated entities around implementation of the guidance once finalised as this will be important to drive the development of overall cyber resiliency.

Q2. Do you agree with the Reserve Bank's general approach of sticking closely to international practice?

ICNZ agrees with the Reserve Bank's general approach of sticking closely to international practice. This is particularly important for those of our members who have parent companies in other jurisdictions and will enable easier peer benchmarking, both domestically and internationally.

Do you have any specific feedback on the draft guidance on cyber resilience?

We make the following specific comments in relation to the draft guidance on cyber resilience:

Part A - Governance

A1 - Board and Senior Management Responsibilities

- We note that the description of the role of the senior executive differs slightly between A1.3 (*The board and senior management should assign a senior executive with the appropriate skills, knowledge and experience to be accountable for the cyber resilience strategy and* framework) and A1.8 (*The board and senior management should appoint a senior executive…to take care of cyber resilience* issues). We assume the same senior executive is being referred to in both A1.3 and A1.8. If not, then we question whether there is a reason why there is a difference. If the difference between the two is that the person in A1.8 must be a senior executive with independence from both the IT/operations department and internal audit activities, this may create difficulties for smaller entities with fewer senior executives who could perform the role with sufficient independence.
- We therefore question whether it would be feasible for small organisations to provide for this requirement (i.e. the cost of employing a senior executive for this specific function or achieving the necessary independence from IT and audit). To provide for more flexibility in the expectation, it should be acceptable to engage a third party to fulfil this function where the scale of operations do not permit a senior executive being assigned to the role, noting that as per A1.1, the Board would retain ultimate responsibility for the entity's cyber resilience.
- Related to the first bullet point, we consider the requirement in A1.8.1 that the senior executive "*can act independently from the IT/operations department and be able to report to senior management and the Board directly*" needs to be clarified as to what 'act independently' means in practice. Cyber resilience is an integral part of the IT/operations department and the executive responsible for IT/operations is often on the senior management team and would have access to the Board.

- Regarding the requirement in A1.8 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 rather one aspect of it (noting that, depending on the size of the entity, it could be a significant part of that individual's role).
- Specifically, in relation to some financial institutions operating in multiple countries, flexibility as to who can be appointed to these roles is necessary so that these entities can design a cyber resilience strategy and framework which is globally consistent and which has oversight at a global level. This will allow for cyber resilience strategies, frameworks and standards to be consistently applied across all countries the financial institution operates in. This will also ensure transparency and accountability while leveraging global expertise, knowledge and skills.

A3 - Culture and Awareness

- A3.1.1 says that "*This culture should be conveyed through clear and effective internal communication, and should include the dissemination of the cyber resilience strategy and framework to all staff*". Financial institutions will have information security and privacy policies which are already conveyed to all staff, so they understand their information security responsibilities. However, these policies differ from the cyber resilience strategy and framework, which we anticipate would be a document that is more targeted to the information security and executive team and may not be easily understood by, relevant to, or appropriate for all staff. It is unclear what the purpose of providing information on organisational cyber resilience to staff generally would be and this is unlikely to be an appropriate tool for educating employees on the key actions they need to take, or avoid, to support the cyber resilience of their organisation. We therefore expect that, rather than the strategy and framework being disseminated, using the principle of proportionality, it would be more appropriate for an organisation to provide information and training which convey the relevant messages about the importance of information and cyber security and the steps that various people need to undertake in this regard.

Part B - Capability Building

Identify - Enhanced

- In relation to B1.5 (*The entity should carry out a holistic self-assessment…*) we would appreciate clarification on what would constitute a "holistic self-assessment". For example, would red team, penetration testing, and vulnerability scans meet the intention behind the wording?

Protect

- We believe that B2.3.2 relating to legacy systems should be removed from the guidance. While entities may consider replacing legacy systems, it will not always be practical to do so, and may not be necessary where other reasonable security measures designed to ensure a level of security appropriate to the risk are implemented.
- B2.6 sets out an expectation of screening and background checks for all new employees and contractors before they are hired/contracted *as well as for existing employees on a regular* basis, proportionate to their access rights. It is unclear why screening and background checks should be conducted for existing employees following the introduction of this guidance, when it is most likely that they would have been screened at the time that they were hired/contracted. We do not believe there should be further screening and checks (unless they were not originally carried

out or the organisation believes they are warranted), as those already carried out would have been appropriate at the time.

- We do not believe that B2.9 (*The entity should implement automated mechanisms that can isolate affected information assets in the case of an adverse event*) should be so prescriptive. While entities may consider automated mechanisms to isolate affected information assets as an appropriate security mechanism, it may not be appropriate to do so in all circumstances.

Detect

- We believe that B3.7.1 (*The penetration tests should be conducted on a regular basis, as well as each time a major change occurs to the cyber threat status of the entity, such as when the entity implements new systems or* technologies) should be amended to reflect that new systems or technologies should not necessarily trigger the need for a penetration test, as application and system vulnerability scans may be more appropriate. Our view is that flexibility should be permitted to allow an entity to make an assessment about whether and when testing is conducted as the circumstances appropriately require.

Respond and Recover

- In relation to C1.2 regarding meeting relevant regulatory requirements for reporting, it will be essential for these guidelines to be checked against and joined up with other governmental agency and regulatory requirements to prevent unnecessary regulatory burden, inconsistencies and duplication.

Part C – Information Sharing

C1 – Channels

- The preamble to Part C provides that "*Information that can be shared includes indicators of compromise (IOC), cyber incidents, threats, vulnerabilities, risk mitigation, best practice and strategic analysis*". Further clarity is required around whether there might be an expectation that information other than the matters already listed should be shared.

Part D – Third-party management

As a general comment, we consider that the Reserve Bank should be clearer in this section about what they consider the definition of "outsourcing" to be. A reading of Part D assumes that an outsourced agreement would be one that has been negotiated between parties and the question therefore arises as to whether the use of Software as a Service (SaaS) solutions would be considered outsourcing. The use of SaaS has become incredibly common and many services are provided on the basis of standard terms and conditions, not negotiated terms. Related to this, we question whether it would be expected that regulated entities report their SaaS arrangements to the Reserve Bank?

D6 – Documentation

- Further clarity is required on guideline D6.1 (*The entity should maintain an up-to-date comprehensive inventory of its third-party service providers and interconnection with other entities, as well as regularly updating the networking map of its external dependencies*). It is unclear on a reading of the guideline what the Reserve Bank believes would satisfy this expectation. We also suggest that the latter requirement in this guideline (regularly updating the networking map of its external dependencies) be removed as it is vague and could become costly to manage. We consider that this requirement should be kept to a high level.

D8 – Outsourcing to Cloud Service Providers

- D8.1 (*The entity should inform the Reserve Bank about their outsourcing of critical functions to cloud service providers early in their decision-making process*) seems to be quite a new concept for New Zealand entities. We believe that the guideline would benefit from the inclusion of additional detail to increase understanding about what the Reserve Bank's expectations are in this regard. First, the Reserve Bank should specify which functions it would consider to be critical and secondly what "decision-making process" they are referring to. Entities may, or may not, run a full procurement process before selecting a cloud service provider – is the reference therefore to the procurement process? Additionally, we expect from the use of the word "inform" that this requirement is just a matter of notification, which we consider appropriate. It would be concerning if the Reserve Bank might consider taking action in relation to cloud service providers, as outsourcing is a common function and appropriately used, provides benefits of economy of scale and cyber security specialization, particularly if the organisation in question is small. In this regard, we question what the Reserve Bank would propose to do if an entity notified them, and the Bank had concerns about the chosen cloud service provider.

Annexes

Glossary

- ICNZ is part of the Global Federation of Insurance Associations (GFIA), a non-profit association representing 41 representative bodies like ICNZ from all corners of the world. Through its GFIA membership, ICNZ is a part of the Cyber Risks Working Group, which had the opportunity to contribute to the FSB's consultation on the Cyber Lexicon in 2018. While generally supportive of the Lexicon, the GFIA submission stressed that "forced terminology for this nascent industry could prevent innovative product development that will naturally converge with changing cyber risks". In addition to this comment and noting the speed with which terminology in the cyber risk area can develop, we question how often the RBNZ glossary will be updated. And whether it will only be updated to coincide with a review of the Cyber Lexicon. On this point, we note that the Cyber Lexicon has not been updated since its introduction in 2018 and does not include terms recommended by GFIA like 'CERT' and 'cyber warfare'. In order to be a meaningful and authoritative document, we believe that the Glossary will need to be updated regularly and would encourage the Reserve Bank not to be limited by alterations to the Cyber Lexicon, which are likely to be slow.

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

ICNZ believes that it is appropriate for the guidance to be at a high-level and principle-based, leaving the execution and implementation to the discretion of the particular financial institution. This will also ensure the guidance will remain flexible as technology changes. However, we also recommend that the Reserve Bank take a collaborative and supportive approach with entities when implementing the guidance to ensure that the requirements are kept practical and realistic.

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

The proportional and risk-based approach adopted in the guidance is appropriate given that cyber risk appetite and tolerance will differ amongst organisations. An entity's approach to the cyber resilience guidance should be able to align with organisational operational and enterprise risk management principles and practices.

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

ICNZ agrees that the guidance should apply to all regulated entities of the Reserve Bank and encourage the Bank, through its membership of the Council of Financial Regulators to advocate for the same guidance to be used by all regulators to ensure a coordinated approach and avoid the duplication we address elsewhere in this submission.

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

While ICNZ is open to the possibility of information gathering and sharing, it is difficult to support the idea without having more information available about what such a regime might specifically entail. It is unfortunate that the timelines for this consultation are such that a framework for information gathering and sharing will not be available until the middle of 2021. It would be helpful if the Reserve Bank could share any definitions or other detail to illustrate what information gathering and sharing would mean for financial institutions and to enable any concerns or barriers to compliance to be raised as soon as possible. For example, it would be useful to know whether there would be an obligation for financial institutions to participate in the information gathering and sharing, and whether there will be integration of such a shared resource for public sector bodies.

In considering information gathering and sharing (alongside coordinating with other public bodies), it is important that the goals and approach are carefully considered and specifically laid out with reference to how information is intended to be used and each regulator body's specific roles so as to avoid duplication. There is little value in data collection if it devolves to a pure information gathering activity - it needs to drive understanding of current cyber threats, background activity, and the effectiveness of approach and security measures. We therefore request further information from the Reserve Bank about how any provided information will be used, and what they will share with regulated entities in return.

As already stated, while still awaiting the specifics of any information gathering and sharing, we would be supportive of a collaborative approach with the Reserve Bank, the FMA, NCSC and CERT. It would however be helpful to have further detail on the roles of the NCSC and CERT in information gathering and sharing.

Given the recent cyberattack on the Accellion FTA platform, it is possible that there could be increased reluctance from entities to share data, and we reiterate the comments outlined in the Overarching Comments of this submission above encouraging the Reserve Bank to be transparent about its cyber security management, and what systems and processes will be in place to ensure the safe and secure storage of regulated entities' data.

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?

ICNZ supports the Reserve Bank's intentions in relation to cyber data collection and appreciates the intention in the consultation document for the Reserve Bank to work closely with other public bodies to maximise the value and to minimise the reporting burden on regulated entities in respect of cyber data collection. As already has been expressed several times in this submission, we consider it is important that the different regulators are coordinated in their oversight of cyber resilience including data collection. This is to avoid entities having to potentially prepare multiple responses with essentially the same or similar information to various regulators but in different formats or through different channels. For example, we see there is a potential overlap between Reserve Bank and the Financial Markets Authority (FMA) in the oversight of cyber resilience particularly with the FMA as the regulator of proposed conduct legislation (the Financial Markets (Conduct of Institutions) Amendment Bill currently before Parliament).

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'[3] report issued in July 2019, which sets out guidance and expectations; and
- the Standard Conditions for Financial Advice Provider licences[4] issued in November 2020 requires Financial Advice Providers to regularly identify and review critical technology risks and cyber threats and to notify FMA in the event of a material information security breach.

With more than one regulator for cyber resilience, we consider that 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 customers. As already pointed out, it is also possible that a cyber incident will result in the loss or potential loss of personal information which would also trigger reporting requirements under the Privacy Act 2020 to the Office of the Privacy Commissioner and any affected individual(s). Given the numerous entities and varying interests involved we would therefore be grateful for any areas where there can be simplification of reporting.

At the 9 December 2020 Reserve Bank Workshop on this consultation, a question was asked about how the Reserve Bank and the FMA would collaborate on reporting and information gathering to lessen the burden on dual-regulated entities which did not receive a particularly clear response. The FMA indicated that they are giving thought to matters like post-incident reporting so that regulated entities do not have to report twice to both the Reserve Bank and the FMA. However, it is important to note that duplication of reporting requirements is not just a 'post-incident' matter. For example, this is also an issue for any reporting that may be required at the time of an event. It is during this time, when entities are trying to focus their resources into dealing with a major incident, that having to provide duplicate reporting would be the most burdensome. This burden could be alleviated by only requiring reporting via one channel, an idea which was raised at the Workshop.

[3] https://www.fma.govt.nz/assets/Guidance/Cyber-resilience-in-FMA-regulated-financial-services.pdf
[4] https://www.fma.govt.nz/assets/Consultations/Standard-Conditions-for-full-FAP-licences.pdf

The reporting burden could also be eased by only requiring the notification of material incidents (perhaps leveraging an organisation's incident risk management priority matrices such as critical and high). We believe that only sharing information on material incidents would also ensure a more consistent approach to data collection and provide more meaningful data. This would also avoid the over-reporting of non-material events. However, what is considered a 'material incident' would need to be clearly defined.

Finally, we raise several questions relating to the intended operation of cyber data collection which would benefit from further clarity:

(1) If data is to be shared, what processes will be put in place when reported incidents contain sensitive information for a regulated entity? There will need to be sufficient safeguards in place to ensure entities feel comfortable with their obligations to report.
(2) Further information is needed about the potential format and prescription for reporting on cyber incidents. While entities will already hold data on past events and will continue to collect further information on cyber incidents, work may need to be done to be able to provide the information in any required format, which, depending on the amount of work, could potentially be costly. We would like to request that consultation with industry groups occur before any prescribed reporting formats are decided and again note the need for consistency of this with any reporting required by other regulators.
(3) Where a New Zealand-regulated entity has an international parent company, our view is that the obligation to report cyber incidents should only extend to cyber security incidents impacting the New Zealand-regulated entity. We consider that the guidance should be clear on this point.

Conclusion

Thank you again for the opportunity to submit on the consultation document. If you have any questions, please contact our Legal Counsel on [redacted].

Yours sincerely,

[redacted]

Tim Grafton
Chief Executive

Jane Brown
Legal Counsel