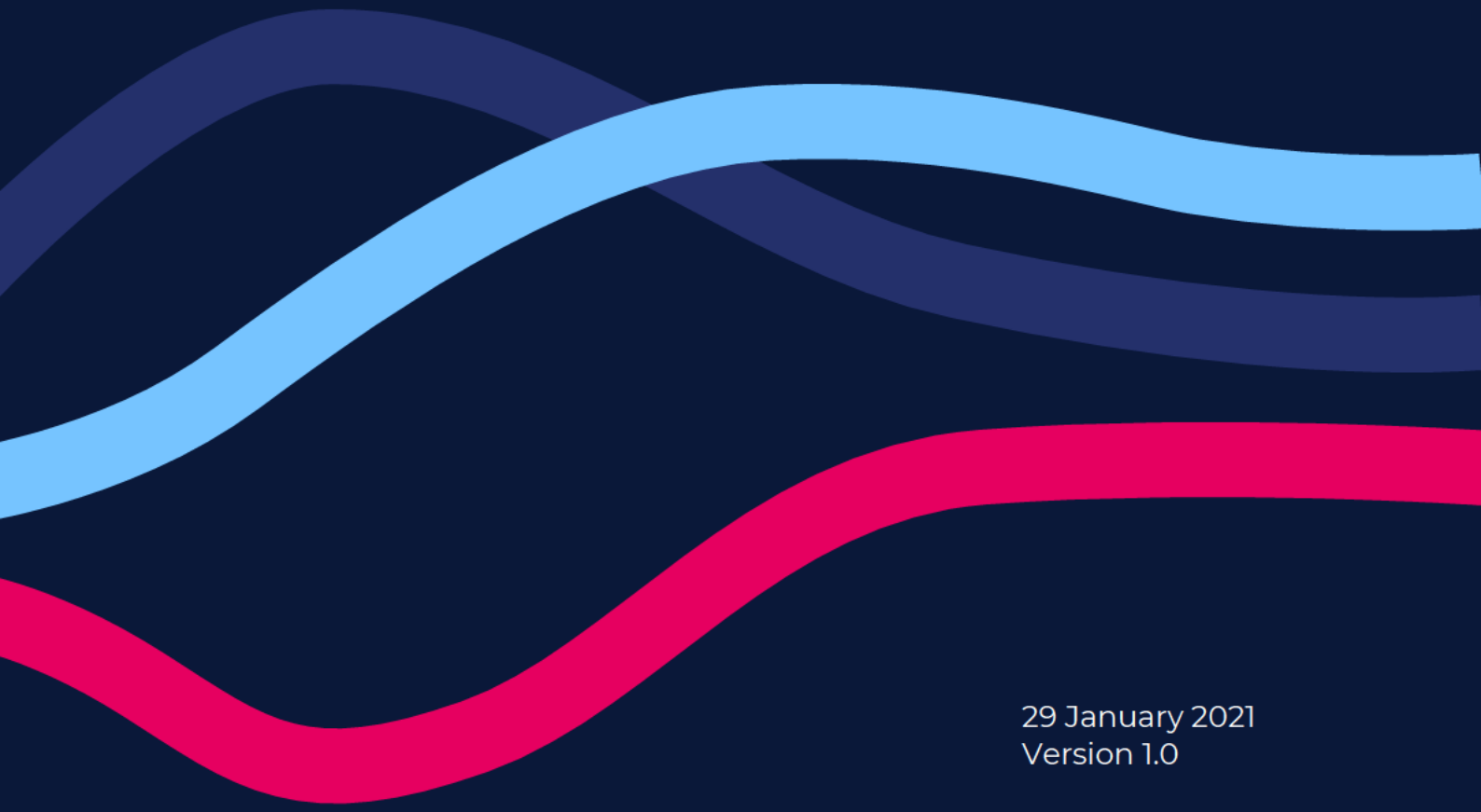
DATACOM

Reserve Bank NZ Cyber Resilience Consultation Paper Feedback



29 January 2021
Version 1.0

CONTENTS

Executive Summary

The Reserve Bank of New Zealand (RBNZ) is looking to become more proactive in promoting cyber resilience in New Zealand's financial sector. This initiative has resulted from the increasing number and severity of cybersecurity threats to our financial sector and from RBNZ wishing to fulfil its values of Innovation in this area by actively improving what they do.

The core element of RBNZ's approach is the development of cyber risk management guidance for all its regulated entities. The Reserve Bank cyber resilience framework includes two elements that build on the risk management guidance: First, information gathering and sharing, and secondly, enhanced incident response coordination, with a key overarching objective of raising awareness on building resilience and setting appropriate expectations for the industry.

RBNZ has highlighted important pillars for building a strong cyber resilience framework within an organisation, but opportunities exist for RBNZ to take further steps to help organisations execute on the existing guidance. For example, RBNZ has accurately captured that "good governance is the foundation effective Risk Management" but has not explained in enough detail how good governance can be achieved and how governance has links in every part of the organisation.

The additional elements (information gathering and enhanced incident response coordination) are both valid and the Datacom Cybersecurity Advisory Practice supports these initiatives, however, it would be advantageous to make the intent and outcomes of these activities clear and making these a requirement will enable RBNZ to get better results from its regulated entities.

In summary, reviewing the consultation paper and understanding that the "objective of the Reserve Bank's programme of work on cyber risk is to raise awareness on how to build resilience and set appropriate expectations on the industry", the realisation that occurs is that guidance is not enough to increase the cyber resilience of the financial sector, and therefore, does not meet RBNZ's objectives. RBNZ is looking to "set expectations", however, this does not enforce change. Instead, proposing requirements (with clear and detailed guidelines) that dictate and drive the minimum expected practice for cybersecurity of the regulated entities drives a more successful outcome for RBNZ and the wider financial sector.

Should RBNZ choose to remain with providing guidance (not mandating any requirements), it is important to acknowledge that the existing guidance is a set of high-level principles and may be insufficient in meeting the set objective. Therefore, there is a need to go one step further and provide information that is easy to

understand, and which will help organisations make the necessary changes to increase their cyber resilience.

Appendix

Questions and Answers

1. **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?**

Datacom Cybersecurity Advisory Practice agrees that RBNZ's current approach is best described as "moderate activity" however, we believe there is a need to increase activity to higher levels commensurate with the increased number of threats facing the financial sector in New Zealand.

Given the broad exposure Datacom has in the New Zealand cybersecurity market, there is a clear need to increase cyber resilience, and this can better be achieved by RBNZ mandating what is expected of the financial sector. Should RBNZ choose to take the path of having legally binding requirements, the guidance document will need to be amended to ensure that the document can be easily interpreted to allow the successful implementation of the controls.

As directors and senior management are the target audience for the risk management guidance, additional detail to the guidance document is required to better support the financial sector and achieve better outcomes in New Zealand's cyber resilience. Clauses in the guidance document are unclear at times, which can lead to organisations not meeting the intent of the clause.

A specific example related to A2. Cyber Resilience Strategy and Framework – "The cyber resilience strategy should outline - The entity's stakeholders' high-level requirements." Organisation's lacking in cybersecurity expertise would struggle to interpret the meaning of "requirements" (Confidentiality, Integrity, Availability), what a stakeholder means in a security context, how to identify these stakeholders, what they are to subsequently do with these requirements, and more specifically how these stakeholders and requirements relate to the rest of the guidance provided.

2. 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?

Datacom Cybersecurity Advisory Practice supports the use of international practices for reference, but it would be beneficial to include mappings back to international standards reference. For example, B2.3.1 maps to NIST CSF ID.RA-1 and PR.IP-12. This allows organisations to leverage the work they have done to comply with other standards and reduce wasted effort in identifying gaps, therefore, encouraging the use of the guidance document.

As for specific feedback on the guidance, please note the following:

1. It would be advantageous to elaborate more on how good governance allows for better risk management (the consultation paper briefly mentions this, but the guidance document does not cover this in the same way; it speaks about information dissemination specifically). Datacom's experience in the governance space shows that many organisations do not understand the need for governance nor understand how to implement governance across the organisation. Therefore, elaborating further on governance benefits and advantages would be beneficial.

2. There is no link between the Security Governance section and the three other sections (Capability Building, Information Sharing, Third Party management). Governance is required across all areas, but as described will likely result in activities taking place in isolation and providing little value - an exercise in 'tick-boxing' rather than meeting the RBNZ's goals around increasing cyber resilience and the associated public good.

3. The terms Strategy, Framework, and Implementation Plan are terms used interchangeably in various contexts; they need to be clearly defined.

4. The 'Mission' (i.e. Goals) should be setting the strategy, however, the guidance document specifies setting the Mission within the strategy.

5. NIST CSF is identified as the basis for capability building without further comment, but the 'Identify' component of NIST CSF is governance, and as such there is an overlap.

6. Boards and senior management are not a given in smaller organisations, therefore, the language should be made more generic and thus widely applicable.

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

Datacom Cybersecurity Advisory Practice agrees that high-level principles should be used to set the direction for the intent of cybersecurity, however, when the intent is to provide clear guidance, high-level principles are insufficient. The guidance document needs to be supplemented with material that provides detail sufficient to allow financial institutions to implement the guidance without requiring extensive external consulting .

4. What is your view on the principle of proportionality and a risk-based approach adopted by the Guidance?

Datacom Cybersecurity Advisory Practice agrees with the principle, however, greater (more detailed) guidance may be required for the organisations to fully understand how it can be achieved. The guidance is unclear on how risk is related to, or driving capability building and as such the principle is unlikely to achieve the intended outcome.

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

Datacom Cybersecurity Advisory Practice supports the guidance being applied to all regulated entities.

If RBNZ wishes to proceed with making this more of a mandate than guidance, alignment with the FMA will provide a more effective outcome for entities where mandatory requirements cannot be enforced by RBNZ (but can be enforced by the FMA).

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

Datacom Cybersecurity Advisory Practice supports the collaborative and coordinated approach. Collaboration and release of lessons learnt enables organisations to adapt to the ever-changing threat landscape.
For example, the NZX de-brief in the NZITF forum allowed organisations to understand the extent of the cyber attack they faced and the necessary steps taken to restore operations.

7. 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?

Datacom Cybersecurity Advisory Practice supports the data collection described, as it would require the regulated entity to prove their cyber resilience, which can be a driver for the organisation to continually improve their cybersecurity posture. Datacom Cybersecurity Advisory supports making the data collection a (mandatory) requirement as well as breach notifications.

The concern with the data collection is that it is not clear what the intent and outcomes are, elaborating on this would help organisations understand the benefits and would enable RBNZ to achieve greater compliance.

General Comments

Covered in the Executive Summary section.