Reserve Bank of New Zealand
Te Pūtea Matua

18 November 2022

Christian Hawkesby
Deputy Governor/ General Manager Financial Stability
Reserve Bank of New Zealand
PO Box 2498
2 The Terrace
Wellington 6140

Paul Gregory
Acting Director of Capital Markets
Financial Markets Authority
PO Box 1179
1 Grey Street
Wellington 6140

By email: Phoebe.Chan@rbnz.govt.nz and Jenny.Eves@fma.govt.nz

Dear Christian and Paul,

Re: FMI Standards exposure draft published for consultation

Thank you for meeting with us on the 3rd of November to discuss the draft standards for the Financial Markets Infrastructure Act. We appreciated the opportunity to ask questions, seek clarification, and convey to you areas where we thought close attention was warranted during this consultation period. Further to the meeting, this note now summarises our thoughts and queries on the draft standards, categorised under General, Practical Implementation, and Specific Observations on Certain Standards:

General:

Overall we acknowledge and support the underlying basis for the formulation of the Standards, being foundationally built from the CPSS and IOSCO principles with an overlay specific to key areas that you consider high focus for FMI Operators in New Zealand. In this regard we acknowledge the importance of risk management, particularly operational risk, cybersecurity, critical service providers, and the need for robust contingency arrangements. These themes have been highlighted to us during 2022 so are consistent with our general expectations.

In a number of these areas there is specific reference to the need for independent external assurance activities to be undertaken by the operator on a periodic basis, or in the case of a material event. We noted a desire to understand the nature of assurance that is expected, and the trigger points / materiality thresholds for events that may require such an assessment. Our desire is to ensure we meet the broad expectations of the Regulator insofar as these engagements are concerned (for example, type of assurance, type of assurance provider, materiality and therefore likely volume of these assessments), and to signal that each individual assurance engagement will involve very careful planning, require considerable thought, and incur material cost that we will, under our financial frameworks, pass back to our NZClear and ESAS users. We understand from your feedback that independent assurance functions within an Institution (such as Internal Audit) will not been appropriate for these assessments. We seek clarity on the definition of materiality for these events and therefore the requirements for any necessary assurance reviews.

Practical Implementation:

We also discussed the effective date for full compliance with the Standards. Our understanding is that November 2023 is the likely effective date for all standards. We ask that this be carefully considered by the Regulators given the various independent assessments that need to be initiated, and that some of the activities require comprehensive consideration to ensure current critical service provider oversight, contingency planning, and framework articulation which aligns to Regulator expectations.

You conveyed to us that there would be an information request at the time of the tentative November effective date and we would appreciate some greater insight into the nature and general intent of this request.

Specific Observations on Certain Standards:

For cybersecurity we already baseline against New Zealand Government standards (NZISM) and also ISO (27001) and SWIFT CSP and complete independently review assessments for the latter. We seek any further insight that you can provide in regard to how we may leverage this work as we seek to meet the requirements of completing independent assessments of our cybersecurity frameworks. Our aim is to align to your underlying expectations whilst minimising duplication of the various assurance and validation processes already in place over our cybersecurity risk management environment.

For risk management in general we noted a need for an annual independent assurance of risk management, along with a two yearly assessment of operational risk, along with the cybersecurity annual assessment. We would request that you consider the cadence and intersections of commonality of these multiple assessments and provide any further guidance around your expectations.

We noted that Critical Service Providers differ in nature from major national and international providers (SWIFT and Telecommunication providers) to specific solutions providers (Datacom and NEXI) and would appreciate any further insight into expectation around the extent of examination anticipated as we seek assurances and corporate level information from these providers, and potentially second tier contracts that appear to meet your definitions of a critical services provider.

As noted during our meeting we are highly focused on identifying any additional actions, processes and frameworks that we need to progress between now and the effective date for these Standards, and the abovementioned points should be interpreted in this context. We look forward to working with yourselves to ensure a successful rollout of the Standards and ensuing engagement between the Regulator and Operator of ESAS and NZClear.

I am happy to discuss any of the points noted above.

Yours sincerely

Steve Gordon
Director of Payment Services

cc:
Jaimee Taylor- Burt, Manager Payment & Settlement Services, Jaimee.Taylor-Burt@rbnz.govt.nz
Ozge Ozbilgin, Compliance & Legal Analyst Payment Services, Ozge.Ozbilgin@rbnz.govt.nz