EL&C Baillieu
1889 ONWARD

E.L. & C. Baillieu Limited
ABN 74 006 519 393
AFSL No. 245421

Participant of ASX Group
Participant of Chi-X Australia
Participant of NSX Ltd

9 August 2019

Andrew McPherson
Senior Specialist
Market Infrastructure
Australian Securities and Investments Commission
Level 5, 100 Market Street
Sydney NSW 2000

By email to: rules.resilience@asic.gov.au

Dear Andrew,

Consultation Paper 314: Market integrity rules for technological and operational resilience

We refer to the ASIC Consultation Paper 314 issued on 27 June 2019 (**CP314**) which proposes amendments to Chapter 8 of the *ASIC Market Integrity Rules (Securities Markets) 2017* (**ASIC MIRs**) relating to Critical Systems and Business Continuity Plans for Market Operators and Market Participants. We thank you for the opportunity to provide you with our comments in respect of CP314.

General comments

We note that the amendments to the ASIC MIRs are to address 5 key areas:

1. Resilience of critical systems
2. Outsourcing arrangements
3. Data and cyber risk
4. Incident management and business continuity
5. Notification requirements.

CP314 details some of the issues that ASIC wishes to address, including the importance of having "more specific expectations" for Market Operators and Market Participants. However, it is difficult to provide feedback on some of the specific provisions due to the lack of certainty around the various definitions. An example is that a "Critical System" is taken to include "functions, infrastructure, processes or systems" which, if failed, would (or would likely) cause "significant disruption" to operations or "materially impact" services. The note to the definition includes references to infrastructure, processes and systems that deliver or support trade acceptance, order entry and routing, client money systems, trust accounts, settlement systems and so on. It is open for interpretation as to what is expected. There are many terms that are similarly vague or which are so broad that it makes it difficult to understand what is actually required, or to anticipate the time that will be required to implement the required changes.

EL&C Baillieu
1889 ONWARD

Outsourcing arrangements

A particular concern relates to the requirements around outsourcing of Critical Systems. As Market Participants, we are heavily reliant on key providers in providing trading infrastructure and market services to us. We have existing contractual arrangements with those vendors. The updated ASIC MIRs will require us to try and renegotiate on terms with these vendors to ensure that our existing arrangements meet the new requirements. Every outsourced arrangement will need to be assessed to determine whether it relates to a Critical System and then what is required to meet the contractual obligations set out in the ASIC MIRs relating to Outsourcing Arrangements. Examples include order and trading systems, 3rd party hosting of infrastructure, client accounting systems, email or other delivery systems (such as those used to deliver trade confirmations to clients) and other service providers of Critical Systems.

The provisions relating to external audit and approval of sub-contracting arrangements pose additional issues in negotiating terms with vendors. It is likely that any such renegotiation of terms will incur additional cost; however, these potential costs are currently unknown given the uncertainty noted.

There should be a requirement for major vendors of market and infrastructure services such as IRESS, GBST, share registries and the like to be captured in these frameworks, and to be required to go through certification of systems (much like what happens, for example, with CHESS releases), and to have minimum terms that are in line with ASIC's expectations. Whilst we understand that these vendors are not generally regulated entities, we would anticipate that our key vendors would be reluctant to renegotiate terms that create additional burdens for them, unless they are compelled to do so.

The requirements for change management around critical systems (including implementation of new Critical Systems) and to notify "persons that may be materially impacted" by any such implementation also have unknown business impacts. An example could be that a major release / change implementation by a vendor would need to be notified to affected persons by all Market Participants (an example could be CHESS upgrade). There would need to be a mechanism to notify all relevant parties as required by the proposed changes to the ASIC MIRs. The time for reporting is unclear, and the content requirements of the notice are not specified. Further, the purpose for these notifications is not clear, and given the additional burden on business, there should be a clear understanding of why such notifications are required and how they will be managed. This also raises the issue of potentially having to make multiple notifications (for example, if a participant is also APRA regulated per CPS 231).

Data and cyber risk

The requirements for the backup of data and timely recovery are again vague. Does this require primary and secondary sites (and the significant costs of same)? Without certainty around these requirements it is difficult to estimate the impact from both a time to implement and a cost perspective.

Incident management and business continuity

The proposed ASIC MIRs relating to incident management and business continuity raise a number of issues.

The difference between an "**Incident**" and a "**Major Event**" is a matter of degree, and the notes to the proposed requirements state that "An incident may, depending on its severity, constitute a Major Event".

We repeat our comments above regarding the notification requirements, in relation to Incidents and Major Events to "persons that may be impacted", including the uncertainty of these obligations or the required method of notification. Identification of persons that may be impacted will vary depending on the type of "Incident" or "Major Event", which will introduce an additional burden to keep people informed while potentially managing a significant matter. The requirement to notify ASIC "immediately" upon become aware of a Major Event will have similar consequences.

We note that the requirement for Market Operators to move to quarterly testing of their Business Continuity Plans is not clearly explained. It adds burden not just to Market Operators but also to vendors and Market Participants as it will affect the provision of services and introduces risk to the market.

EL&C Baillieu
1889 ONWARD

Summary

We acknowledge ASIC's concern to have more certainty around the requirements for Market Operators and Market Participants with respect to technological and operational resilience, given the heavily reliance we have on technology to carry out our services and to perform our various obligations.

There is, however, considerable uncertainty in the proposed ASIC MIRs as drafted, including uncertain obligations on Market Operators and Market Participants. This makes it difficult for us to estimate how much time it will take for us to implement the required changes, and the resultant costs. We repeat that there should be a requirement for major vendors of market and infrastructure services such as IRESS, GBST, share registries and the like to be captured in reporting frameworks, and to be required to go through certification of systems and to provide contractual terms that capture the requirements of the proposed ASIC MIRs.

We would welcome the opportunity to further discuss these matters with ASIC.

Regards,

Gavin Powell
Managing Director