Results of Consultation on Guidance Note changes for ASX Clear, ASX Settlement, ASX Clear (Futures) and Austraclear participants

Proposed changes to Guidance Note 1 *Admission as a Participant*, and Guidance Note 10 *Business Continuity and Disaster Recovery* relating to business continuity and cyber resilience

05 August 2019

Contacts

For general enquiries, please contact:

Lyn Allsop-Guest
Manager, Review and Investigations
E participants.compliance@asx.com.au

Contents

Consultation process

On 8 March 2019 ASX released a Consultation Paper seeking comment from stakeholders on proposed changes to ASX's guidance to clearing and settlement participants on their business continuity, disaster recovery and cyber resilience arrangements in Guidance Notes 1 and 10.

The proposed changes to Guidance Note 1 are relevant to participants in ASX Clear, ASX Clear (Futures) and ASX Settlement (other than specialist settlement participants). The proposed changes to Guidance Note 10 are relevant to participants in ASX Clear, ASX Clear (Futures), ASX Settlement (other than specialist settlement participants) and Austraclear (other than collateral manager special purpose participants, foreign currency settlement bank participants and special purpose participants permissioned for cash only transactions).

ASX received two written submissions in response to the Consultation Paper, one of which was designated "confidential". The non-confidential submission is available on the 'Public Consultations' page of the ASX website http://www.asx.com.au/regulation/public-consultations.htm next to the entry for 05/08/19. ASX also received oral feedback from some participants.

ASX wishes to thank the respondents who took the time and trouble to share their views during the consultation process.

ASX proposes to make the changes set out in the Consultation Paper but with the amendments outlined below. A copy of the final consolidated Guidance Note amendments is available on the 'Public Consultations' page of the ASX website http://www.asx.com.au/regulation/public-consultations.htm next to the entry for 05/08/19.The changes will become effective on Monday 5th August 2019.

Consultation feedback and ASX responses

Guidance Note 1

The respondents were supportive of the proposed changes to Guidance Note 1, which clarify the types of risk that ASX expects a participant's risk management framework to address and, in particular, to specifically reference cyber risk. ASX is therefore proceeding with the proposed changes to Guidance Note 1.

Existing participants will have 6 months following the date of publication of the revised Guidance Note to comply with the changes. At the end of that period, ASX will be requesting each existing participant to confirm that it has updated its risk management framework to conform to the revised Guidance Note 1 and to specify the cyber resilience standard(s) it has considered as part of its risk management framework. ASX may also ask participants to provide evidence that they have done an assessment of their framework against the relevant standard(s).

All new applicants for admission as participants will need to comply with revised Guidance Note 1 as a condition of being admitted as a participant.

Guidance Note 10

The respondents were supportive of ASX's work in enhancing Guidance Note 10 to reflect current regulatory and market expectations. In particular, the respondents were supportive of the proposed changes in relation to "Proper records", "Incident management records", "Independent review", "Connectivity requirements" and "Other minor enhancements".

The respondents provided feedback on the following four areas in Guidance Note 10:

System resilience

The respondents supported ASX's proposal not to impose prescriptive requirements on how participants should manage cyber risk and instead require participants to align their cyber resilience arrangements to one or more of the latest global or national cyber standards and guidance.

ASX has made an amendment to this section of Guidance Note 10 to state that ASX may, from time to time, determine specific technical requirements for participants to maintain adequate security and technical arrangements within the clearing and settlement facilities.

Core personnel

One respondent suggested ASX should allow business continuity and disaster recovery responsibilities to be allocated to multiple personnel instead of assigning the accountability to one nominated business continuity officer ("nominated officer"), as was originally proposed.

ASX understands that the nature and scale of a participant's operations will affect its business continuity and disaster recovery arrangements, and that it may have a number of personnel responsible for BCP and disaster recovery. However, in view of the heightened standards of accountability expected of senior executives in the financial services industry, ASX expects ultimate accountability to remain with a senior member of the participant's management team.

ASX is therefore proceeding with the requirement that a participant allocates overall responsibility for business continuity and disaster recovery to a nominated officer. Participants will have a 6 months' transition period after the publication of Guidance Note 10 to notify ASX of their nominated officer. Thereafter, they will be required to notify ASX of the appointment and any subsequent departure of the nominated officer within 10 business days.

ASX also acknowledges that the nominated officer may want to appoint a contact person who will act as ASX's first point of contact for discussions related to the participant's business continuity and disaster recovery arrangements and any disruptions that may occur, and has reflected this in Guidance Note 10.

Recovery time objective (RTO)

The consultation proposed that a participant's business continuity plan (BCP) should specify the following target RTOs after the initiation of its BCP:

- for a tier 1 participant,[1] 2 hours for critical ASX operations and 4 hours for resumption of business-as-usual ASX operations; and
- for a tier 2 participant,[2] 4 hours for critical ASX operations and 6 hours for resumption of business-as-usual ASX operations.[3]

The respondents commented that an RTO of 2 hours would be challenging for participants with complex businesses and systems.

In relation to incidents involving site failures, the respondents also asked ASX to consider aligning the RTO requirements with the RBA's Standards[4] for Compliance Level 1 RITS Members to reduce regulatory burden and harmonise obligations across regulatory frameworks.

Having regard to the feedback, ASX has determined that it will take a 3 stage approach to implementing the target RTOs, as set out in the table below. Stage 2 will align ASX's target RTOs with the RBA's Standards for incidents involving a site failure for 18 months. Thereafter, participants will be expected to move to the target RTOs mentioned above.

---

[1] Refer to existing Guidance Note 10, 'Participant tiering' for guidance on how ASX classifies tier 1 and tier 2 participants.
[2] Ibid.
[3] ASX acknowledges that in some cyber-related incidents there may be exceptions to these RTOs, for example, where moving to an alternate site may risk propagating the cyber incident further into the network. However, in these cases, participants should design their BCP to enable safe resumption and completion of critical ASX Clear operations as close to the applicable RTO as possible.
[4] The RBA's *Business Continuity Standards for RITS Members* apply only to RITS Members that operate an Exchange Settlement Account or are a batch administrator.

	Stage 1 To be completed by 1st February 2020	Stage 2 To be completed by 1st February 2021	Stage 3 - Final state To be completed by 1st August 2022
Tier 1	ASX expects participants to carry out a gap analysis within **6 months** of the date of publication of the revised Guidance Notes, and to prepare a plan to meet the required RTO of Stage 2 and 3 accordingly.	Within 12 months of the completion of Stage 1 a participant's business continuity and disaster arrangements must comply with a **2 hour RTO for all incidents excluding a site failure.** **A site failure is to comply with a 4 hour RTO target,** this is aligned with RITS obligations for Compliance Level 1 members.	Within 18 months of the implementation of Stage 2 a participant's business continuity and disaster arrangements must comply with an **RTO of 2 hours for all incidents, including a site failure.**
Tier 2	ASX expects participants to carry out a gap analysis within **6 months** of the date of publication of the revised Guidance Notes, and to prepare a plan to meet the required RTO of Stage 2 and 3 accordingly.	Within 12 months of the completion of Stage 1 a participant's business continuity and disaster recovery arrangements must comply with a **4 hour RTO for all incidents excluding a site failure.** **A site failure is to comply with a 6 hour RTO target**, this is aligned with RITS obligations for Compliance Level 2 members.	Within 18 months of the implementation of Stage 2 a participant's business continuity and disaster recovery arrangements must comply with an **RTO of 4 hours for all incidents, including a site failure.**

The respondents agreed that the RTO target period should commence when a participant initiates its business continuity and disaster recovery plan, but requested further clarification on when ASX would regard this as occurring.

ASX notes that the current version of Guidance Note 10 states that:

- the RTO commences "following the initiation of [the] BCP"; and
- "participants should aim to make a decision on whether or not to initiate their BCP as quickly as they reasonably can following a disruption so that it does not significantly extend the time during which their ASX Clear operations are down."

Hence the RTO commences when a participant makes a determination that recovery is required. ASX is satisfied that the existing guidance provides sufficient clarity as to the commencement of the target RTO period.

Change management

A respondent questioned ASX's expectations regarding testing of changes by vendors and service providers. ASX confirms that a participant is expected to test only those changes initiated by vendors or service providers that may impact on the participant's ASX clearing and settlement operations. Changes that are not reasonably expected to impact the participant's ASX clearing and settlement operations need not be tested.

Self-assessment form

To assist participants to review their compliance with Guidance Note 10 and, in particular, the periodic assessment obligation, ASX will create a self-assessment form which participants can use for these purposes. The self-assessment form will be made available to participants following the publication of the Guidance Note.

Transition

For existing participants, the proposed reduction in the recovery time objective (RTO) in Guidance Note 10 set out above will be phased in over a 3 year period.

Existing participants will have 6 months from the date of publication of the revised Guidance Note 10 to comply with all of the other changes in Guidance Note 10. At the end of that period, ASX will be requesting each existing participant to confirm that it has aligned its arrangements to conform to the revised Guidance Note 10. ASX may also ask participants to provide evidence that they are in compliance with the Guidance Note.

All new applicants for admission as participants will be expected to comply fully with revised Guidance Note 10, including the proposed reduction in RTO, as a condition of being admitted as a participant.