6 May 2019

Ms Lyn Allsop-Guest
ASX Limited
PO Box H224
Australia Square NSW 1215

By email: participants.compliance@asx.com.au

Dear Ms Allsop-Guest

Proposed changes to Guidance Note 1 and Guidance Note 10 relating to business continuity and cyber resilience

AFMA welcomes the opportunity to provide comment on ASX's consultation paper in relation to guidance changes for clearing and settlement members relating to business continuity and cyber resilience.

AFMA membership includes a number of clearing and settlement participants of ASX clearing and settlement businesses.

The review of guidance in these areas is timely. Information security is an increasing focus for the industry and the government with July 2019 seeing the commencement of APRA's new prudential information security standard. Similarly following the RITS outage last year and its flow-on effects for clearing and settlement the industry has been engaged on issues around resilience.

AFMA has considered the proposed changes through its Markets IT and Information Security Committees. This response is informed by those considerations.

1. Amendments to Guidance Note 1

AFMA supports the minor change proposed to Guidance Note 1 as appropriate and helpful.

2. Amendments to Guidance Note 10

AFMA raises no objections to the proposals in relation to "proper records", incident management records, the proposals around independent review, connectivity requirements, or the "other minor enhancements".

2.1. Core personnel

Australian Financial Markets Association
ABN 69 793 968 987
Level 25, Angel Place, 123 Pitt Street GPO Box 3655 Sydney NSW 2001
Tel: +612 9776 7993 Email: djeffree@afma.com.au

On the recommendation around core personnel, we note that some members have business models which spread the Business Continuity Plan (BCP)/ Disaster Recovery (DR) responsibilities across a number of roles, and as such may need to nominate a number of personnel depending on the market involved. Others may use an operational contact or contacts within a business resilience team which would then direct any enquiry from ASX to the relevant parties. This may involve the use of a distribution list or registering a role on the ASX Online system with relevant contact details.

2.2. Recovery Time Objective

A 2 hour RTO for critical ASX clearing and settlement operations can pose a challenge to participants with complex businesses and systems, who may operate in multiple markets.

Members note the RBA's requirements in relation to RITS payments, for Compliance Level 1 Members the RBA allows a 4 hour RTO for site failures.

Participants have stated that, consistent with the RITS requirements, and experience within the markets, for serious outages that involve complex systems or that require fail-over to a DR site, 2 hours for resumption of clearing and settlement operations is likely to be unrealistic and 4 hours is a more realistic timeframe.

A 2 hour RTO might only be appropriate for relatively simple outages such as a communications failure, or a relatively simple system problem. AFMA supports ASX working with industry to define the types of outages that might be responded to within this timeframe.

A four hour timeframe is appropriate for more significant outages given the need for:

- crisis management teams to meet and decide on actions within an incident management framework;
- the coordination with offshore teams;
- the coordination with potentially multiple vendors; and
- to allow for travel to back up sites.

Back up sites are often placed some distance from the primary site to decrease the likelihood they will be impacted by the same factors (e.g. power, telecoms and access). Travel times alone can take one hour or more depending on the distance to the site and it should not be assumed these can be operated remotely from the primary site. It would not be beneficial to create incentives for locating back up sites closer to primary sites.

It is also important to note that BCP is an objective. It is not necessarily an outcome in a real-life scenario. Participant systems should be determined to meet this objective if they can do so in a controlled test environment. It should be recognised, as all significant entities have experienced at one time or another, that real-life scenarios can introduce contingencies and complexities that are difficult to fully plan for, and which can slow system restart. AFMA supports ASX's recognition that some cyber incidents will be exceptions to these RTOs and that firms should design their systems to be as close to the relevant RTOs as possible.

AFMA also supports the use of the terminology “operations” in the rules as the target for restoration as this can potentially be achieved by different “systems”.

2.3. Commencement of timing

The proposed rule change state that the timing applies from the initiating of a participant’s BCP.

AFMA supports the timing commencing from the time the firm recognizes there is something to recover and that it cannot operate. This lies in important distinction to the time an incident has commenced.

It would be helpful if this timing commencement distinction could be made clearer in the rules. The timing should commence only once the participant has reached a firm conclusion that there is a problem that prevents normal operation.

2.4. Implementation timing

In the event that ASX proceeds with the proposed guidance where participants currently have RTOs greater than 2 hours AFMA believes that 18 months should be the minimum time period to allow participants to move to a 2 hour RTO with confidence that a 2 hour RTO might be achieved in a real crisis. Participants indicate that given current resourcing loads some flexibility in the timing may be necessary.

2.5. System resilience

AFMA supports ASX approach of not imposing prescriptive standards on firms in relation to cyber resilience and instead to require participants to align their cyber resilience arrangements to one or more of the latest global or national cyber standards and guidance. Firms adopt a variety of standards in relation to cyber resilience, often determined by the country in which their headquarters are based. These standards aim for similar ends albeit with some differences in approach.

Locally there are regulatory developments in relation to cyber standards being prescribed by APRA in CPS 234 that commences 1 July 2019, and for participants in Open Banking a new hybrid standard proposed by the ACCC in the Consumer Data Right rules. AFMA is working to minimise the number of competing regulatory standards, and has been supportive of the development of CPS 234.

AFMA supports ASX maintaining flexibility as a means to limit overlapping and potentially incompatible requirements.

The avoidance of duplication and inconsistency is an avoided cost and allows for gains for many firms in efficiency and managed risk through the better deployment of available resources.

2.6. Change management

AFMA supports the proposed approach to change management as consistent with prevailing good practice standards and appropriate for participants of ASX clearing and settlement services.

Suitable engagement with vendors and service providers on changes that might affect a participant's clearing and settlement operations is appropriate. We do note and seek clarification that it is not appropriate to test all vendor and service provider changes as some of these changes should not reasonably be expected to have the potential impact participant operations or to be testable with the participant systems. For example, a vendor may upgrade a storage device connected to their system that is not visible to participant systems and can be appropriately tested by the vendor without involvement of the participant.

2.7. Business Continuity Plan

As possible causes of disruption are numerous and varied, we would like to propose a more holistic, simplified and flexible "All Hazards" approach for which the broad disruption groups are (1) loss of staff, (2) loss of site, (3) loss of technology, (4) loss of third party (or a combination thereof), be an acceptable alternative to the specific listing of the 10 minimum disruption scenarios under the Business Continuity Plan section of the Guidance Notes. Whilst the listing is helpful, each Participant needs to have regard to their unique disruption scenarios, having regard to the scale and complexity of their operations.

2.8. Other

AFMA also requests clarification in relation to the notification requirements rules regarding which channels of communication are preferred by ASX.

Participants accept that the proposed transition arrangements are sufficient for participants to align their current business continuity arrangements with the updated guidance in Guidance Note 10.

Conclusion

AFMA supports ASX's work in reviewing Guidance Notes 1 and 10 to update them for the evolving needs around cyber security and resilience.

We note the appropriateness of closer alignment of the RTOs with those required by the RBA for RITS, particularly where DR plans are to be invoked and fail-over is required.

Thank you for the opportunity to comment on the matters raised in the Consultation.

Please contact me either on 02 9776 7993 or by email at djeffree@afma.com.au if further clarification or elaboration is desired.

Yours sincerely

Damian Jeffree
Director of Policy