16 August 2019

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

Email: rules.resilience@asic.gov.au

Dear Mr McPherson

Consultation Paper 314: Market Integrity Rules for Technological and Operational Resilience

The Australian Financial Markets Association (AFMA) welcomes the opportunity to comment on *Consultation Paper CP 314 Market Integrity Rules for Technological and Operational Resilience* (the Consultation/the Consultation Paper). AFMA has long been an active participant in the development of technological and operational aspects of the financial markets and over the course of 2018/9 has established additional analytical capacity in the area of information security.

AFMA is supportive of a number of the initiatives in the Consultation Paper and more generally of ASIC's work in relation to information security and system-wide resilience. We do have some concerns in relation to the very wide scope of matters considered by the consultation and the current uniformity in the type of response proposed. We suggest a narrowing of scope and that a wider range of risk-appropriate responses may be in order.

With the breadth and depth of matters to consider in forming final proposals we would encourage ASIC to consider an ongoing engagement with the broader industry, perhaps through an industry working group, to explore the form and detail of ways forward.

At a high level we suggest careful consideration of what should constitute a regulatory driver, particularly where there is a clash between standards issued by IOSCO and the approach to regulation determined by the Australian Government.

More generally we suggest ASIC consider the opportunity presented by the Consultation to better define the proper motivations and role for regulation in a market-based economy. The role of the

regulator is to define boundaries and regulatory outcomes not the technical means to achieve an outcome. With very quickly developing technology, Australian technology regulation has demonstrated a constant failure to anticipate change and failed to serve community needs. Considering these matters may suggest limits to the role for regulation in business operations. Particularly where there is a reasonable basis to expect market forces will address any shortcomings over time, and the impacts of any shortcomings would not be systemically significant.

In this submission we also argue that the regulatory stance and drafting in relation to operational and technological matters should be adjusted to accommodate unavoidable failures to achieve perfection. These are generally highly complex systems and it should not be an offence merely because there is an issue with a system.

We also raise a number of more specific concerns as part of our response to the questions in the Consultation Paper.

We note our interest in ASIC commencing consultations at the issues phase rather than when draft rules and regulations have already been formed. Consultation processes that leave external engagement to consider a fully formed draft may have missed opportunities to avoid further regulation, or to approach the regulation in a different manner.

Increasing the early, active and empowered participation in the regulatory process by the regulated community and broader public is likely to be associated with more democratic and supported[1], and in our view more likely to be of net benefit to the Australian economy.

We thank ASIC for the ongoing material engagement and efforts around resilience and look forward to continuing to assist in finding the optimum balance in regulatory outcomes.

For more information or if you have questions in relation to our submission please do not hesitate to contact me at [redacted] or 02 9776 7993.

Yours sincerely

Damian Jeffree
Director of Policy and Professionalism

[1] See Fung, Archon (2006), 'Varieties of participation in complex governance', *Public Administration Review*, 66 (S1), 66–75. http://faculty.fiu.edu/~revellk/pad3003/Fung.pdf Revisited in 2015 in Fung, Archon. "Putting the Public Back into Governance: The Challenges of Citizen Participation and Its Future." *Public Administration Review* 75.4 (July/August 2015): 513–522. http://archonfung.net/docs/articles/2015/Fung.PAR2015.pdf

Regulatory Drivers

The Consultation Paper takes place in the context of the jurisdictional focus on information security and the accompanying move to ensure security standards for firms operating in the local market are at a high common standard.

ASIC has made numerous welcome contributions to these areas over recent years including benchmarking assessments of the resilience of firms within the industry (Report 555) as well as REP 429, REP 468, REP 509 and REP 592 and various initiatives to assist the industry progress its resilience.

Continuing this work through the Consultation is entirely appropriate. We also support ASIC using the Consultation to continue its response to the market-wide outage in 2017.

AFMA supports the alignment of definitions with international standards and will note specific instances of this in this submission. However, where ASIC is introducing regulation due to

- multilateral initiatives including IOSCO standards that do not support more principles-based regulation; and
- regulation having been implemented overseas (including as noted in the paper GDPR);

we do note some concern.

Australian regulatory processes must maintain their integrity and must not be subordinated to multilateral initiatives unless this is the express will of the Government.

The Australian regulatory systems must drive the policy settings and outcomes especially at a macro-level. Australia has long set a clear course for principles-based regulation. Such an approach is preferable for Australian businesses as it allows them to more efficiently determine how best to implement the requirements.

It is also compatible with ASIC's legislated first obligation to find such efficiencies and reductions in business costs:

> "maintain, facilitate and improve the performance of the financial system and the entities within that system in the interests of commercial certainty, reducing business costs, and the efficiency and development of the economy" (Australian Securities Investment Commission Act Part 1 Division 1 Section 1 (2) (a)

It is entirely within the remit of the Government to change this approach and more towards more prescriptive, check-box type approach to regulation (noting we would recommend against this), but this should be done in response to Australian Government policy. It may not be appropriate to move away from principles-based regulation on the basis of an IOSCO standard.

Similarly, in relation to international legislation, there are significant differences between the broad policy settings in jurisdictions including the EU and the US. The US specifically does not tend to use principles-based regulation preferring a more rules-based approach.

In relation to the EU processes and GDPR in particular, there may be reason for caution and deferment to Australian policy processes. GDPR has been widely criticised [2] and may not be an appropriate model for local emulation.

Role of Regulation

More generally the Consultation provides an opportunity to consider more clearly defining the boundaries of the proper role for regulation in a market-based economy. While the proposals are consistent with prevailing good practice at market participants and logically the inclusion of these practices in market rules would likely increase consistency in achieving these outcomes, this may not be sufficient to justify the rule making.

Different firms will have risk profiles and will have different appetites for the risks they face given their particular business models. For example, a proprietary trading firm may consider itself inclined to forgo lost trading revenue due to a systems outage rather than duplicate the systems needed to ensure a gold standard of backup and resilience. A small broker may provide only limited backup in the event of an outage as part of its market offering to keep costs low. A broker positioning itself as a provider of high-speed access may forgo some of the resilience features of a market connectivity system in order to ensure speed of connectivity is not compromised, such an outcome might be valued by their clients who accept the trade off in reliability.

We note that in the case of market operators the single point of failure may alter the calculations to some degree although even here to ensure optimal outcomes any regulation intervention must be very carefully calibrated and be sure to avoid being overly prescriptive.

In an ideal world there would be no need to make any compromises any operational matters, however, in practice businesses will assess their particular needs and implement different business plans. There is no reason to expect that market forces cannot be relied upon to correct imbalances over time. Maintaining the flexibility of businesses to make decisions, even those that have accompanying risks for their clients, ensures the business environment remains open to innovation (including, for example, the move to Agile[3] development processes), competitive and dynamic.

Government intervention in such business decisions is certainly costly and may not be beneficial. A measure that implements the prevailing change management processes seems innocuous and currently at no cost, yet might block the use of Agile development techniques. Regulatory obstacles to these techniques would see Australian firms stuck in an outdated development modality that is no longer competitive with international peers. One could imagine similar paradigm changes in relation to BCP, IMP, other areas of technology risk management and controls.

---

[2] See, for example, The National Law Journal - https://www.law.com/nationallawjournal/2018/06/26/the-surprising-news-about-the-gdpr-for-us-law-firms/?slreturn=20180810235058 Forbes https://www.forbes.com/sites/forbestechcouncil/2017/11/13/its-time-to-get-ready-for-strict-new-eu-privacy-regulations/#483fb29456d9 Lawyers Defence Group UK http://www.lawyersdefencegroup.org.uk/gdpr-and-your-firm/

[3] Referring here to the Agile Manifesto https://agilemanifesto.org/

Regulation risks increasing business costs, and damaging the efficiency and development of the economy.

In terms of the mischief that is being addressed in regard to market participants the Consultation Paper notes:

> …we are seeing more errors with participants' systems and processes that result in worse price outcomes for clients; client money being put at risk; settlement failures; and anomalous, and in some cases manipulative, orders impacting the integrity of the market.

Putting to one side manipulative orders, which are already covered under other legislation, the other matters raised can be dealt with by the forces in a market-based system. There is no single provider for access to Australian financial markets. Clients that see poor results from provider can choose a different provider, one more aligned with their risk appetite, in the highly contested and competitive market place.

Merely because some undesirable outcomes are experienced does not necessarily mean that regulation is required or even appropriate. The ICSA Principles for Better Regulation[4] Principle 1 suggests regulators:

> Establish first whether there is a significant market failure or financial misbehaviour arising from firms' conduct, risk management or relations with consumers, which is not appropriately addressed by existing regulations and their enforcement and *which is unlikely to be mitigated over a reasonable period of time by market forces*. [Emphasis added]

Given this, it may be the case that a regulative response, particularly in the form of a new enforceable rule, might not be the optimal approach for some of the issues identified.

The scope of the rules proposed is broad enough that the regulator would be provided with the opportunity to issue sanctions in relation to almost all matters of business operations. This is a significant change to the structure of the business environments in relation to the financial markets.

Business processes will be more defensive, less likely to innovate and more costly for end users. It may be appropriate to pause to consider whether this level of government oversight and intervention in the operational aspects of businesses is appropriate, particularly given the 'mischief' primarily cited is around ensuring sound outcomes for clients and is not related to prudential standards. Matters that are likely to be addressed by market forces.

Government regulation of business operational activities to such a detailed level may not appropriate in a market-based economy.

[4] https://afma.com.au/afmawr/_assets/main/lib90021/icsa%20better%20regulation%20guidelines.pdf

Scope of Consultation and Range of Responses

Consultation Paper 314 covers a wide range of industry practices relating to technology and risk management as well as touching on issues around fair access to markets and trading controls. The scope of affected firms include all market participants and market operators.

We are concerned that the scope of the Consultation may be too wide to comprehensively address all the issues related to these areas in a way that will set a firm foundation for future policies and rulemaking. Further, the consideration of such a wide range of disparate issues could promote a tendency to see the issues as more alike than they might actually be.

As such, we encourage ASIC to consider phasing its response and deferring further consideration of some proposals (for example kill switches and fair access) to separate consultation papers that have the potential to cover these technically highly complex matters in greater technical detail.

Given the breadth and depth of the remaining issues we would support ASIC having an ongoing deep engagement with industry to explore the form and detail of ways forward. Such an approach, perhaps through an industry working group, could assist in ensuring unintended consequences are avoided or minimised.

We would also recommend for future consultations that issues relating to market operators and market participants be dealt with through separate consultation papers to ensure that, given their very different risk profiles, that each is dealt with in a way that is suitably calibrated.

We note also that despite the wide range of issues covered by the Consultation Paper the responses are all to create a Market Integrity Rule. Within the matters considered for Market Participants are:

- system resilience (including IMP and BCP);
- system reliability;
- system integrity;
- system security;
- change management;
- outsourcing;
- data and cyber risk; and
- governance.

These are very different issues and each should be treated according to its accompanying risks, and the wider regulatory framework into which it fits. There are valid reasons, for example, why the character of regulatory response to matters of information security at a market operator might properly have a different response to considerations about how the IT department of a small broker handles change management.

The appropriate regulatory response for the disparate areas covered may, if suitably adjusted, be more varied than MIRs. Some may benefit more from a guidance response, other areas from increased education and dialogue with firms. A structured working group process may be best placed to assist in finding the best calibrated responses.

Regulatory coordination

We encourage ASIC to consider the closer integration of its regulatory framework with the requirements on stakeholders made by other regulators.

Many of the requirements relating to information security, business continuity and outsourcing are already covered for ADI participants and their Related Body Corporates (RBCs) under their obligations to APRA. There may be areas where duplication of these obligations for these participants might be unnecessary.

The relevant APRA standards include CPS 231 (Outsourcing), CPS 232 (Business Continuity Planning), and Information Security (CPS 234). The obligations are for the most part similar or the same as those proposed under the Consultations. Where there are differences these are manageable, for example the scope of obligations might be extended to all AFSL related matters, and could be complimented by a reporting dual obligation if APRA was not disposed to share the relevant reporting.

Regulatory Stance on Operational Matters

A key point of concern in relation to the MIRs as drafted is that it is AFMA's view that the present drafting may characterise all outages and operational imperfections as breaches of regulation.

The use of the word 'ensure' can and in our view likely will be read to mean that a failure of a system will mean that the "arrangements" were not "adequate" to "ensure" resilience, reliability etc. Ensure is usually understood to mean 'make certain'.

Operational matters particularly those involving complex systems are challenging and while ideally there will be no issues, as any operator of complex systems, including the Government, is aware this cannot be guaranteed. We understand that ASIC is keen to ensure that appropriate measures that *could reasonably be expected to* limit the frequency and severity of problems have been undertaken. The industry is supportive of this approach.

While drafting using the term 'ensure' has been used previously by ASIC, given the imperfect nature of operational matters it is appropriate to move the standard drafting that incorporates a recognition that perfection should not be required from these complex systems.

We suggest the legal constructions of:

- "reasonable steps have been taken to reduce, manage or avoid issues with" or
- "must have adequate arrangements to support"

in this regard.

Answers to Questions

B1Q1 Do you agree with the definition of 'critical systems' and 'critical systems arrangements'? In your response, please give detailed reasons for your answer.

The draft approach of broad definitions of critical systems that capture most market related operational activities (as per the consultation paper excluding functions such payroll) may not be sufficiently attuned to the differing risks of different parts of the industry (market operators, market participants, clearers etc.) and the different aspects of operational resilience that ASIC is concerned about (e.g. BCP vs Information Security, vs reliability etc.)

ASIC should consider approaching the definition of the risks it wishes to regulate by using a risk assessment of the potential impacts of issues in each area and for each type of firm. See Table 1 for an indicative assessment of the broad nature of risks to the market system *as a whole* of issues. This could be further broken down by dividing market operators into listing venues and alternate execution venues etc. The table is not intended to be definitive but indicative of the type of risk assessment that could be undertaken

Table 1 Risks to the Market System as a Whole of Outages or Inadequacies

Risks to market system as a whole	Market Operator	Clearing & Settlement Participant	Market Participant
Information Security Breach	Higher	Higher	Higher
System reliability	Higher	Medium	Lower
System Resilience – BCP/IMP failure	Higher	Medium	Lower
System Integrity	Higher	Medium	Lower

At the top level it is important that for *market participants* the definitions are consistent with the redundancy and multi-provider nature of the market for *execution* services.

Market operators, given their services both in regard to execution of certain products and clearing and settlement, can be single points of failure for the industry, and would sit at a higher point on the risk curve. These may be areas where the appropriate response could be the application of an existing regulatory standard (e.g. CPS 234) or carefully calibrated regulations.

Lower than Market Operators but still higher on the risk curve are clearing and settlement participants. Issues with systems at these providers can impact multiple market participants. However, the risks associated with Clearing and Settlement Participants are already covered by recently updated comprehensive requirements in relation to their system resilience, as part of the ASX Operating Rules and associated Guidance. We query whether there has been a market failure that requires regulatory intervention in relation to these providers.

Further down the risk curve are market participants and their execution offerings. Given that investors at the wholesale level typically have relationships with multiple brokers, an issue at a single broker, while undesirable, is unlikely to have significant impacts. In any event market participants are required by the market operating rules to have adequate resources in place. Again, from a regulatory theory perspective we query whether the case has been made that regulatory intervention is appropriate.

While ASIC has noted that it has observed increased system failures with the increased use of electronic trading systems these issues would seem likely to be addressed by market forces over time and are unlikely to be fully eliminated by a regulatory intervention.

Critical systems in this execution context could be limited to those needed to flatten risk positions and manually trade orders that were unable to be re-routed to other participants in the event of a failure. It would not include low-latency or algorithmic services, or trading related facilities such as email, chat, or internet. Ensuring the graceful exit of a provider in a multi-provider context should create, at a system-wide level, sufficient resilience.

AFMA is of the view market participants should have the flexibility to determine which systems are 'critical' to their business subject to a materiality test they determine. ASIC may wish to specify some factors that participants should take into account when assessing systems. Market participants could provide information on the systems they have determined to be critical and their reasons for doing so.

There is a risk that a wide definition of critical systems as proposed will discourage the provision of services unless they can be implemented in a fully fault-tolerant manner. Full fault tolerance (for example hot failover) is generally expensive to provide and would be likely to render many offerings uneconomic. It would certainly discourage innovation as the costs of any proposed innovative service would increase to cover redundancy costs despite the initial minimal impact of any outage.

In the alternate, participants would prefer ASIC align definitions and associated requirements with existing international and domestic standards. Currently the proposed definitions vary significantly from those in other jurisdictions including Singapore and Hong Kong, in the case of the critical systems definition it is much broader. Participants note that, for example, MAS Notice 644 includes in its guidance that a critical system has '*severe and widespread impact* to the bank's operations'. We note also in this regard to the ASX definitions of 'core' systems. ASX Group focuses on potential material impact on the ability of a participant to comply with its obligations under applicable ASX Group Operating Rules.

Firms have a preference for narrowing the definitions to better align with these standard definitions, which would allow firms to follow existing global and local policies and procedures. In the event this approach is taken further detail would be requested on what would constitute 'significant'.

> B1Q2 Do you agree that market participants and market operators should have rules that require them to have in place adequate arrangements for critical systems?

As per our response to B1Q1 this question is different for market operators and market participants due to the different risks associated with outages.

For market operators there are higher risks to the broader system given the utility or single provider nature of some services. Even here though we caution against requiring perfection and rules whereby any outage places operators into a defensive mode. There is a risk that an excessive approach could discourage innovation and create costs that will be passed on to users of the system.

For Information Security for all firm types there may be heightened risks to the market as a whole in the event of this type of compromise. However, it is appropriate, and consistent with the ASIC Act's requirements for efficiency, that there be recognition of the APRA information security standard be for financial firms. AFMA has consistently made the case for this standard to be recognised as sufficient by all regulators.

While the proposed rules are high level and appear consistent with APRA standard CPS 234, we would suggest that firms (and their Related Body Corporates (RBCs)) who conform to CPS 234 due to their requirements as ADIs should have this recognised as sufficient by ASIC.

For clearing and settlement participants while potential operational consequences are, as we have suggested in Table 1, potentially more widely significant, as noted there are comprehensive requirements under the terms of the Operating Rules and guidance. These appear to have worked well and there would appear no case for regulatory intervention.

For execution services in the wholesale markets, at a system-wide level the case for regulatory intervention may be yet to be made for most aspects of operational resilience ASIC is considering.

Activity that is damaging to markets is already caught by the regulations and this requires systems to be appropriate designed and implemented to avoid issues.

Participants also note considerable uncertainty about what 'adequate' means. There is a concern that ASIC in enforcing the rule will deem any failure as proof that the arrangements were not 'adequate'.

Participants also note uncertainty around the case where vendor dependencies are involved and these dependencies fail.

B1Q3 Do you agree with the types of arrangements that market participants and market operators should have to ensure the continued reliability of their critical systems?

Participants note concern around the use of the term 'ensure' which as we have discussed is not appropriate for use in a rule relating to complex systems.

Putting this concern to one side the types of measures proposed are consistent with prevailing good practice.

AFMA understands that Rule 8B.2.2 (1) applies equally to changes that result from changes to market rules, please advise if this is incorrect.

B1Q4 Do you see any challenges for institutions in complying both with the proposed rules and other obligations they may be subject to including, for example, under Basel II or the Financial Stability Standards? In your response, please give detailed reasons for your answer.

Participants report that as the proposals are consistent with prevailing good practice there are no challenges observed complying with the proposed rules and other obligations. If ASIC does proceed to make rules in this regard harmonisation with other international regimes is supported to avoid the need for Australia-specific policies.

Some clarity is sought on the scope of system documentation and change data that is expected to be retained.

B1Q5 How will these proposed rules affect your business? If you are a market operator or market participant, please provide an estimate of the time and costs to implement these arrangements. In providing this estimate, please compare this with your expenditure on your current critical systems arrangements.

Participants advise that more information is needed to make definitive determinations as to the costs associated with implementing the proposals as drafted.

The quantum of costs would depend on factors including the consistency with international jurisdictions and existing local requirements, and detail around matters such as the level of record keeping required.

While firms already have measures in place that would be expected to meet the requirements ASIC is proposing, a full project to ensure this is the case would be a substantial undertaking for large firms, particularly considering the broad range of matters that would need to be investigated and considered.

B2Q1 Do you agree that market participants and market operators should have rules that require them to have in place adequate arrangements for change management of critical systems?

As per our discussion above it may be appropriate to separate out this question for market operators, clearing and settlement participants, and market participants.

For clearing and settlement providers change management there does not appear to be a market failure which would justify regulatory intervention at this time, particularly as change management is already required by ASX Operating Rules and Guidance.

While change management is certainly appropriate for market participants and is the standard industry practice, it is unclear whether the case for regulatory intervention is yet made. If regulatory intervention is appropriate whether this would sit most appropriately in Market Integrity Rules, or in exchange operating rules, or in Regulatory Guidance.

The creation of rules around change management is likely to increase costs as firms adopt a more defensive posture and seek to create evidence for regulatory inspection each step of their internal processes.

There is also a risk as noted in response to B1Q1 that evolutionary developments in software deployment such as Agile software development (or other future evolutions) will be deemed incompatible with ASIC's change management expectations and this will impact the competitiveness of local firms.

AFMA notes the concerns related to the definition of 'critical systems' noted above in response to B1Q1, and related to the definition of 'adequate' noted in response to B1Q2.

There is also concern that in fleshing out the requirements associated with 8B2.2 there may evolve practices unique to the Australian market and this could create additional costs for firms if they differ from practices in other jurisdictions.

B2Q2 Do you agree with our proposed rule? If you disagree, please give detailed reasons why.

AFMA supports some change requirements for market operators. Market operators should communicate significant changes well in advance and provide appropriate testing environments. We do note some concern with the phrasing 'ensuring, to the extent practicable' that persons are adequately prepared may be too prescriptive. It may be appropriate for a large project such as the CHESS project to proceed even if not participants are fully ready, the market should not be constrained from moving to upgrade by, for example, the single slowest moving participant.

In addition to our concerns noted in response to B2Q1, as 8B2.2 (1) and 8B2.1 (a) are operational matters they may be more appropriately located in exchange operating rules.

We query for 8B2.2 (2)(b) and 2(c) are properly matters for management by regulators. Market forces in the highly contested broking space could be expected to manage these risks. They would also rate as having low associated systemic risks.

> B2Q3 How will this proposed rule affect your business? If you are a market participant or market operator, please provide an estimate of the time and costs to implement these arrangements. In providing this estimate, please compare this with your current expenditure on arrangements for change management of critical systems.

AFMA notes firms will have difficulty at this stage in modelling implementation costs. While change management practices are already in place that would be expected to conform with any rules, more detail is required about ASIC's expectations before costs of implementation can be estimated.

There would be expected to be one off costs in compliance updates to policies and training and ongoing costs in relation to testing systems, tracking updates and costs associated with notices.

There would be an overall incremental increase in costs to the business environment associated with the existence of new rules, the costs of which would depend to some extent on the approach of the Commission at the time.

In the event new rules are introduced members request a 12-month transition period.

> B3Q1 Do you agree with our proposed rule that requires market operators and market participants to have outsourcing arrangements? If not, please give detailed reasons why you disagree.

AFMA notes that outsourcing requirements already exist for AFSL holders and ASX participants in *Regulatory Guide 104* and *Guidance Note 9* respectively.

It is clear from the existing guidance that firms cannot outsource their responsibilities as licensees.

Members note that the drafted rules take a highly prescriptive approach to the regulation of outsourcing. Outsourcing is a commercial contract-based activity undertaken by firms in a market economy. AFMA queries whether the extent of regulatory intervention in private contractual arrangements as proposed in the draft rules is appropriate.

The particulars of an outsourcing arrangement will be best understood by the firms involved given the need for the contractual arrangements to reflect the nature of the firm's business and their risk appetite.

Some elements of the proposed rules as we will discuss below are not compatible with the commercial practices that prevail globally.

There is the potential for the creation of a disincentive for third party software and service vendors to participate in the Australian market if they are required by the obligations to notify participants and

gaining their approval prior to making changes and sub-outsourcing. There is a real risk some vendors would remove their offering from the Australia financial markets if this were to be a requirement. Australia would lose the benefit of international software developments and service offerings.

In practice the quality of service offerings in matters, including information security, for the largest vendors can be of the highest order and may exceed the level of security achievable by smaller firms. It would be to the detriment of the jurisdiction's security if such a loss were to occur.

> B3Q2 Do you agree with the definition of 'outsourcing arrangement'? In your response, please give detailed reasons for your answer.
> B3Q3 Do you consider that the definition of 'outsourcing arrangement' covers the provision of services provided by all third-party service providers and not just those that may have been performed by the entity itself? If not, what if any risks do you see in relation to the provision of services by these entities?
> B3Q4 Do you agree with the specific outsourcing arrangements proposed?

These questions are addressed as a group.

AFMA does not support the proposed definition of 'outsourcing arrangement'.

The definition proposed is broad and not compatible with existing and internationally accepted definitions of outsourcing.

ASIC could further refine any outsourcing rules to relate only to 'Participant's Critical Systems' but in our view, this should build upon a more standard definition of outsourcing.

The broad proposed definition could also introduce some matters such as the provision of internet services into the scope of outsourcing which is likely not intended. Where a third party provides a system (e.g. a computer operating system) but does not support or operate it, this would not constitute an outsourcing arrangement under standard outsourcing definitions.

Intragroup arrangements, while contemplated at paragraph 66 in the Consultation, should also be addressed by the definition and rules.

The definition of outsourcing should:

- Be restricted to a business activity that is or could be undertaken by the participant itself (this would exclude matters such as internet, telephony or banking services; and
- Be performed on an ongoing basis by the outsourcing provider.

Business practices which are outsourced that are not part of the services that could or would typically be performed by the business as part of their licenced services have a different risk profile and would not be appropriate to include in the ASIC definition.

Any definition of outsourcing used by ASIC should align with the ASX (Guidance Note 9) definitions. We note also the APRA definition (CPS 231) as a potential avenue for alignment.

AFMA supports the use of the ASX definition[5]:

'"Outsourcing" occurs when a participant (or another group entity acting on behalf of the participant) enters into an arrangement with another party to perform, on a continuing basis, a business activity that currently is, or could be, undertaken by the participant itself. That other party could be a related body corporate or an unrelated third party.'

ASX does not regard arrangements between wholly-owned group entities to be outsourcings for the purposes of guidance note 9:

> Inhouse arrangements between wholly-owned group entities
> ASX acknowledges that many participants form part of a larger wholly-owned corporate group and that those groups often conduct their business activities as if the entities in the group were part of a single enterprise. It is not uncommon, for example, for various activities relating to the business of a participant to be performed by functions that sit within, or staff who are employed by, another entity within the group, without the arrangements between the entities being formally documented in legally binding agreements. These arrangements can extend to the provision of premises, equipment, technology, finance, accounting, legal, compliance, risk, administration and other support services.
>
> So long as these activities remain wholly inhouse – that is, between wholly-owned group entities – ASX does not consider them to be "outsourcings" for the purposes of this Guidance Note. They may, however, constitute an "offshoring" if and to the extent that the wholly-owned group entity performing the activities does so outside Australia.

Misalignment between the ASIC and ASX would cause dual lists of 'outsourced' activities to be maintained with attendant complexity, administrative burden and confusion. For example, a delegation to a wholly owned group entity would be an 'outsourcing' under the proposed ASIC definition but not under the ASX definitions.

We note that some of the particular provisions are not compatible with standard commercial practice globally:

- The requirement for 'prompt audit rights' (8B2.3 (1) (f)); and
- the proposal that sub-outsourcing services require approval from the Participant.

These are not practical in a globally connected business with multiple affiliates, and considering the prevailing practices and should be removed.

The requirement for Boards to provide be involved in and provide a written attestation (8B2.3(1) (h)) is an inappropriate requirement for a governance body. It is not appropriate to require Boards as part of their governance oversight role to make attestations to the actions of management. From a

[5] See ASX Clear Operating Rules, Guidance Note 9 https://www.asx.com.au/documents/rules/asx_clear_guidance_note_09.pdf

practical perspective to properly do so they would require costly external audit verification if they were avoid reliance on the firm's management.

The requirement for senior management to provide a written attestation that they have complied with ASIC rules when engaging in private contracts with other private firms is unnecessary given their responsibilities to follow all relevant rules and regulations. It is unclear why this particular rule should be singled out from all the rules that senior management must follow for specific attestation.

Suggested redraft:

> "ensure that for each outsourcing arrangement, the market operator's and market participant's ~~board and~~ senior management **have taken reasonable steps to** confirm~~ed~~ they have complied with their obligations above. ~~and have made a written attestation to that effect~~"

AFMA notes that the requirements around conflicts of management identification and management require further explication. The drafting is broad and it may be of benefit if there is greater clarity around the particular concerns of ASIC.

> B3Q5 Do you consider that the risks associated with outsourcing to the cloud warrant a rule specific to that outsourcing arrangement? In your response, please give reasons for your answer.

AFMA supports cloud outsourcing being covered by the more general outsourcing rules. Creating a delineation for cloud services could create difficulties and overlap between requirements.

We note that cloud computing is already covered by the APRA standard for ADIs. ADIs and their Related Body Corporates should be able to rely on complying with the APRA standard.

> B3Q6 How will these proposed rules affect your business? If you are a market participant or market operator, please provide an estimate of the time and costs to implement these arrangements. In providing this estimate, please compare this with your expenditure on your current outsourcing arrangements.

AFMA supports a minimum 12 months for any changes. Final costs will depend on the final form of the rules, the extent to which requested changes are made, and the compatibility with prevailing global practices.

AFMA also notes that related party should be defined.

> B4Q1 Do you agree with the proposed rules? If not, please give detailed reasons why you disagree.

AFMA notes that the proposed rules are already covered for ADI participants by the APRA Information Standard CPS 234.

AFMA has been keen to see the ability for firms to rely on a single information security standard from the Australian regulatory environment where possible and appropriate. At a minimum, ADIs and their Related Body Corporates should be able to rely on their conformance to the APRA

standard. There will be additional costs for no benefit in having these entities demonstrate their conformance to a duplicate set of requirements.

We encourage regulators to coordinate their activities to minimise the costs of regulatory activities to Australian business. This is consistent with Act Part 1 Division 1 Section 1 (2) (a) of the ASIC Act.

> B4Q2 Should the proposed requirement for market operators to notify ASIC of any unauthorised access to or use of their critical systems and market-sensitive, confidential or personal data be extended to market participants? Please provide detailed reasons for your answer.

AFMA is not in a position to support the proposed notification requirements.

There are existing requirements for reporting of unauthorised access or disclosure of personal information to the Office of the Australian Information Commissioner.

If ASIC does proceed to make a rule in this regard then the drafting should be significantly refined.

AFMA would support the introduction of a materiality threshold around the reporting requirement. This should be used to limit the need to advise ASIC of minor matters which should not be within the scope of regulatory rules. The current drafting appears broad and would appear to risk capturing where a staff member might still be on an access list after changing roles but before the list was reviewed.

Members are concerned that clarity should be given that unsuccessful attempts to infiltrate systems should not be reportable.

If ASIC does proceed to create a separate information security standard, then further clarification and explication of 'adequate arrangements' would be appropriate.

There are also concerns that 'timely' should be defined in a way that does not interfere with the firm's first priority of responding to events. Firms should have clear air to prioritise their response to these type of events rather than focussing on regulatory reporting obligations, which is an increasingly common issue.

> B4Q3 How will these proposed rules affect your business? If you are a market participant or market operator, please provide an estimate of the time and costs to implement these arrangements. In providing this estimate, please compare this with your expenditure on your data protection arrangements.

The proposed rules will add to the regulatory burden and risk profile of participating in the Australian financial markets.

> B5Q1 Do you agree with the definition of 'incident' and 'major event'? In your response, please give detailed reasons for your answer.

AFMA suggests that the definition of 'incident' be altered to include a qualifier such as 'significant' rather than 'unexpected' as IMP are not appropriate for application to minor matters even if unexpected. It may be appropriate to allow firms to determine what factors would lead an incident being found to be significant or a major event depending on their business model and risk appetite.

We also note that 'usual operations' may need further explication as firms may define these differently depending on the type of outage.

> B5Q2 Do you agree with our proposed rule that requires market operators and participants to have plans for dealing with an incident or major event? If not, please give detailed reasons why you disagree.

It is appropriate and prevailing good practice to have plans for dealing with incidents and major events. For market operators given their potential in some cases for systemic impact there may well be a case for a regulatory requirement.

For market participants we query whether the prescriptive approach proposed is appropriately calibrated to the risks. Guidance may be more appropriate given the risks and this may provide more flexibility for varying levels of response appropriate to firm appetite risk and business model.

8B.3.1 (2)(a) requires IMP and BCP plans "**must** be designed to enable: to the extent possible, continuation of the usual operation of Critical Systems" [Emphasis added]. This is a prescriptive requirement and may not be aligned with existing practice at many firms.

Firms may, having assessed the balance of reliability required to meet their client expectations, opt to run on lower specification machines (for example the machines that were previously installed as front line systems), with a more limited set of functionality. In our view this type of approach should not be a breach of the rules.

The requirement at 8B.3.1 (2)(b) which requires IMP and BCP plans to 'timely and orderly restoration of those usual operations' restoration of services, may also not be aligned with the business plans of all participants. A proprietary trading firm might decide that it will only work slowly to restore operations in the event of a major outage given the risks of prompt restoration of services. This type of approach similarly should not be a breach of the rules.

More generally we are concerned that the prescriptive approach taken will decrease the flexibility of firms in the market economy to adjust their IMP and BCP approaches to provide economic and cost effective responses.

We will not discuss each of the requirements suggested in the proposed rules, but note that we have a range of concerns, including around the potential for regulatory adjudication post factum around matters such as whether in the heat of a 'Major Event' event classification, internal escalation, external communications, were as planned and whether time objectives were met. If these were not ideal then ASIC may find the participant did not have adequate arrangements to carry out its plans (required by 8B.3.1 (5)).

> B5Q3 Do you agree with the frequency of reviewing and testing incident management and business continuity plans?

The review and testing timing is aligned with standard industry practice. We note only that calendar year-based testing should be allowed to facilitate flexibility in timing of testing to, for example, avoid significant exchange software release dates. This would result in the period between tests being longer than 12 months in some instances but overall would create no change in the amount of testing over time.

B5Q4 Do you agree with the specific arrangements required in an incident management plan or business continuity plan?

AFMA does not support the proposal to require immediate notification to ASIC of a Major Event. The notification of regulators should not be the top priority when responding to an outage. Firms should be free to focus their energy on responding to the event and minimising the impact on their clients and the market. Regulatory notification should only be required when practical. Where reporting is required ASIC should provide a standard template.

B5Q5 How will these proposed rules affect your business? If you are a market participant or market operator, please provide an estimate of the time and costs to implement these arrangements. In providing this estimate, please compare this with your expenditure on incident management and business continuity arrangements.

AFMA queries the benefit of the requirement to hold the documentation for 7 years as opposed to five. This would appear to add cost without operational benefit.

B6Q1 Do you agree with our proposal to introduce this rule to ensure adequate governance arrangements and resourcing? If you do not agree, please provide detailed reasons why you disagree.

AFMA raises the importance of distinguishing between governance and management. Boards should not be required to provide shadow management. We suggest the phrasing be changed to "Board *or* Senior Management". Many Boards will delegate the detailed operational aspects of BCP arrangements to senior management. The Board's role is then to ensure governance of these arrangements is in order.

B6Q2 How will these proposed rules affect your business? If you are a market participant or market operator, please provide an estimate of the time and costs to implement these arrangements. In providing this estimate, please compare this with your expenditure on governance arrangements.

The proposed requirements around Boards may not be readily compatible with some corporate structures and if they were to proceed there could be significant costs associated with making arrangements to integrate offshore Boards into these processes.

B7Q1 Do you agree with our proposal to introduce this rule to ensure fair access to the market? If you do not agree, please provide detailed reasons why you disagree. B7Q2 How will this proposed rule affect your business? If you are a market operator, please provide an estimate of the time and costs to implement this fair access rule

We note this is a complex area and might be best deferred for more detailed consideration.

B8Q1 Do you agree with our proposal to introduce trading controls? If you do not agree, please provide detailed reasons why you disagree. B8Q2 How will these proposed rules affect your business? If you are a market operator, please provide an estimate of the time and costs to implement these trading controls.

AFMA views ‘kill switch’ functionality as an important part of pre-trade risk management. However we are of the view that there may be benefit in further consideration of the issues before proceeding to rule-making.