



16 August 2019

Mr 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

Re: Response to ASIC Consultation Paper 314 – Market integrity rules for technological and operational resilience

Thank you for the opportunity to comment on the proposal to establish new Market Integrity Rules (MIRs) governing the technological and operational resilience of market operators and participants.

ASX recognises the importance of appropriate arrangements for the management of technological and operational resilience. Our initial thoughts on the impacts, costs and benefits of the specific rules proposed by ASIC are set out below. In summary:

- The proposal applies only to certain licensed market operators and market participants. This excludes a number of service providers whose operations are arguably equally or more significant to the functioning of Australia's financial markets. This leaves a gap that reduces the effectiveness of the rule framework.
- ASIC has indicated that it will take account of the market operator's or participant's importance to the operation of the market in applying the rules, but there is no certainty of this or how it would apply. Rules themselves do not differentiate between participants in a way that will enable participants to confidently and consistently interpret how they apply to particular circumstances.
- Rules are drafted in general terms which create problems of interpretation and consistency of application – most significantly, the core concept of "Critical System". At the same time, the rules impose a standard of perfection, using concepts such as "ensure" and "prevent" when, in practice it is not possible to extinguish all risks.
- If absolute standards of compliance are imposed then in our view the requirements must be specifically and clearly articulated. Alternatively, if requirements are expressed in broad terms, then there must be allowance for judgement and difference in the approach to compliance.
- Rules relate to matters that are subject to existing regulation (e.g. privacy and data security) with no sense of how these different requirements interact.
- The six month transition period appears significantly short of what could reasonably be required to implement the new arrangements. This is particularly the case for outsourcing obligations which potentially involve significant contractual renegotiations with multiple counterparties.
- Change management rules lack definition required for market operators and participants to understand when and how much notification is required. They also put an obligation on market operators and participants to ensure, to the extent reasonably practicable, that persons who may be materially impacted by any change to a critical system are prepared for implementation. This approach risks materially impacting on the timing and deliverability of significant projects.
- Outsourcing rules impose requirements for outsourcing contracts that are outside the control of market operators and participants and rely on cooperation from contractual counterparties. If counterparties do not agree, then

20 Bridge Street
Sydney NSW 2000

market operators and participants will be faced with the choice of terminating arrangements for critical services or being in breach of the MIR. This seems likely to result in significant disruption and may result in sub-optimal selection of contract counterparties based primarily on their preparedness to agree to terms required by ASIC.

- Incident reporting rules do not sufficiently distinguish between incidents based on severity or complexity which may result in inconsistent or over/under reporting. Rules requiring quarterly market operator BCP testing are excessive and potentially disruptive to operations.

Encouraging best-practice technological and operational risk management practices across service providers can strengthen the resilience of Australia's financial markets. It is not clear that a rules-based framework is the best approach to deliver this outcome.

Our initial assessment, in the time available, of the draft rules and preliminary discussions with other market operators and some participants in our markets has identified a number of issues with the potential application and implementation of the rules. These discussions have been valuable in enhancing the understanding of those involved with the practical impacts of these proposals.

This is consistent with our recent experience with the CHES replacement project where the establishment of working groups involving the sharing of information and the perspectives of different stakeholders has been more effective in teasing out issues and identifying solutions than is possible with more traditional written consultation processes.

We suggest that ASIC establish working groups or other appropriate fora to work through these issues with a wide range of stakeholder across the end-to-end securities value chain before proceeding further with these proposals.

Gaps in coverage of the new rules would reduce effectiveness

ASIC is consulting on changes to the MIR framework, which would impose the new requirements only on certain licensed market operators and market participants. While it is appropriate for there to be a level of focus on these important financial market intermediaries, there are other important service providers in financial markets who are not subject to the MIR, and so this approach would leave significant gaps in the framework.

Arguably, those gaps are so significant that the new framework would not result in improvements that outweigh the cost of implementation.

Key service providers who are critical to the efficient operation of Australia's securities markets and the management of systemic risk and who are not subject to the MIR include trading and data system vendors and share registries. System failures within these other service providers could significantly disrupt the operation of financial markets, and arguably would have a greater impact than a failure within many smaller to mid-sized market participants who are subject to the MIR.

Any measures intended to improve technological and operational resilience in our securities markets will be sub-optimal if they do not identify and address all material points of vulnerability. A partial solution, which addresses some points of vulnerability while leaving others in place, may be ineffective. We encourage ASIC to consider and engage with the industry on an end-to-end solution.

We also note that not all licensed financial markets are subject to the MIR. Again, this leaves a significant gap in the proposed framework. It is not clear to us – and no reason is given in the consultation paper – why issues that are relevant to one group of market operators are irrelevant to another. Without having looked at this in detail, we can see that there would be arguments for having different levels of expectation for different types of market operator. But an “all or nothing” approach seems inconsistent with ASIC's expressed view of the seriousness of these matters.

The proposed MIR will impact market operators and larger group of participants in those markets. While some of the more significant service providers will already have well-developed governance arrangements in place they may need to revise some processes to comply with the detailed requirements set out in the new rules. Smaller firms may have more work to do to comply with the new rules.

Market operators and participants would have a six month transitional period from the date the proposed rules are made to implement the necessary arrangements. Our view is that this is likely to be materially insufficient, particularly if existing contractual arrangements are expected to be renegotiated. A 12-18 month period (or a staggered implementation) may be more achievable, but we recommend that ASIC should bring together all industry stakeholders

to understand the issues involved in implementation and to agree an appropriate transition period. The interconnectedness of systems highlights the importance of having all stakeholders engaged if the market resilience is to be strengthened.

Rules may not be superior to guidance in enhancing risk management practices

Regulatory expectations with respect to market operators (RG 172) and participants (RG 104) are currently set out in guidance associated with the licensing regimes for market operators and participants. It is now proposed to codify more prescriptive requirements in the MIR.

There may be a case for moving from a guidance-based approach to a rules framework if there is an identified problem requiring an enforcement approach, where rule breaches can be readily identified and penalties assessed. However, this approach does not appear best placed to the task of encouraging a best-practice approach to risk management of technology and operational resilience. This is the responsibility of senior management, and in some cases Boards, to consider how best to manage operational resilience.

Guidance can be expressed in more general terms that can be an effective way for a regulator to articulate its expectations and influence outcomes. This is particularly the case given disruptions to market operator and participant systems in recent years have been rare and are usually quickly resolved.

It is important to consider whether the introduction of new rules will deliver outcomes that justify the higher compliance costs for market operators and participants. As an alternative, additional clarity on ASIC's expectations with respect to these matters could be achieved through further or redrafted guidance. Updated guidance could achieve the promotion of best practice arrangements that would better position firms to adapt to unexpected events or respond to sudden disruptions to other systems.

Many service providers, particularly the larger and more significant firms, already have appropriate systems in place. It is not evident from the consultation paper that there is a systemic problem requiring a new regulatory framework. A cost-benefit analysis of different regulatory approaches to enhancing system resilience would have been useful in highlighting the relative merits of different alternatives in achieving the desired policy objectives.

If this proposal to codify obligations in MIR proceeds, then we would encourage ASIC to consider which parts of the regulatory framework may be best suited to rules and which is more appropriate for guidance. Where rules are favoured these should be drafted in a precise manner and accompanied by clear guidance on expectations.

Enhancing resilience does not require prescriptive rules

The embedding of guidance into rules can potentially give market operators and participants greater certainty about their regulatory obligations, provided that the rules are clear and specific. This is particularly important when there are significant penalties for non-compliance with the rules.

It needs to be recognised that there is no one-size-fits-all solution to managing these risks and building operational resilience. Prescriptive rules can discourage firms from applying solutions that are most appropriate to their circumstances. Firms need to reflect on their own risk tolerances, resources, systemic importance and the impact a system failure would have on others.

An overly prescriptive approach to achieving the policy objectives can also have a significant impact on market structure (by driving out smaller players thereby increasing market concentration) and reducing innovation (by discouraging new entrants and service enhancements). This can stifle new products and services and detract from the attractiveness of Australian markets.

Rules may have a significant impact on sections of the industry.

- As noted above, clear guidance is a good alternative to prescriptive rules, particularly when dealing with issues such as technological and operational resilience.
- One reason is the flexibility that guidance provides to firms to develop internal processes that are most appropriate and designed for their specific circumstances.

While ASIC proposes to take a proportionate approach to applying these rules, based on a service provider's importance to the operation of the market, there is no indication how this will work in practice. Firms are not in a position to make these judgements themselves without clearer guidance.

Guidelines on best-practice approaches to identifying and managing risks are more likely to be effective in encouraging firms that need to improve their practices and to deliver more consistent approaches across different service providers.

Critical systems arrangements concepts in the draft rules are not well defined

There needs to be greater clarity about which systems are considered to be 'critical' and subject to higher obligations. The classification of a system or service as critical determines how broadly the new obligations will impact. Setting the definition too broadly or leaving too much ambiguity as to how it should be interpreted could capture a multitude of systems and make the associated obligations very unwieldy to meet.

The 'critical' designation is defined by reference to the significance that a disruption may cause to the operation of the market. This is not always straightforward to assess in advance of an incident regardless of the steps taken to manage operational risk. A strict interpretation of the rules would be that this constitutes a breach of the MIRs.

There needs to be a practical approach to defining what constitutes a 'critical' system. There also needs to be some mechanism to provide firms with some degree of regulatory assurance that they have interpreted this concept appropriately and it is applied consistently across all providers of similar services.

The concept captures systems that 'deliver or support' a range of functions. The inclusion of systems that 'support' the delivery of functions has the potential to catch many, often minor systems, within the new obligations.

The responsibility for identifying critical systems lies with the service provider. Without sufficient clarity, there may be an incentive to overclassify systems to minimise regulatory (not operational) risk. It is also likely there will be an inconsistent approach taken by firms in similar circumstances – this would be an inefficient and unfair outcome.

Establishing an industry working group that could, for example, discuss what constitutes a critical system for this purpose would be an effective way to ensure a common approach across the industry to this important question.

There should be a process for a firm to receive some assurance from ASIC that their assessment is correct, perhaps through a formal designation of a firm's critical systems. This would also assist in promoting consistent outcomes.

New rules should not be imposed in a manner that imposes additional regulatory burdens on some providers of particular business services (e.g. information and technical services, data centre hosting, network connectivity, etc) which may be provided by a number of suppliers. The obligations should be based on what functions are provided not whether they are provided by an entity that holds, for example, a market licence if competitive neutrality is to be maintained.

Some of the terminology used in the draft rules around the need for operators to have adequate critical systems arrangements (e.g. 'ensuring', 'preventing', etc) suggests a zero tolerance for system disruptions when that is not a reasonable expectation. A more appropriate formulation would be to achieve an outcome 'to the extent reasonably practicable'.

Change management of critical systems

Managing change in critical systems is an important responsibility for market operators and participants, particularly given the need to regularly upgrade systems to reflect the most up to date technology and when the time comes to replace legacy systems.

The approach to defining 'critical systems' will have a significant impact on the practicality of the proposals related to obligations around managing change of critical systems. The broader the definition the more systems (including relatively minor systems that support service delivery) that will be captured.

Notification requirements should not apply to minor changes or changes to ancillary systems but only to those that are material.

ASIC also needs to clarify what constitutes a 'reasonable time period prior to implementation' when notifying them of system change and in what circumstances it would intervene in a market operator's system change process.

Outsourcing critical systems

Market operators and participants make significant use of third-party providers to supply technological systems and services that support or deliver business functions. They should conduct appropriate due diligence prior to engaging third-party providers and have in place appropriate contractual arrangements with these suppliers.

Licensed entities are aware that they remain responsible for fulfilling their regulatory obligations, even if some or all of the technology or operational support is provided through an outsourcing arrangement.

ASIC proposes that a market operator should be required to give written notice to ASIC before entering into an outsourcing agreement for a critical system to allow ASIC to monitor emerging risks. There may be reasons of timing or commercial confidentiality why this would not be practicable, and the stated rationale does not require pre-notification. We suggest replacing this with notification within a reasonable time of entering into the agreement.

The proposed rules also require that market operators and participants ensure ASIC has 'the same access to all books, records, and other information' maintained by the third party supplier as they would if there was no outsourcing arrangement in place. This requirement may impact the ability of local operators to use the services of large, local and global technology firms who may be unlikely to agree to any such condition in an outsourcing agreement.

This could have an impact on the ability of market operators and participants to use the most suitable technology or service provider for their circumstances and it may require them to terminate existing arrangements. This would result in potentially very significant disruption and prevent firms from making sound outsourcing decisions.

The requirement for an attestation that the appropriate processes have been followed should fall on senior management, with Board attestation required only for the most significant projects. The Board will not be responsible for managing the contracting processes and is not in the best position to provide the attestation.

Risk management – Data and cyber risk

Data management, protection of sensitive market and personal data, and effective management of cybersecurity risks are all important responsibilities of both market operators and participants.

In a number of areas (eg. cybersecurity and privacy) there are multiple regulatory requirements imposed by different authorities and there needs to be a whole of government approach to develop common standards to ensure firms captured within the new MIR framework are not subject to overlapping or conflicting regulation.

There is a proposed requirement that a market operator or participant must notify ASIC in writing, as soon as practicable on becoming aware of any unauthorised access to, or use of, critical systems or sensitive data. Notification should occur once the nature of the impact of the incident is known.

Incident management and business continuity arrangements (BCP)

Having plans to manage incidents and to recover systems in the event of an outage is an important element of a market operator's tool kit.

It is also proposed to establish a rule [Rule 8A.4.1(6a)] requiring market operators to 'immediately' advise ASIC when these incidents occur. Operators of other markets, clearing facilities and participants impacted must be notified 'as soon as practicable' [Rule 8A.4.1(6b)] after being aware the incident. The priority of a market operator (or participant) should be to advise affected users in the first instance to enable them to manage any impact the incident has on their operations.

The MIRs would require market operators to conduct BCP testing at least every three months as well as after a material change to a 'critical system'. Such frequent BCP testing is excessive as it is a very resource intensive process (for both market operators and their participants) that carries some risk to being operational for the next business day while not materially enhancing system resilience. ASX currently conducts annual BCP tests and does not see a strong argument for more frequent testing.

Governance arrangements and adequate resources

The proposed MIRs will require market operators and participants to have governance arrangements and adequate financial, technological and human resources to support compliance with the proposed rules. As these requirements

are being codified into rules there will need to be clear guidelines on the expectations of what constitutes 'adequate' resources.

Trading controls

A proposed MIR requires a market operator to have controls, including automated controls that enable immediate suspension, limitation or prohibition of the entry by a participant of trading messages is noted.

Having 'kill switch' functionality and other controls available is normal practice for market operators but decisions around when, and how, to employ that functionality to ensure a fair, orderly and transparent market requires judgement and may not be appropriate for prescriptive rules.

It is not clear if ASIC proposes to introduce any guidance around its expectations in this regard. The rule should not be applied in a manner that seeks to second-guess or penalise the real-time decisions of market operators to apply these controls.

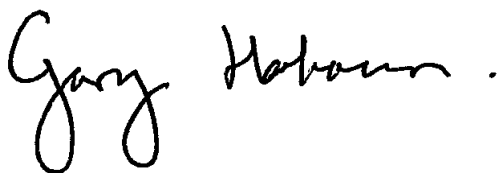
This submission sets out ASX's initial views on the proposals advanced in CP 314. It is difficult to provide more detailed comment on the nature, and potential impact, of individual rules given the uncertainty around how they are meant to be interpreted.

In our view the best way to resolve these issues and produce a regulatory framework that achieves its objectives in an efficient and effective manner would be to convene a working group of relevant industry stakeholders (including representatives from across the end-to-end value chain) to exchange views, discuss solutions and identify the practical costs and benefits of different proposals.

As ASIC has noted, the use of technology has grown and become increasingly complex and interconnected. The ability for a wide range of stakeholders to share their perspectives on these matters will deliver a more robust outcome, and a more consistent approach to these issues across service providers than can be achieved through a process of individual written submissions.

ASX would welcome the opportunity to participate in such an open exchange of views involving regulators, market operators, participants, and other critical service providers in Australia's financial markets.

Yours sincerely



Gary Hobourn
Senior Economic Analyst
Regulatory and Public Policy
+61 (0)2 9227 0930

