8 June 2022

Ms Katrina Purvis
Australian Securities and Investments Commission
Level 5, 100 Market Street
NSW 2000

Email: Katrina.Purvis@asic.gov.au

Dear Ms Purvis

Re: Draft Guidance on technological and operational resilience

AFMA welcomes the opportunity to provide feedback on the draft guidance for the technological and operational resilience Market Integrity Rules.

Please find attached a table which summarises AFMA's feedback on the draft guidance.

At a high level AFMA remains concerned about the continued proliferation of information security standards, and supports participants being able to nominate alternative standards such as the APRA CPS 234 standard where they are regulated already by that standard.

To ensure efficient application firms should be given greater discretion to apply materiality thresholds to matters, particularly in relation to Critical Business Services.

We would be pleased to discuss our feedback further if that would be of assistance and to work with ASIC in rolling out the guidance to market participants.

Yours sincerely

Damian Jeffree
Senior Director of Policy

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 7907 Email: secretariat@afma.com.au Web: www.afma.com.au

RG265.1	Chapter 8B of the Securities Markets Rules and this section of the guide applies to all market participants that trade in equity market products and CGS depository interests. Similar rules also apply to participants of the futures markets. Guidance for futures market participants can be found in RG 266.	AFMA asks if the futures guidance will be substantially different from the current draft securities guidance? We note that RG266 has yet to be updated for technological and operational resilience requirements.
RG265.2	While the rules apply to market participants, the obligations set out sound practices that have more general applications. Other AFS licensees should consider applying the principles in the rules to their business.	While we support the view that the guidance has utility beyond its MIR scope, as drafted this guidance could be read to suggest that the rules might also apply to non-participant activities. We suggest the language be clarified to ensure no obligation is placed on other AFS licensees.
RG265.6	Market participants must identify the critical business services relevant to their business: Rule 8B.2.1(2)(a). We expect market participants to determine which services are critical in the context of their own businesses and consider the nature, scale, and complexity of their operations. The factors that may be considered in identifying critical business services include the criticality of a service to users, the ready availability of other services for users in the event of prolonged disruption, and any dependencies that third-party businesses may have on a service.	AFMA supports further dialogue with ASIC to assist refinement of understanding of expectations around this guidance.
RG265.7	In defining critical business services, we have provided examples of what we consider likely to be critical business services for market participants: see the definition of critical business services and related note in Rule 8B.1.2. Critical business services generally include functions, infrastructure, processes, and systems that deliver or support: (a) order acceptance; (b) routing and entry; (c) clearing and settlement of transactions; (d) payments and deliveries of securities and funds; (e) accounting for and reconciling client money; (f) trust accounts; (g) securities and funds; (h) provision of trade confirmations; and (i) regulatory data reporting to market operators.	It would be useful if ASIC could provide examples of what it does not consider to be a Critical Business Service. This would assist larger Participants from applying a broad interpretation of the current definition which may lead to long lists of unnecessary systems or services that may not have been ASIC's intention.

RG265.11	Market participants must have critical business services arrangements for identifying, assessing, managing and monitoring for any risks to the resilience, reliability, integrity and security of their critical business services: Rule 8B.2.1(2)(b). In order to identify and appropriately manage any risks, a market participant should have a risk management framework that facilitates a consistent approach to the identification, assessment, management and monitoring of risks. The risk management framework would generally include relevant policies, procedures and adequate organisational resources.	It may be preferable to refer to RG 104 rather than create a duplicate separate requirement for a risk management system.
RG265.13	The board or senior management of a market participant should have appropriate oversight of the risk management framework. The board or senior management should take an active role in reviewing and approving the risk management framework.	This requirement appears duplicative to existing risk management system requirements.
RG265.15 and 16	Sufficient and scalable capacity RG 265.15 Market participants should have arrangements for ensuring their critical business services have sufficient and scalable capacity for the participant's ongoing and planned operations and services: Rule 8B.2.1(2)(c). Human capacity RG 265.16 Market participants should have sufficient human resources to conduct their business and provide their services properly. What is 'sufficient' will depend on the nature, size and complexity of the market participant. As a market participant's businesses may change over time, a market participant should keep under review whether it still has sufficient human resources, including the right balance of skill sets.	Requirements appear duplicative to existing licence condition requirements.
RG265.23	At a minimum, market participants must review their critical business services arrangements following each material change to their critical business services and at least once every 12 months: Rule 8B.2.1(3)(b). However, it may be appropriate for larger and more complex businesses to review their arrangements more frequently.	AFMA requests that the last sentence be removed. The regulatory requirement is at least once every 12 months. All participants should be held to the same bar.

RG265.24	A market participant's critical business services arrangements should be reviewed to ensure they remain adequate and are within the risk appetite and risk tolerance levels of the market participant. Market participants must implement any recommended changes to critical business services arrangements arising from the review. The monitoring and review of arrangements should be proportional to the nature, scale and complexity of the business: see RG 104 at RG 104.21–RG.104.22.	While requirements around review are appropriate, we do not support mandatory implementation of review recommendations. Decisions around resource prioritisation are matters for firms to manage and while reviews will provide one input to this function, they cannot be the sole determinant. As a practical matter it may not always be possible to implement all recommended changes, and this should be allowed.
RG265.28	Market participants must have adequate arrangements to ensure they continue to comply with Rule 8B.2.1(1) following the implementation of a new, or change to an existing, critical business service: Rule 8B.2.2. Adequate arrangements include, but are not limited to, testing of a new critical business service or material changes to an existing critical business service. We expect that testing includes all planned changes to processes, technology, data and infrastructure, and considers the effect on stakeholders relying on the critical business service. Testing should occur before the live implementation of a new critical business service or material changes to a critical business service.	Requiring testing on all releases without a materiality threshold is not an efficient solution. Some changes by their nature may not require testing, such as process cessation.
RG265.30	Market participants must have effective internal and external communication strategies that form part of these arrangements. These strategies must ensure persons who may be materially impacted by an implementation of a new critical business service, or a material change to an existing critical business service, are adequately informed about the nature, timing and impact of the implementation a reasonable time before it occurs. What a reasonable time is will depend on the size, complexity, and impact of the change, including the impact on clients and other third parties.	AFMA supports scoping of this requirement to be based on 'those who could reasonably be expected to be materially impacted' to avoid including those with the merest possibility of impact, and that flexibility be created around the 'reasonable time' requirement as this may not always be an efficient or desirable restriction.
RG265.36	Testing - When introducing or modifying a critical business service, relevant testing should be performed before going live. Examples of relevant testing include, but are not limited to, the following: (a) Functional testing…	AFMA asks ASIC to please confirm whether these are just examples of testing that the market participant may consider or whether each of these testing categories are required?

	(b) Connectivity testing… (c) Conformance testing…. (d) Regression testing…	
RG265.42	Critical business services that are commonly outsourced by a market participant include, but are not limited to: (a) order acceptance, routing and entry using trading platforms supplied by third-party vendors; (b) clearing and settlement of transactions by a central clearing house; (c) accounting for or reconciling client money and trust accounts conducted by a third-party custodian; and (d) regulatory data reporting.	AFMA requests clarification that clearing and settlement systems are not within scope of the regulations as per RG265, or delete (b). A materiality test should be included to support an efficient approach. Where outsourcing providers are related body corporates this should be allowed to factor into risk calculations.
RG265.45	Market participants must ensure that the outsourcing arrangement is contained in a legally binding agreement between the market participant and the service provider: Rule 8B.2.3(1)(b). The agreement must provide, among other things, for the orderly transfer of services in the event of termination of the arrangement. An outsourcing agreement should clearly define the ownership of intellectual property and provide specifications relating to the transfer of information to the market participant following the termination of the outsourcing arrangement.	We propose an edit for clarity: "An outsourcing agreement should clearly define the ownership of intellectual property and provide specifications relating to the transfer of information to the market participant *or the new service provider, as instructed by the market participant* following the termination of the outsourcing arrangement". We also seek clarification on whether the (return) transfer of information back to the market participant can also be made directly to a new service provider, as instructed by the market participant.
RG265.46	Additional safeguards can be implemented in the contractual arrangements between market participants and service providers. For example, market participants may include, in an agreement with the service provider, provisions that: (a) terminate the contract if the service provider subcontracts services material to the outsourcing arrangement; (b) require the market participant to grant approval before the service provider subcontracts services material to the outsourcing arrangement; (c) require the service provider to provide an annual assurance about the adequacy of their security controls and resilience capability;	Request for guidance to be limited to what are mandatory requirements to be included within an agreement. More specifically to note that: - Instead prescribing for a termination of contract (a) if a service provider subcontracts services material to the outsourcing arrangement, the market participant should be given the prerogative to consider approving the engagement of such service provider, by considering the criteria/assessments which has been made by the service provider on the proposed

	(d) require the service provider to give a copy of its business continuity program to the market participant; and (e) permit the market participant to make an annual onsite visit to the service provider's premises to assess whether it is meeting its obligations.	subcontractor, taking into consideration the type of arrangement which the subcontractor is engaged to perform. - the regulatory requirement with respect to (b) is for the Service Provider to give written notice before entering into any arrangement with a Sub-Contractor i.e. not for the market participant to grant approval to the Service Provider; - Sub-paragraphs (c), (d) and (e) are not regulatory requirements and we suggest therefore be deleted. (e) is notably problematic in the case of some global providers.
RG265.47	Market participants must monitor the performance of the service provider to ensure it is providing, and continues to provide, the services effectively: Rule 8B.2.3(1)(c). They are expected to have written supervisory procedures that set out how they will monitor and oversee the outsourced tasks provided by service providers.	We request ASIC confirm that such written supervisory procedures may be part of an overall framework (eg. an Outsourcing framework) rather than at the service provider level.
RG265.50	They should have measures for the service provider to identify, record, and remediate instances of failure to meet contractual obligations or unsatisfactory performance and to report such instances in a timely manner	We request that ASIC clarify that this reporting is between the service provider and the Participant; rather than externally to the regulator.
RG265.52	Market participants must also have in place adequate arrangements to identify and manage any conflicts of interest which have been identified or could arise between the participant and the service provider: Rule 8B.2.3(1)(d). This includes any conflicts involving sub-contractors and related entities of the service provider.	We seek clarity on the guidance's extension to the MIR requirements. We request that ASIC provide some examples of perceived conflicts of interest between a participant and a sub-contractor and / or related entities of a service provider and how they expect these to be identified and managed.
RG265.54	The access arrangements should be tested from time to time to ensure that access and the information are readily accessible as expected.	To clarify if control validation of the access management is acceptable as opposed to testing by the Market Participant.

RG265.56	Where the outsourced tasks do not relate to critical business services, we encourage market participants to consider the appropriateness of applying the principles in Rule 8B.2.3(1) as a matter of good practice.	We support the view that the principles can be a good model for best practice, AFMA requests that it be made clearer that no obligation is created as this would be outside the scope of the new MIR's.
RG265.57	Market Participants must ensure, for each outsourcing arrangement, the participant's board or a director or senior manager have confirmed that they have complied with the participant's obligations in Rule 8B.2.3(1) and made a written attestation to that effect: Rule 8B.2.3(1)(h).	AFMA requests that this may be conducted at a local governance level e.g. a local Outsourcing committee or forum. As a matter of efficiency AFMA suggests that if it can be demonstrated by a participant that its outsourcing framework addresses all of ASIC's requirements, then this confirmation should not be required for each individual outsourcing service arrangement.
RG265.58	The written attestation should be made each time a market participant enters into a new outsourcing arrangement with a service provider. This includes when a market participant renews an existing outsourcing arrangement with a service provider.	AFMA does not support a re-attestation requirement where there is no material change to the terms of an existing outsourcing arrangement, for example the renewal is only an extension of the expiration date of outsourcing arrangement as per the contract? In any event we request that ASIC confirm that this guidance does not apply in relation to existing outsourcing agreements entered into prior to March 2023 until they are renewed.
RG265.60	Outsourcing involving cloud computing services	For transparency purposes, reference to expectations around cloud services should be made within the regulatory requirements rather than being embedded in regulatory guidance.
RG265.62	Rules 8B.3.1(1) and (2) require market participants to have adequate arrangements to ensure the confidentiality, integrity and availability of information obtained, held or used by the market participant in relation to its operations and services. This includes: (a) arrangements to identify and document information assets that are integral to the provision of the participant's operations and services; and (b) adequate controls (including automated controls) to prevent unauthorised access,	Consistent with our previously noted concerns around the MIRs, the drafting should reflect that while firms should make reasonable efforts in relation to controls, as ASIC is well aware, there can be no guarantee that systems will prevent access. The drafting should reflect this by replacing the word ensure with alternate wording.

	and to identify, assess, manage and monitor for unauthorised access, to information assets. The arrangements must be designed to prevent the theft, loss or corruption of information assets. This helps to address increasing concerns relating to cyber-attacks and privacy requirements.	
RG 265.79	Market participants must have adequate arrangements to provide for the back up and timely recovery of data obtained, held, or used by the market participant in the event of any theft, loss or corruption of the data: Rule 8B.3.1(4). Adequate arrangements include, but are not limited to: (a) data backups that mirror data stored in the primary data centre; (b) geographically separate secondary data centres and/or off-site storage; (c) assessment of the geographical area risks of the secondary data centre; (d) penetration testing of the backup site to prevent backups from compromise; and (e) technical recovery tests to ensure data backups can be recovered.	We request ASIC please confirm that these are just examples of arrangements that the market participant may consider. If these are required, are ASIC specifically requiring penetration tests of back up tapes, or is it sufficient to demonstrate alternate controls are in place such as encryption of back up tapes? We suggest further discussion with industry to further clarify expectations and definitions.
RG265.89	Market participants should establish backup sites for critical operations that have the same basic capabilities of primary sites. Market participants should also consider the need for geographic diversity of backup sites	Has ASIC considered alternative resiliency strategies outside of back up sites such as remote working? Post-COVID many firms consider alternate sites for trading and operational staff differently to data centre sites where primary and secondary physical sites are maintained due to hardware requirements. Having staff working from home as their ‘’alternate” site has become to be considered a resilient and workable option. AFMA suggests coordination and alignment of some terms with ASX GN10. We would like confirm our understanding that critical operations is the same as critical business services.
RG265.93	Market participants must notify ASIC immediately on becoming aware of a major event: Rule 8B.4.1(6). We also request that ASIC be notified when operations return to normal.	ASIC’s priority should be supporting firms responding to incidents, rather than creating bureaucratic requirements and risk. ASIC is not well placed to support firm’s systems and the immediate notification requirement

		detracts from the ability of firms to respond. In the context of a cyber event, a short window for breach notification means firms are not given proper time and focus to understand, remediate and mitigate the impacts of an incident. We propose establishing a feasible incident reporting timeline of at least 72 hours, that are commensurate with corresponding incident severity levels and in alignment with global best practices, enabling firms to focus on responding appropriately to incidents and providing more pertinent and contextualised information to the Government. Further we note the terms "immediately on becoming aware" and "when operations return to normal" are not defined.
RG265.94	RG 265.94 The market participant must also give ASIC a written report within seven days. The report must set out the circumstances and the steps taken by the participant to respond to the major event: Rule 8B.4.1(7). The following elements should be set out in the report:	A major cyber event could involve, for example, having to perform forensics on a large number of servers which would take many months to complete. New findings that emerge during the process can change the impact statements and root cause analysis findings. Therefore, the timeline for the written report should take into consideration the type of information required for reporting. Additional time would allow the firm to provide more contextualised information to the Government. A 7-day period might only be possible for a "summary of facts known at the time" on a reasonable resource-constrained basis and should not be treated as the final report on the cyber incident nor should it create any liability.
RG265.97	Testing scenarios should be designed to cover a variety of major events and recovery scenarios. This should go beyond partial scenarios, where only specific components of business continuity plans are tested. For example, off-site tests that involve switching off the main system to operate the backup system will not suffice. Tests should incorporate full scale	AFMA suggests that the requirement might benefit from redrafting to reinforce that it is principles-based and not prescriptive. Testing of the suggested nature would take time to develop (ie. beyond March 2023) given the global nature of some banks businesses and associated critical business services.

	simulated 'real life, end-to-end' scenarios that test all aspects of the business continuity plan, including the initial response and invocation, recovery and continuity, and return to normal operation phases.	We suggest ASIC work with the industry to develop understanding of expectations in this area.
RG265.99	We also expect market participants reviewing their business continuity plans to conduct small-scale exercises to improve and increase understanding and effectiveness within the business.	Similarly, further engagement to understand this expectation is requested.
MIR 8B.2.3(3)	the Participant must take into account the extent to which the Service Provider is providing the same or similar services to other Participants	This information is generally commercially sensitive and may not always be available from a service provider. This should not be a requirement on the MIR.
MIR 8B.3.1 (5)	(5) A Participant must maintain, for a period of at least seven years after the relevant event, records of any: (a) unauthorised access to or use of its Critical Business Services that impacts the effective operation or delivery of those services; or (b) unauthorised access to or use of market-sensitive, confidential or personal information.	We seek further guidance on the expectation around IT log retention. It can take time for an organisation to uncover unauthorised access. Does the new rule imply all critical service/applications should keep the user activity logs for min. 7 years? Retention periods for user activity logs is often not kept past 200 days. Anything further would require an immense data storage capacity. Does the rule operate only following actual knowledge of unauthorised access having occurred?
172.34	Market participants should have appropriate testing arrangements to ensure that their critical business services are functional and reliable. The testing methodologies should be designed to ensure: (a) the operation of the critical business service complies with relevant regulatory obligations; (b) controls embedded in the critical business service work as intended; and (c) critical business service can continue to work effectively in stressed market conditions.	Testing can never fully ensure outcomes; therefore the drafting might be more accurate to be phrased "should be designed to support the following aims"