REPORT 719

Response to submissions on CP 314 Market integrity rules for technological and operational resilience

March 2022

About this report

This report highlights the key issues that arose out of the submissions received on Consultation Paper 314 *Market integrity rules for technological and operational resilience* (CP 314) and details our responses to those issues.

About ASIC regulatory documents

In administering legislation ASIC issues the following types of regulatory documents.

Consultation papers: seek feedback from stakeholders on matters ASIC is considering, such as proposed relief or proposed regulatory guidance.

Regulatory guides: give guidance to regulated entities by:

- explaining when and how ASIC will exercise specific powers under legislation (primarily the Corporations Act)
- explaining how ASIC interprets the law
- describing the principles underlying ASIC's approach
- giving practical guidance (e.g. describing the steps of a process such as applying for a licence or giving practical examples of how regulated entities may decide to meet their obligations).

Information sheets: provide concise guidance on a specific process or compliance issue or an overview of detailed guidance.

Reports: describe ASIC compliance or relief activity or the results of a research project.

Disclaimer

This report does not constitute legal advice. We encourage you to seek your own professional advice to find out how the Corporations Act and other applicable laws apply to you, as it is your responsibility to determine your obligations.

This report does not contain ASIC policy. Please see:

- Regulatory Guide 172 *Financial markets: Domestic and overseas operators* (RG 172);
- Regulatory Guide 265 *Guidance on ASIC market integrity rules for participants of securities markets* (RG 265); and
- Regulatory Guide 266 *Guidance on ASIC market integrity rules for participants of futures markets* (RG 266).

Contents

A Overview and consultation process

1 In Consultation Paper 314 *Market integrity rules for technological and operational resilience* (CP 314), we consulted on proposals to introduce market integrity rules for market operators and market participants, to ensure the resilience of their critical systems. These proposed rules would be part of the *ASIC Market Integrity Rules (Securities Markets) 2017* and the *ASIC Market Integrity Rules (Futures Markets) 2017*.

2 The proposed rules that we consulted on would require market operators and their market participants to:

(a) have adequate arrangements in place to ensure the resilience, reliability, integrity and security of their critical systems;

(b) ensure their arrangements for critical systems continue to remain adequate following the implementation of a new critical system or a change to an existing critical system;

(c) ensure that outsourcing arrangements in relation to their critical systems include appropriate controls;

(d) have adequate arrangements to ensure the confidentiality, integrity and security of data obtained, held or used;

(e) establish, maintain and implement plans for dealing with an unexpected interruption to the usual operation of their critical systems and for dealing with an emergency or other event that causes significant disruption to operations and services; and

(f) have appropriate governance arrangements and adequate financial, technological and human resources to support the arrangements contained in the above proposals.

3 The proposed rules would also require market operators to:

(a) provide access to the market and other services they provide on reasonable commercial terms and on a non-discriminatory basis; and

(b) have controls that enable immediate suspension, limitation or prohibition of the entry by a market participant of trading messages.

4 This report highlights the key issues that arose from the submissions received on CP 314 and our responses to those issues.

5 This report is not meant to be a comprehensive summary of all responses received. It is also not intended to be a detailed report on every question from CP 314. We have limited this report to the key issues.

6 We received 10 confidential and 12 non-confidential responses to CP 314. Responses came from a range of interested parties, including market operators, market participants, data service providers, professional and industry bodies, and members of the public. We are grateful to respondents for taking the time to send us their comments.

7 For a list of the non-confidential respondents to CP 314, see the appendix. Copies of these submissions are currently on the CP 314 page on the ASIC website.

Responses to consultation

8 Generally, the respondents recognised the importance of ensuring resilient market operators and market participants. They were broadly supportive of the proposed rules.

9 The main issues raised by the respondents related to those proposals in CP 314 that would require market operators and market participants to:

(a) comply with new requirements for critical systems arrangements;

(b) meet new contractual, review, approval, notification and oversight requirements for outsourcing arrangements;

(c) implement regular testing for business continuity plans and incident management plans; and

(d) establish appropriate board and senior management oversight of governance arrangements.

10 The other issues raised by respondents related to the market operator proposals which would require a market operator to:

(a) provide fair access to their market, services, data, and associated products; and

(b) implement automated trading controls.

Alignment with APRA standards

11 The Australian Prudential Regulation Authority (APRA) is currently conducting a comprehensive review of its prudential requirements for operational resilience. This is expected to include revisions to the existing Prudential Standard CPS 231 *Outsourcing* (CPS 231) and Prudential Standard CPS 232 *Business continuity management* (CPS 232) and set expectations for operational risk management.

12 These standards will form part of a suite of standards covering operational resilience, which also includes Prudential Standard CPS 234 *Information security* (CPS 234), which was updated in 2019.

13 Since we released CP 314, we have continued to work with APRA to align our proposed rules and APRA standards. As a result of this process, we have made some minor amendments to the drafting of our proposed rules, which we have also highlighted in this report.

Implementation and transition period

14 As a result of industry feedback, we have extended the initially proposed six-month transition period to 12 months from the date the rules are made. In large part, this change responds to submissions that more time is needed to update legal agreements for outsourcing arrangements to meet the new requirements. This extended transition period will also provide additional time for market operators and market participants to make changes to their processes and controls to comply with the rules. The extension also recognises that progress may be slower in the current COVID-19 pandemic environment.

15 We will also update the guidance in Regulatory Guide 265 *Guidance on ASIC market integrity rules for participants of securities markets* (RG 265), Regulatory Guide 266 *Guidance on ASIC market integrity rules for participants of futures markets* (RG 266) and Regulatory Guide 172 *Financial markets: Domestic and overseas operators* (RG 172). The updated guidance is informed by the feedback we received on CP 314 and further explains the approach and scope of the rules, and our expectations of how the guidance may apply in practice.

B Rules for market operators and market participants

Key points

This section outlines the key issues highlighted by the submissions in relation to our proposed rules in CP 314, including:

- having adequate arrangements in place to ensure the resilience, reliability, integrity and security of their critical systems;
- ensuring arrangements for critical systems continue to remain adequate following the implementation of a new critical system or a change to an existing critical system;
- ensuring that outsourcing arrangements in relation to their critical systems include appropriate controls;
- having adequate arrangements to ensure the confidentiality, integrity and security of data obtained, held or used;
- establishing, maintaining and implementing plans for dealing with an unexpected interruption to the usual operation of their critical systems and for dealing with an emergency or other event that causes significant disruption to operations and services; and
- having appropriate governance arrangements and adequate financial, technological and human resources to support the arrangements contained in the above proposals.

In addition, for market operators:

- providing access to the market and other services they provide on reasonable commercial terms and on a non-discriminatory basis; and
- having controls that enable immediate suspension, limitation or prohibition of the entry by a market participant of trading messages.

This section also includes our responses to the feedback received.

Critical systems arrangements

16 In CP 314, we sought feedback on the proposal to introduce the concept of 'critical system' to the market integrity rules and set out arrangements for managing these critical systems. We considered that a system in this context includes infrastructure, functions, and processes, including the technological systems of a market operator or a market participant.

17 The proposed arrangements required market operators and market participants to have adequate arrangements to ensure the resilience,

reliability, integrity and security of their critical systems and to review, test and regularly update these arrangements for their critical systems.

18 We received 19 submissions on this proposal. The majority of those submissions provided full or in-principle support to the proposal, recognising the importance of adequate arrangements for safeguarding the resilience, reliability, integrity and security of critical systems.

19 However, several submissions expressed concerns with the proposed definition of critical systems. They were concerned that it was too broad, and could be interpreted to capture a multitude of systems that would make the associated obligations difficult to meet. One respondent suggested that market participants should have the flexibility to determine which systems are 'critical' to their business subject to a materiality test they determine.

20 Two submissions suggested the definition should be more aligned with international standards. Other submissions requested clarification and further guidance on the definition of critical system and what constitutes a 'critical system'.

21 In relation to the requirement to have adequate arrangements for critical systems, several respondents, although broadly supportive of the proposal, expressed concern with the use of the word 'ensure'. One respondent was concerned that requiring 'adequate arrangements to ensure the resilience, reliability and integrity of its critical systems' meant that a failure of a system would automatically mean that their critical system arrangements were inadequate and therefore in breach of the proposed rule.

22 One market operator respondent did not support the introduction of the adequate arrangements requirement. It considered that these requirements already existed for market operators under the existing regulatory framework.

ASIC's response

We have introduced rules that require market operators and market participants to have in place adequate arrangements for critical systems.

We have carefully considered feedback that the definition of 'critical system' is too broad and have decided not to make any changes to the definition. We think that 'functions, infrastructure, processes or systems' reflects the whole of the operation of an entity and the totality of resources, skills, controls and systems required to be resilient from operational disruptions.

The COVID-19 pandemic has highlighted that human resources and expertise, processes and controls are as critical as information technology (IT) systems in ensuring operational resilience.

However, to ensure consistency with international standards and APRA standards on operational risk management, we have replaced the term 'critical systems' with 'critical business services'. The term 'critical systems arrangements' has also been replaced with 'critical business services arrangements'.

We have considered the feedback about the lack of certainty about the interpretation and application of the rules.

As a result, we will clarify in RG 265, RG 266 and RG 172 that these rules are intended to be scalable. What is considered a critical business service is dependent on the size and complexity of the market operator or market participant's business. We will also provide examples of the types of critical business services intended to be captured by these rules.

We have also carefully considered feedback about inclusion of the word 'ensure' in the adequate arrangements requirement.

The term 'ensure' is relatively standard language in ASIC market integrity rules. Further, the current drafting of this rule does not suggest that failure of a critical business service automatically means a market operator or market participant has failed to have adequate arrangements. This rule requires entities to demonstrate they have adequate arrangements to avoid failures. If a failure occurs, entities should be able to demonstrate they had adequate arrangements to deal with a failure.

Change management of critical systems

23 In CP 314, we sought feedback on proposed rules to require market operators and market participants to have adequate arrangements to ensure the continued resilience, reliability, integrity and security of their critical systems following the implementation of a new critical system or a change to an existing critical system.

24 We received 15 submissions on this proposal. A majority of those submissions provided full or in-principle support to the proposal, recognising that change management of critical systems is an important responsibility.

25 Three respondents considered, to varying degrees, that ASIC's existing regulatory framework already adequately dealt with change management. One of these respondents considered that while formal change management rules may be warranted for market operators, they are not warranted for market participants.

26 The second respondent considered that the existing regulatory framework for change management was already adequate for market operators.

27 The third respondent, although they agreed in principle with the change management requirements for market operators and market participants, did not think they were required for clearing and settlement participants. This is because there have been no market failures that justify regulatory intervention, and because of pre-existing requirements in ASX operating rules and guidance.

28 Some submissions considered that as the requirement covers every change to a critical system, it could lead to notification fatigue and issues with resourcing. As such, it was suggested that there should be materiality thresholds for any change management requirements of critical systems. One respondent had the view that notification requirements should not apply to minor changes or changes to ancillary systems, but only to those that are material.

29 One submission considered that, while market operators should communicate significant changes before implementation, and also provide appropriate testing environments, the proposed rule was too prescriptive. It noted that, in some cases, it may be appropriate for a large project to proceed even if not every market participant is fully ready.

ASIC's response

We have introduced rules that require market operators and market participants to have in place adequate arrangements for change management of their critical business services.

We consider that the current regulatory framework has fallen below international standards, particularly the recommendations of the International Organization of Securities Commissions (IOSCO) and best practices. The current regulatory framework may be insufficient to mitigate the risk of failure of critical business services.

In response to feedback that these proposed rules should not apply to settlement and clearing participants, we note that the rules apply to market participants only.

As a result of feedback about notification fatigue and constraints on resources, we have amended the proposed rule so that testing is only required for *new* critical business services or *material changes* to existing critical business services. This change also aligns this rule more closely with CPS 232, which requires testing of business continuity plans at least annually, or more frequently if there are material changes to business operations.

We consider these changes will still result in market operators and market participants having appropriate testing arrangements to ensure that their critical business services are functional and reliable.

We will provide guidance on our expectations, along with examples of material changes that would require appropriate testing in RG 265, RG 266 and RG 172.

Outsourcing critical systems

30 In CP 314, we sought feedback on the proposal to establish a framework regulating critical system outsourcing arrangements.

31 We received 20 submissions on this proposal. The majority of the submissions agreed in principle that market operators and market participants should have adequate outsourcing arrangements.

32 There was agreement from respondents that responsibility should lie with market operators and market participants, even when functions are outsourced. One respondent noted it is undesirable for outsourced arrangements to be subcontracted by a service provider to a third party.

33 Broadly, respondents that did not agree with the proposed rule were concerned:

(a) by ASIC's definition of outsourcing arrangements, and that the broad scope of the rule had the potential to capture a wide range of services;

(b) that outsourcing requirements are already covered in the existing regulatory framework, including in Regulatory Guide 104 *AFS licensing: Meeting the general obligations* (RG 104); and

(c) about inconsistency with other regulatory requirements, particularly with CPS 231, and incompatibility with international standards.

34 One submission held the view that this proposed rule should not apply to market participants, particularly principal traders.

35 Respondents also expressed concern with the requirement to ensure outsourcing arrangements are contained in 'legally binding written contracts'. They were concerned about the likely need for market operators and market participants to renegotiate terms with existing vendors to comply with these new obligations, and also the costs associated with this.

36 Specifically, there was concern that the requirement for a 'legally binding written contract' was not appropriate for group entities providing services under service level agreements. One respondent believed that this requirement failed to account for the contractual frameworks used by cloud service providers.

37 Other specific issues raised by the submissions that opposed the proposed rules related to the following requirements and concerns:

(a) the requirement for written attestation by the board and senior management, confirming compliance with the proposed rules. Respondents were concerned that the proposal required inappropriate involvement of the board and extended beyond the scope of their governance oversight;

(b) the requirement to obtain approval from market operators and market participants prior to subcontracting of services by the service provider. Respondents suggested that the approval requirement should be replaced with a notification requirement; and

(c) the requirement to ensure auditors and ASIC have access to records held by a service provider. This requirement was considered unfeasible by one respondent.

38 Two submissions opposed the proposed rule requiring market operators only to provide written notification to ASIC before entering into an outsourcing agreement. They considered that this may not be practicable, due to reasons of timing or commercial confidentiality.

39 We also consulted on whether the risks associated with outsourcing to the cloud required a rule specific to this type of outsourcing arrangement. Some respondents supported a cloud-specific rule, with the view that the increasing use of the cloud and risks associated with outsourcing warranted cloud-specific rules. However, most submissions did not share this view. These respondents considered that general outsourcing rules were adequate for this issue and that a cloud-specific rule could create duplicate regulatory requirements.

ASIC's response

We have proceeded with the proposal to introduce rules that require market operators and market participants to have in place a framework for managing outsourcing arrangements in relation to critical business services. We consider that these requirements are necessary to strengthen the technological and operational resilience of market operators and market participants.

We have carefully considered the feedback, and as a result have changed:

- the requirement for a 'legally binding written contract' to 'documented legally binding agreement' to include intra-group service agreements and to align with CPS 231;
- the requirement for written attestation by the 'board and senior management' to 'board, director or senior manager' to address concerns from respondents that requiring attestations from both the board and senior management is too burdensome. It is our view that this will also ensure individual accountability for completing the attestation;
- the requirement for service providers to obtain 'written approval' from market operators and market participants, to a requirement for service providers to provide 'written notification' before subcontracting or making material changes to the manner in which outsourced services are provided; and

- the requirement for market operators to notify ASIC before entering into outsourcing arrangements to as soon as practicable after entry into an outsourcing arrangement, and in any event within 20 business days, to align with CPS 231.

We have also considered the requirement for market operators and market participants to have arrangements with the service provider to ensure the confidentiality, integrity and availability of data. To ensure consistency with CPS 234 we have:

- replaced the term 'data' with 'information' and defined 'information asset' as including software, hardware and data (both soft and hard copy); and
- changed the requirement to ensure the 'confidentiality, integrity and security' of data, to a requirement to ensure the 'confidentiality, integrity and availability' of information.

We also considered the feedback in relation to the scope of outsourcing arrangements and have agreed to provide guidance in RG 265, RG 266 and RG 172 on the scope of services that would be covered under the updated rules.

We have carefully considered the feedback in relation to a cloud-specific rule on outsourcing and formed the view that at this time this is not necessary.

Risk management—Data and cyber risk

40 In CP 314, we sought feedback on the proposal to introduce rules that require market operators and market participants to have adequate arrangements to ensure the confidentiality, integrity and security of data obtained, held or used.

41 We received 15 submissions on this proposal. Most of the submissions either agreed, or agreed in principle, with the proposed rules and supported the introduction of a more comprehensive regulatory framework in relation to data.

42 Some submissions were concerned about:

(a) the regulatory overlap between APRA and ASIC, including in relation to CPS 234; and

(b) the use of the word 'ensure'. The view was that requiring 'adequate arrangements to ensure the confidentiality, integrity and availability of information' was too high a threshold to comply with.

43 One respondent suggested that the rule should only apply to data that is 'market sensitive, confidential or personal', rather than data 'obtained, held or used'.

44 This proposal included a requirement for market operators only to notify ASIC as soon as practicable of a data breach. One market operator respondent, although supportive of the proposal, considered that notification should only be required once the nature of the impact of the incident is known.

45 We also consulted on whether the requirement to notify ASIC of a data breach should extend to market participants. Of the respondents who provided comment:

(a) four respondents supported extending the notification requirement to market participants; and

(b) five respondents held the view that existing requirements concerning data breach notifications were sufficient, and that additional requirements would be of limited benefit.

ASIC's response

We have proceeded with the proposal to introduce rules that require market operators and market participants to have in place adequate arrangements to ensure the confidentiality, integrity and security of data obtained, held or used.

However, we made the following changes to the rules to align with CPS 234:

- replaced the term 'data' with 'information' and defined 'information asset' as including software, hardware and data (both soft and hard copy);
- replaced 'confidentiality, integrity and security' of data with 'confidentiality, integrity and availability' of information;
- added a requirement for information security arrangements to identify and document information assets that are integral to the provision of operations and services by market operators and market participants; and
- modified the data breach notification requirements for market operators from 'as soon as practicable' to 'as soon as possible and, in any case, no later than 72 hours' on becoming aware of the unauthorised access.

We will provide guidance on our expectations and how our revised rules interact with other regulatory requirements in RG 265, RG 266 and RG 172.

We have carefully considered the feedback in relation to extending data breach notifications to market participants. We have decided not to extend this notification requirement to market participants. Market participants will be required to maintain records of any data breaches for seven years.

Incident management and business continuity arrangements

46 In CP 314, we sought feedback on the proposal to introduce rules that require market operators and market participants to establish, maintain and implement:

(a) incident management plans for dealing with unexpected interruptions to the usual operations of their critical systems; and

(b) business continuity plans for dealing with an emergency or major event that causes significant disruption to market-related operations and services.

47 We received 19 submissions on this proposal. The majority of the submissions provided full or in-principle support for the proposed rules.

48 Most of the submissions agreed with the definition of a 'major event' and the requirement for market operators and market participants to have business continuity plans for dealing with a major event.

49 In contrast, several submissions did not agree with the definition of 'incident' and the proposed requirement to have an incident management plan. One respondent suggested that such a plan would be beyond what could reasonably be achieved by many market participants, from a financial and practical standpoint.

50 Another respondent held the view that the breadth of the term 'incident' may result in the rule capturing substantially more incidents than intended and justified on a reasonable cost-benefit analysis, resulting in increased regulatory burden.

51 One respondent considered that both the terms 'major event' and 'incident' were similarly vague or so broad that it was difficult to understand what was required.

52 One market operator submission also disagreed with the incident management plan requirement. It observed that the proposed obligations were broad and uncertain, and already covered by the existing regulatory regime. It also disagreed with having specific arrangements in place due to the inability to predict future events.

53 Some respondents raised concerns about the proposed requirement for market operators and market participants to notify ASIC immediately on becoming aware of an incident or major event. One respondent was of the view that their priority should be to respond to the event rather than notify ASIC. Another respondent had the view that their priority was to advise affected users.

54 Most respondents agreed with the proposed requirement for market operators and market participants to review and test their plans. Although some

respondents agreed with the proposed frequency, some considered the proposed frequency of reviewing and testing onerous and potentially costly.

55 In particular, market operator respondents held the view that the requirement for market operators to conduct quarterly testing would be resource intensive and could potentially carry operational risks. It was suggested that an annual testing frequency for market operators would be more appropriate.

56 In contrast, another submission recommended that ASIC establish a two-tiered continuous monitoring requirement, to flag incidents and identify systemic risks on a real-time basis.

ASIC's response

We have introduced rules for business continuity arrangements only.

As a result of industry feedback about the regulatory burden of having both an incident management plan and a business continuity plan, we have removed the requirement to have an incident management plan. We consider that this change is consistent with the focus on significant disruptions to services or material impacts to operations, addressed by a business continuity plan.

However, we have retained the incident notification requirement for market operators where the unexpected disruption may interfere with the fair, orderly or transparent operation of any market. We have also retained the requirement for a market operator to provide a written report to ASIC of that incident within seven days.

We have also added a requirement for a business continuity plan to contain:

- activation procedures including trigger conditions for enacting a business continuity plan; and
- procedures to ensure affected persons are adequately informed about the likely timing of the resumption of services.

As a result of feedback received about the frequency of market operator testing, we have amended the rule to require market operators to test their business continuity plans at least annually rather than 'quarterly', and to test their business continuity plans as soon as practicable after the occurrence of a major event. We consider that annual testing is already being conducted by market operators.

We have carefully considered the feedback on the requirement to notify ASIC of a major event. It is our view that this notification requirement would not significantly affect the ability of a market operator or market participant to respond to a major event.

We will not implement the recommendation to establish two-tiered continuous monitoring reporting requirements, given the potential

compliance costs that may be incurred (particularly for smaller market operators and market participants).

We will provide guidance on our expectations for complying with the proposed rules for business continuity arrangements in RG 265, RG 266 and RG 172.

Governance arrangements and adequate resources

57 In CP 314, we sought feedback on the proposal to introduce a rule that requires market operators and market participants to have governance arrangements and adequate financial, technological, and human resources to support all the arrangements outlined within the proposed rules. This included, but was not limited to, oversight by the board and senior management of the establishment, maintenance and implementation of incident management and business continuity arrangements.

58 We received 13 submissions on this proposal. Almost all of the submissions provided full or in-principle support for the proposed rule.

59 The respondents who were not in full support of the proposal disagreed with the requirement that both the board and senior management should have overall oversight of the incident management plan and business continuity plan. One respondent held the view that board involvement would result in burdensome compliance costs, particularly for offshore boards. Another respondent proposed that the responsibility for oversight should be with a nominated person that has the relevant expertise (e.g. the Chief Information Officer), rather than the board.

60 A few submissions considered that it was unclear what would constitute 'adequate' resourcing and that guidance on ASIC's expectations of what would constitute appropriate and effective board oversight would be helpful.

ASIC's response

We have introduced rules requiring market operators and market participants to have adequate governance arrangements and resourcing.

In response to feedback, we have replaced the requirement for 'board *and* senior management' oversight to 'board *or* senior management' oversight.

We have removed the obligation requiring oversight of incident management plans, consistent with ASIC's intention to remove the requirement for market participants and market operators to have incident management plans.

We will provide guidance on our expectations for governance arrangements and adequacy of financial, technological, and human resources in RG 265, RG 266 and RG 172.

Fair access to the market—Market operator rule only

61 In CP 314, we sought feedback on the proposal to introduce a rule that requires market operators to provide access to their market and services on reasonable commercial terms and on a non-discriminatory basis.

62 This approach aligns with international practice and would ensure we have an adequate enforceable framework for matters arising as markets continue to innovate and develop their systems, technology and services.

63 We received 12 submissions on this proposal from market participants, industry bodies and market operators. Almost all respondents supported the proposal to have a rule requiring market operators to provide fair access to their market and services.

64 In particular, one submission considered that the proposed rule would be beneficial for market functioning and would prevent market operators in a dominant market position from restricting competition and innovation in the marketplace.

65 Two submissions were of the view that the existing framework was sufficient. One of these submissions considered that there was no regulatory gap to fill and that the proposed rule would be a significant new regulatory intervention. It further considered that the proposal extended beyond current ASIC guidance and would overlap and potentially conflict with existing competition laws. The same submission raised concerns that 'data' could be broadly interpreted and goes beyond the scope of what the rule intended to capture.

66 Although it agreed in principle with the proposal, another submission considered this to be a complex area which should be deferred for more detailed consideration.

67 Some submissions requested further guidance on key definitions such as 'reasonable commercial terms'.

ASIC's response

We have considered the feedback that the existing framework is sufficient and, as such, a rule is unnecessary. However, we are of the view that a fair access rule is likely necessary to prevent the use of discriminatory access requirements as a competitive tool.

ASIC has a competition mandate, which requires us to consider the effect that our work and the exercise of ASIC's powers will have on competition in the financial system. The proposed rule on fair access supports and is consistent with this mandate.

Considering the feedback, we intend to further consult with industry and the Australian Competition Consumer Commission.

We also intend to further consider the appropriate drafting of this rule, particularly as it relates to data.

Since the release of CP 314, IOSCO's Committee on Regulation of Secondary Markets (Committee 2) has issued Consultation Report CR03/2020 *Market data in the secondary equity markets* (PDF 288 KB).

This report sought feedback on the market data necessary to facilitate trading in today's markets (i.e. what is considered 'core' data) and how to ensure fair, equitable and timely access to that market data. It is anticipated that IOSCO will publish its findings in the first half of 2022.

Given the relevance of CR03/2020 to this proposal, we consider it appropriate to finalise this proposal after IOSCO has released its findings. This will ensure that the drafting of this rule aligns with IOSCO's recommendations and principles on this issue.

We will further consider and consult on this rule at a future time.

Trading controls—Market operator rule only

68 In CP 314, we sought feedback on the proposal to introduce a rule that requires market operators to implement trading controls.

69 We received seven submissions on this proposal. Most of these submissions agreed with the proposed rule.

70 One submission agreed in principle with the proposed rule, but opposed the implementation of automated controls in markets where automated order processing has not been adopted.

71 One submission noted that the current framework is sufficient but did not provide any explanation as to how the current framework is sufficient. This same respondent stated that it was likely to have the required controls in place and the impact may be minimal.

72 One submission agreed with the principle of introducing 'kill switch' functionality but wanted further consideration of the issues before the rule is made. Another submission requested guidance on the implementation of automated controls.

ASIC's response

We have proceeded with this proposal to implement trading controls for market operators. We consider it important that market operators have automated controls in place and the ability to automatically shut off trading when disruptions occur or the need arises, to ensure a fair, orderly and transparent market.

We may consider a waiver from these rules where a market operator accepts trading messages via manual order entry only. However, it is our view that all market operators should have controls (if not automated) to suspend or prohibit trading messages.

We will provide guidance on the situations where automated controls may be needed in RG 265, RG 266 and RG 172.

Appendix: List of non-confidential respondents

- Amazon Web Services, Inc
- Asia Cloud Computing Association
- ASX Limited
- Australian Financial Markets Association
- Australian Shareholders' Association Limited
- Chi-X Australia Pty Ltd (now known as Cboe Australia Pty Ltd)
- Depository Trust and Clearing Corporation
- E.L. and C. Baillieu Limited
- Euroz Securities Limited
- National Stock Exchange of Australia Limited
- Stockbrokers and Financial Advisers Association Limited
- Sydney Stock Exchange Limited