CONSULTATION PAPER 314

Market integrity rules for technological and operational resilience

June 2019

About this paper

This consultation paper seeks feedback on proposed market integrity rules for securities and futures market operators and market participants to promote the resilience of their critical systems.

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.

Document history

This paper was issued on 27 June 2019 and is based on the Corporations Act as at the date of issue.

Disclaimer

The proposals, explanations and examples in this paper do not constitute legal advice. They are also at a preliminary stage only. Our conclusions and views may change as a result of the comments we receive, or as other circumstances change.

Contents

The consultation process

You are invited to comment on the proposals in this paper, which are only an indication of the approach we may take and are not our final policy.

As well as responding to the specific proposals and questions, we also ask you to describe any alternative approaches you think would achieve our objectives.

We are keen to fully understand and assess the financial and other impacts of our proposals and any alternative approaches. Therefore, we ask you to comment on:

- the likely compliance costs;
- the likely effect on competition; and
- other impacts, costs and benefits.

Where possible, we are seeking both quantitative and qualitative information.

We are also keen to hear from you on any other issues you consider important.

Your comments will help us develop our policy on rules for the maintenance and recovery of critical systems. In particular, any information about compliance costs, impacts on competition and other impacts, costs and benefits will be taken into account if we prepare a Regulation Impact Statement: see Section C, 'Regulatory and financial impact'.

Making a submission

You may choose to remain anonymous or use an alias when making a submission. However, if you do remain anonymous we will not be able to contact you to discuss your submission should we need to.

Please note we will not treat your submission as confidential unless you specifically request that we treat the whole or part of it (such as any personal or financial information) as confidential.

Please refer to our privacy policy for more information about how we handle personal information, your rights to seek access to and correct personal information, and your right to complain about breaches of privacy by ASIC.

Comments should be sent by 9 August 2019 to:

Andrew McPherson
Senior Specialist
Market Infrastructure
Australian Securities and Investments Commission
Level 5, 100 Market Street, Sydney, NSW 2000
Email: rules.resilience@asic.gov.au

What will happen next?

Stage 1	27 June 2019	ASIC consultation paper released
Stage 2	9 August 2019	Comments due on the consultation paper
Stage 3	November–December 2019	Consultation response ASIC market integrity rules to be released

A Purpose of the proposed rules

Key points

Resilient market operators and market participants are essential to the integrity of our securities and futures markets and to the efficient functioning of the economy.

We propose market integrity rules for market operators and market participants to ensure the resilience of their critical systems, which include functions, infrastructure, processes, and technological and other systems.

The proposed market integrity rules apply to both the securities and futures markets and address the following key areas:

- change management in relation to implementing new critical systems or changing existing critical systems;
- outsourcing;
- risk management, and data and cybersecurity;
- incident management and business continuity planning;
- governance and resourcing; and
- fair access to markets and trading controls.

The proposed rules are consistent with international standards and clarify and strengthen existing obligations for market operators and market participants.

The draft rules are available on our consultation papers webpage under CP 314.

1 Financial markets play a central role in the growth and prosperity of our economy. They facilitate capital raising for businesses to grow and they facilitate the efficient allocation of resources and risks within the economy.

2 This process is most effective when markets operate with integrity and efficiency. The integrity of the Australian market has been key to our success in attracting international capital, which has helped to fuel economic growth.

Technological developments

3 Over the past decade, there have been significant changes in the technology and associated processes underpinning financial markets, as well as the nature of users and how they interact with financial markets. For example, we have seen:

(a) continued advancements in automation across the financial market—systems such as those used for trading, order management, company

announcements and surveillance have become increasingly automated, interconnected and complex. The use and complexity of algorithmic trading has also increased;

(b) an exponential increase in the volume, complexity and use of data that has become critical to the effective operation of markets and participants;

(c) continued financial technology (fintech) disruption with an increase in digital services (such as online trading, robotic advice and cloud computing services) being offered, and the introduction of new capital raising approaches such as crowdfunding and initial coin offerings.

4 Failures of critical systems can have a severe impact on market integrity. For example, 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.

5 The multi-market environment for Australian listed securities creates interdependencies between market participants and market operators. The ASX equity market outage that occurred in September 2016 (ASX outage) created a ripple effect that affected the operation of the Chi-X market and participants' access to Chi-X, as well as the operation of crossing systems. It also caused considerable uncertainty among market users, stifling trading volumes on the day and impacting trading revenues across the market.

6 Outsourcing and off-shoring of critical systems is becoming more prevalent. They provide the potential for efficiencies and better systems and services, and they can free up capacity for an entity to stay focused on its core business. However, they can introduce additional risks that need to be managed.

7 Cyber risk also continues to be a key concern across the financial market, with cyber attacks increasing in frequency and sophistication. The protection of data—in particular sensitive, confidential or personal data—is critical for the sound operation of the market and to facilitate investor trust and confidence in the market. There have been many instances in Australia and abroad of confidential client information being compromised.

ASIC's assessments of ASX

8 In late 2016, we conducted an extensive review of how ASX and various stakeholders responded to the ASX outage in September 2016. We liaised with Chi-X, market participants, fund managers and data vendors, and drew on perspectives from regulators in major jurisdictions.

9 In Report 509 *Review of the ASX equity market outage on 19 September 2016* (REP 509), we provided a whole-of-market perspective of the impact of the ASX outage and highlighted a number of recommendations designed to support the resilience and robustness of the Australian equity market. The recommendations included, for example, strengthening business continuity and disaster recovery, system testing and a review of communication strategies. We also advised we would undertake a wider, non-incident-driven review in 2017 of the operational and technological risk management arrangements across ASX Group.

10 In 2017, we undertook a more extensive review of ASX's technology and operational risk framework with the assistance of KPMG and working closely with the Reserve Bank of Australia (RBA). The review benchmarked ASX Group's practices and arrangements against internationally recognised technology governance and risk management standards. In 2018, we published Report 592 *Review of ASX Group's technology governance and operational risk management standards* (REP 592). The report included observations, findings and recommendations from the review as well as a number of associated observations from our ongoing oversight of ASX Group's market and clearing and settlement facility licensees. Many of the findings and recommendations, including the need to evaluate the maturity and effectiveness of risk management frameworks and arrangements for technology governance and incident management, are relevant to other financial institutions regulated by ASIC.

11 There have been a number of other incidents that have impacted the operation of ASX or ASX 24 markets and their customers. In June 2018, for example, accidental activation of the gas fire suppression system damaged some customers' hardware and their ability to trade.

International regulatory developments

12 The resilience of market operators and participants has been a key focus for regulators globally since the global financial crisis and the increased incidences of 'flash crashes' (i.e. when prices swiftly and significantly fall and rebound) in automated markets.

13 Regulators have been raising standards for the systems and controls of market operators and participants at both a jurisdictional level and through multilateral initiatives.

IOSCO

14 For example, the International Organization of Securities Commissions (IOSCO) has been active in this area. IOSCO brings together the world's securities regulators and is the global standard setter for the securities sector.

IOSCO members cooperate in developing, implementing and promoting adherence to consistent standards of regulation, oversight and enforcement in order to protect investors, maintain fair, efficient and transparent markets, and seek to address systemic risks.

15 IOSCO has issued a range of reports outlining principles for managing risks to critical systems, outsourcing and for the protection of data, including:

(a) *Cyber security in securities markets—An international perspective*, FR02/2016 (IOSCO Report FR02/2016);

(b) *Market intermediary business continuity and recovery planning*, FR32/2015 (IOSCO Report FR32/2015);

(c) *Mechanisms for trading venues to effectively manage electronic trading risks and plans for business continuity*, FR31/2015 (IOSCO Report FR31/2015);

(d) *Regulatory issues raised by the impact of technological changes on market integrity and efficiency*, final report, FR09/11 (IOSCO Report FR09/11) and corresponding consultation paper CR02/11;

(e) *Principles on outsourcing by markets*, final report, July 2009; and

(f) *Principles on outsourcing of financial services for market intermediaries*, final report, February 2005.

Other international developments

16 Examples of other international regulatory initiatives include the General Data Protection Regulation (EU) 2016/679 (GDPR). This regulation on data protection and privacy for all individuals within the European Union was implemented on 25 May 2018. The regulation requires controllers of personal data to have in place appropriate technological and organisational measures to implement the data protection principles. It has had wide-reaching implications for market operators and participants in the European Union and in Australia.

17 In the United States, the Securities and Exchange Commission introduced Regulation Systems Compliance and Integrity (Reg SCI) in 2014 to strengthen the technology infrastructure of the US securities markets. Specifically, the rules are designed to reduce the number of market disruptions stemming from system issues and improve resilience and recovery when disruptions do occur. Reg SCI requires relevant entities to establish, maintain and enforce policies and procedures to ensure their systems have levels of capacity, integrity, resilience, availability and security adequate to maintain their operational capability and promote the maintenance of fair and orderly markets.

Regulation in Australia

18 In Australia, market operators and participants, along with other Australian financial services licensees, have general obligations under the *Corporations Act 2001* (Corporations Act) to ensure they have adequate resources and risk management systems in place. We have also provided some guidance on what we look for in assessing compliance with these obligations.

Existing expectations for market operators

19 Under existing obligations for market licensees in the Corporations Act, market operators are required to do all things necessary to ensure that their market is fair, orderly and transparent (s792A(a)) and to have sufficient resources (financial, technological and human) to operate the market (s792A(d)). Beyond this, there are no specific regulatory requirements governing the technological resilience of markets.

20 Our expectations on market operator obligations, including what we consider sufficient resources, are set out in Regulatory Guide 172 *Financial markets: Domestic and overseas operators* (RG 172), which was published in 2012 and updated in 2018. We consider 'technological resources' to be a broad concept that includes the requirement to apply robust IT governance arrangements, and have adequate controls to ensure the delivery of critical services and ensure critical services are resilient to system failures and security breaches. Our expectations in RG 172 also include that market operators should:

(a) review their critical systems to ensure they function as intended, are reliable and do not pose a threat to fair and orderly trading;

(b) test for function, conformance and connectivity with each other;

(c) ensure affected stakeholders can test their systems against the licensee's modifications;

(d) have robust business continuity planning, backup and disaster recovery plans; and

(e) have arrangements for system security and proactive strategies to prevent cyber attacks.

Existing expectations for market participants

21 Under the Corporations Act, market participants are required to have:

(a) adequate resources (including financial, technological and human resources) to provide the financial services covered by the licence and to carry out supervisory arrangements (s912A(1)(d)); and

(b) adequate risk management systems (s912A(1)(h)).

Note: Section 912A(1)(h) does not apply to entities that are also authorised deposit-taking institutions (ADIs) and regulated by the Australian Prudential Regulation Authority (APRA).

22 Regulatory Guide 104 *Licensing: Meeting the general obligations* (RG 104) describes what we look for when we assess compliance with the obligations under s912A(1) of the Corporations Act, including:

(a) the requirement for adequate resources—you must have enough resources to enable you to comply with all your obligations under the law and meet your current and anticipated future operational needs; and

(b) the requirement for risk management—you must explicitly identify the risks you face and have measures in place to keep those risks to an acceptable minimum.

23 Guidance on adequate risk management systems notes that systems should:

(a) be based on a structured and systematic process that takes legal obligations into account;

(b) be able to identify and evaluate the risks that face a business;

(c) establish and maintain controls to manage and mitigate risks; and

(d) be fully implemented and monitored.

24 However, ASIC guidance does not properly address the increased risks and the systemic vulnerability arising from market operators' and market participants' growing reliance on increasingly complex, interrelated systems.

25 Market participants also have targeted obligations under the ASIC Market Integrity Rules (Securities Markets) 2017 (Securities Markets Rules) to ensure they have and maintain the necessary organisational and technical resources so that, among other things, trading messages submitted by them do not interfere with the efficiency and integrity of the market or the proper functioning of the trading platform (Rule 5.5.2).

26 Other domestic financial institutions are subject to specific requirements for technological infrastructure, business continuity, information security and outsourcing. For instance, controls in response to technological developments have been introduced for ADIs, licensed clearing and settlement facilities, trade repositories and clearing and settlement participants. A small number of market participants will be subject to those other requirements in addition to our proposed rules, and we acknowledge that there may be some overlap. We will take into account these other obligations in considering how market participants comply with our rules.

Purpose of this paper

Why is ASIC proposing rules?

27 While the provisions in the Corporations Act are broad and core system and operational risk management expectations are implied in those obligations, we believe it is important to have more specific expectations for market operators and market participants given the critical role they play in the market. With the growing reliance on technology, it is our observation that formalised baseline obligations are needed to ensure that market operators' and participants' systems and controls are adequate for their operations, to protect clients and to maintain the integrity of the market.

> Note: We have been working with market operators for several years to ensure they are adequately managing their technology risk and operational resilience. Our work has included thematic surveillances (see REP 592, REP 509 and Report 555 *Cyber resilience of firms in Australia's financial markets* (REP 555)), and ASIC surveillance of market operators and participants.

28 In addition to keeping pace with market developments, it is important that our regulatory regime aligns with international best practice. The proposed rules in this paper closely align with IOSCO principles and overseas regulation, and they respond to technological and operational threats here and abroad and supplement existing obligations in Australia.

29 By making our expectations clear in rules with associated penalties, we will enhance ASIC's enforcement toolkit in this area and, importantly, raise technological and operational risk management standards and controls.

Transitioning guidance to market integrity rules

30 The regulatory framework for market operators has historically been based on high-level principles in the Corporations Act and supplemented with relatively limited guidance. This reflects that, before the transfer of market supervision to ASIC on 1 August 2010, market operators conducted this function and were regarded as quasi-regulators.

31 Since then, markets have evolved considerably, there are competing operators and they have become commercial (demutualised) entities. It is appropriate that regulatory expectations for market operators are reflected in rules in much the same way as they are for market participants.

32 Over time, we will continue to transition expectations for market operators that currently reside in guidance into rules and, where appropriate, implement new expectations through rules. Many proposals for market operators in this consultation paper are transitioning existing expectations into rules.

Proposed rules

33 This paper seeks feedback on our proposed market integrity rules that set out requirements for critical technological and operational systems of market operators and market participants. The proposed rules are intended to clarify and strengthen the existing general obligations for market operators under s792A(a) and (d), and for market participants under s912A(1)(a) and (1)(d), of the Corporations Act as well as the Securities Markets Rules and the ASIC Market Integrity Rules (Futures Markets) 2017 (Futures Markets Rules). They will provide baseline expectations for market operators and participants, which align with international regulatory developments and IOSCO principles.

34 Under s798H(1) of the Corporations Act, operators of licensed markets and participants in those markets are required to comply with the market integrity rules for that market, breaches of which may result in penalties of up to $1 million per breach. A breach of the market integrity rules may be dealt with by ASIC on an administrative basis or civil proceedings.

35 Our proposals and the form of the draft market integrity rules are only an indication of the approach we may take and are not our final policy.

36 The proposed rules apply to:

(a) futures and securities market operators of ASX, ASX 24, Chi-X, NSX and SSX; and

(b) participants of those markets.

37 The proposed rules require that:

(a) robust arrangements are implemented and maintained to ensure the resilience, reliability, integrity and security of critical systems;

(b) change management arrangements are identified and implemented;

(c) outsourcing arrangements are implemented and managed;

(d) incidents are efficiently identified and rectified and, where appropriate, reported to ASIC in a timely and comprehensive manner;

(e) robust arrangements are implemented for business continuity management, data security, backup and disaster recovery;

(f) access to the services of market operators is provided on reasonable commercial terms and on a non-discriminatory basis; and

(g) market operators have trading controls to prevent the entry of trading messages to ensure a fair, orderly and transparent market.

38 These new and specific obligations for market operators and market participants will also:

(a) ensure consistency in approach between market operators and market participants in meeting their general obligations;

(b) provide credible deterrence for poor technology, operational governance and controls;

(c) facilitate our supervision of Australian financial markets; and

(d) better align the Australian framework with international peers.

39 Market operators and market participants will need to undertake a review of their existing arrangements to determine whether any additional arrangements need to be put in place to ensure compliance with these proposed rules. We understand that it may take time to implement the necessary arrangements and so we propose to give market operators and market participants a six-month transitional period from the date the proposed rules are made.

40 ASIC guidance in relation to general obligations for market operators and market participants is provided in RG 172 and RG 104 respectively. Guidance on market integrity rules is provided in 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). It is anticipated that these regulatory guides will be updated to reflect any implementation of the new rules.

Relevance for other financial institutions

41 While the proposed market integrity rules would apply to market operators and market participants, the proposed obligations set sound practice and could have more general application. Other financial services licensees should consider applying the principles in the rules to their business.

B Proposed rules for market operators and market participants

Key points

We propose to update the Securities Markets Rules and Futures Markets Rules to require market operators and market participants to:

- have adequate arrangements in place to ensure the resilience, reliability, integrity and security of their critical systems;
- 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;
- ensure that outsourcing arrangements in relation to their critical systems include appropriate controls;
- have adequate arrangements to ensure the confidentiality, integrity and security of data obtained, held or used;
- 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
- have appropriate governance arrangements and adequate financial, technological and human resources to support the arrangements contained in the above proposals.

In addition, for market operators we propose rules to require them to:

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

Critical systems arrangements

42 Our proposed rules introduce the concept of 'critical system' to the market integrity rules and set out arrangements for managing these critical systems. We consider that a system in this context includes infrastructure, functions, and processes, including the technological systems of a market operator or a market participant.

43 A market operator's or market participant's system is considered a 'critical system' if, in the event the system fails to operate effectively, it would (or

would be likely to) cause significant disruption to their operations or materially affect provision of their services.

44 Examples of what we consider to be critical systems include, but are not limited to, functions, infrastructure, processes and systems:

(a) for market operators—that deliver or support order entry, routing and matching, trade execution, dissemination of market data, trading risk management, market surveillance, reporting of executed trades to a clearing and settlement facility and regulatory data reporting; and

(b) for market participants—that deliver or support order acceptance, routing and entry, clearing and settlement of transactions, payments and deliveries of financial products and funds, accounting for or reconciling client money, trust accounts, financial products and funds, confirmations and regulatory data reporting.

Note: Regulatory data reporting systems refers to systems responsible for complying with market operators' and market participants' regulatory data requirements under Part 7.4 of the Securities Markets Rules.

45 Critical systems are client or market facing and exclude systems, functions, infrastructure and processes which are non-essential to the operation of the market or a market participant's capacity to deliver market services to its clients. We do not consider payroll functions and systems for reporting suspected breaches of law or an entity's policies, for example, to be critical systems.

46 The proposed rules require market operators and market participants to have adequate arrangements to ensure the resilience, reliability and security of their critical systems. These arrangements would generally include appropriate policies, procedures and organisational resources, including adequate financial, human and technological resources (e.g. system controls).

47 To ensure the continued effectiveness of these arrangements, the proposed rules require market operators and market participants to review, test and regularly update these arrangements for their critical systems to ensure they remain adequate.

Proposal

B1 We propose introducing rules that:

(a) define 'critical system' to mean functions, infrastructure, processes or systems which in the event of failure to operate effectively, would or would be likely to cause significant disruption to the market operator's or market participant's market-related operations and services;

(b) require market operators and market participants to have adequate arrangements in place to ensure the resilience, reliability, integrity and security of their critical systems;

(c) require critical systems arrangements to include:

(i) identifying the critical systems;

(ii) identifying, assessing, managing and monitoring risks to the resilience, reliability, integrity and security of the critical systems;

(iii) ensuring the critical systems have sufficient and scalable capacity for ongoing and planned operations and services;

(iv) preventing unauthorised access to or use of critical systems;

(v) managing the implementation of new critical systems and changes to existing critical systems;

(vi) dealing with an incident or major event affecting the critical systems; and

(vii) managing outsourcing arrangements in relation to critical systems;

(d) require market operators and market participants to:

(i) review their critical systems arrangements following each material change to their critical systems, and at least annually; and

(ii) change the critical systems arrangements as required to ensure they continue to comply with the above obligations; and

(e) require market operators and market participants to:

(i) document their critical systems arrangements;

(ii) document the scope and results of reviews of their critical systems arrangements;

(iii) document any changes to the critical systems arrangements; and

(iv) maintain that documentation for a period of at least seven years.

Your feedback

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

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?

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?

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.

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.

Rationale

48 Failure of a market operator's or market participant's critical systems can have far reaching repercussions for the rest of the market and for clients and can undermine the integrity of Australia's financial system. Increased interdependencies and globalisation in market infrastructure increases the risk that a disruption to a critical system will have widespread and serious effects on market operators, market participants and investors, both in Australia and in other jurisdictions. Clients of market participants can also be affected and their confidence in the market lessened where, for instance, the disruption results in inferior trade execution outcomes or delays/misallocation of securities or funds.

49 Our observations have been that, in the event of market disruptions, market players tend to focus heavily on immediate avenues to maximise their own position. In doing so, there is the risk that the full impact on the wider market from their actions will not be adequately evaluated. More specific requirements that provide baseline expectations for all market operators and market participants will help to mitigate the impacts of this.

50 We already expect (through guidance) market operators to review their critical systems to ensure they function as intended, are reliable and do not pose a threat to fair and orderly trading. They must also test their critical system connectivity with each other to ensure they are able to coordinate trading suspensions. We do not expect the proposed rules to impose significant additional burden.

51 The ASX outage in 2016 created considerable confusion among market users about the nature of the incident and which products were available to trade. As a result, liquidity was significantly dampened, and spreads were wide: see REP 509. In addition, Chi-X's own market opening was affected due to issues in processing the individual trading status of each security.

52 Critical systems arrangements should be clearly documented so that staff from across an organisation can access a central, single source of information. This should include results from critical system reviews and

testing undertaken by a market operator or market participant. A central repository of detailed documentation will help market operators and participants in recovery efforts in the event of a critical system failure.

53 The focus on identifying and managing the risks of market operators' critical systems is consistent with IOSCO sound practices in IOSCO Report FR31/2015. This report identifies that market operators are reliant on technology and, consequently, must ensure their technological and critical systems remain resilient and reliable. Further, systems and services also need to have integrity so that confidence in the operations of a market operator is maintained. The report recognises that this is accomplished by having mechanisms, policies, procedures and processes in place that, among other things, ensure that existing systems operate effectively and securely, and have controls for when market operators introduce or make changes to critical systems.

54 Identifying and managing the risks of market participants' critical systems is consistent with principle 1 of the joint forum business continuity plan principles set out in IOSCO Report FR32/2015 which provides that financial industry participants should have effective and comprehensive approaches to business continuity management.

Change management of critical systems

55 Our proposed rule will require market participants and market operators 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.

56 To ensure that critical systems arrangements remain adequate we propose a requirement that market operators and market participants have appropriate testing arrangements. For market operators, this is already an expectation detailed in ASIC guidance.

57 Due to the interconnected nature of markets, our proposed rule will also require effective internal and external communication strategies to ensure persons who may be materially impacted by an implementation are adequately informed. Persons likely to be materially impacted may include clients, data vendors, ASIC, other market operators or market participants and the operators of licensed clearing and settlement facilities.

58 Market operators will have an additional requirement to ensure they provide written notice of the proposed implementation to ASIC within a reasonable timeframe before the implementation.

Proposal

B2 We propose introducing rules that:

(a) require market operators and market participants to ensure their critical systems arrangements remain adequate following the implementation of a new critical system or a change to an existing critical system;

(b) require additional arrangements that include:

(i) testing new critical systems or changes to the existing critical system before implementation;

(ii) communicating with anyone that may be materially affected by the implementation to ensure they are adequately informed about the nature, timing and impact of the implementation before it occurs;

(iii) ensuring, to the extent reasonably practicable, that anyone materially affected by the implementation is adequately prepared for the implementation before it occurs; and

(iv) providing written notice of the proposed implementation to ASIC in a reasonable time before the implementation (market operators only).

Your feedback

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?

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

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.

Rationale

59 We consider that our proposed rules provide additional clarity and reinforce existing expectations for market operators and market participants about their obligations under s792A(a) and (d) and s912A(1)(a) and (d) of the Corporations Act respectively.

60 To ensure that their technological resources are sufficient, it is important that market operators and market participants have appropriate testing arrangements to confirm that their critical systems are functional and reliable.

61 Technology governance and change management is crucial. In the absence of adequate change management controls (which may include regression testing of up/downstream systems, data and processes as well as data migration) unidentified issues may arise during the deployment of a critical system or a change to a critical system. These issues can lead to flow-on effects that can cause market disruption.

62 Effective testing and communication with persons that may be affected by changes to critical systems is essential to ensuring that changes or new critical systems are functional and reliable and do not impact on the resilience, reliability, integrity and security of existing systems or the critical systems of others.

63 Deepening interdependencies among industry participants have also increased the likelihood that changes to critical systems will have an impact on other financial industry participants. It has been our experience that market participants have many interconnected systems. For example, market participants can be unaware for years that client money is not accurately reconciling or that certain clients (who are expecting access to all markets) only have access to one market. Also, errors in origin of order data impacts ASIC's surveillance capabilities (and in some cases industry funding allocations). There are very real and tangible consequences from poor change management processes.

64 Notifications from market operators prior to the implementation of critical systems provide ASIC with information about any potential impact of these changes on the market and its participants. These notifications may lead to ASIC providing input in circumstances where we believe it should not solely be within the market operator's discretion to make such an implementation. Such notifications also inform ASIC about the appropriate level of surveillance required over the market operator to ensure the implementation is suitably planned and managed.

65 IOSCO Report FR31/2015 recognises the need to have controls for the introduction of new, or changes to, critical systems.

Outsourcing critical systems

66 Many market operators and participants use third-party service providers to perform processes, services or activities relating to their critical systems. The service provider may be a related party within the corporate group or an unrelated third party.

67 Outsourced functions may be provided domestically or overseas. Many market participants outsource critical system functions such as market surveillance or clearing and settlement. Increasingly, firms are relying on the

delivery of computing services over the internet (cloud computing services). Such services include the transmission, storage, analysis and management of data.

68 Outsourcing can provide benefits, such as lower costs and allowing access to specialist expertise and the latest technology solutions. However, outsourcing may also impede the ability of market operators and market participants to manage risks and monitor compliance with their obligations. Importantly, market operators and market participants can not outsource to a service provider their responsibility for meeting regulatory obligations.

69 In Australia and other jurisdictions, market participants are responsible for the actions of any third-party service providers on which they rely. Under s769B of the Corporations Act, a market participant remains responsible for complying with its obligations as a licensee in relation to its outsourced services: see RG 104.

70 Internationally, certain jurisdictions have already set out specific rules to ensure market participants maintain adequate outsourcing arrangements (see IOSCO Report FR32/2015). Some jurisdictions have specifically considered the outsourcing recommendations in relation to cloud computing services.

71 The use of cloud computing is still somewhat in its infancy, with a focus more on storage of data rather than analysing or synthesising data. However, firms of all sizes are looking to cloud computing as a cost-effective means of providing scalability in data storage, artificial intelligence and analytics. Increased reliance on cloud service providers may concentrate risk in a small number of service providers and heighten cybersecurity risks. We are closely monitoring developments with cloud computing and may release further, more targeted, guidance in this area.

72 APRA has recently released an information paper,'Outsourcing involving cloud computing services', which identifies a range of issues we think are relevant for all financial services entities. We do not propose a specific rule in relation to cloud computing services, but instead expect the outsourcing arrangements rules to apply to this service.

73 Market operators are required under s792A(c) of the Act to have adequate arrangements (which may involve the appointment of an independent person or related entity) for operating the market, including arrangements for:

(a) handling conflicts between the commercial interests of the licensee and the need for the licensee to ensure that the market operates in a fair, orderly and transparent manner; and

(b) monitoring and enforcing compliance with the market's operating rules.

74 Where market operators rely on outsourced services for their critical systems, we already expect them to consider business continuity, capacity management and stress testing as part of their arrangements: see RG 172.

75 To ensure regulatory expectations remain aligned to IOSCO's outsourcing principles and other local and international developments, the proposed rules will provide an outsourcing control framework and supplement the existing requirements under the Corporations Act.

Proposal

B3 We propose introducing rules that:

(a) define an 'outsourcing arrangement' as an arrangement under which a third party provides, supports or operates a critical system;

(b) require market operators and market participants to conduct due diligence prior to entering into an outsourcing arrangement to ensure the service provider has the ability to provide the services effectively;

(c) require market operators and market participants to ensure that an outsourcing arrangement is covered by a legally binding written contract with the service provider that:

(i) sets out the nature, scope and quality of services to be provided;

(ii) requires a service provider to obtain approval before outsourcing any of the services already outsourced to them to another party and before making any other material change to the manner in which the services covered by the outsourcing arrangement are provided; and

(iii) includes termination provisions, including a provision for the orderly transfer of services following termination of a contract;

(d) requires market operators and market participants to:

(i) monitor the service provider's performance in providing the outsourced services and ensure it has the ability and capacity to continue to provide those services effectively;

(ii) have in place arrangements to identify and manage any conflicts of interest involving the service provider or related party;

(iii) in relation to any outsourced critical systems, have in place adequate arrangements to ensure they can comply with their obligations under the Corporations Act and market integrity rules;

(iv) ensure that they and their auditors can promptly, upon request, access books, records and other information relating to the critical systems from the service provider;

(v) ensure that ASIC has the same access to all books, records and other information relating to the critical systems and

maintained by the service provider, that ASIC would have if not for the outsourcing arrangement; and

(vi) ensure that for each outsourcing arrangement, the market operator's and market participant's board and senior management have confirmed they have complied with their obligations above and have made a written attestation to that effect;

(e) requires market operators and market participants to:

(i) comply with all of the above requirements in a manner appropriate to the nature, complexity, risks and materiality of the outsourcing arrangement; and

(ii) in determining whether the service provider has the ability and capacity to provide the outsourced services, consider the extent to which the service provider is providing the same or similar services to other market operators or market participants; and

(f) requires a market operator to give written notice to ASIC before entering into an outsourcing arrangement.

Your feedback

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.

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?

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.

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.

Rationale

76 Market operators perform an important role in market orderliness. The responsibilities of a market operator include the provision of critical infrastructure that facilitates trading, compliance oversight and the handling of market-sensitive data. Consequently, the outsourcing of critical systems or the operation or support of those systems brings with it unique risks and challenges that differ from other financial entities.

77 Poor controls and a lack of due diligence when considering outsourcing can lead to or exacerbate market disruption. An inappropriate selection and engagement of a service provider by a market operator or participant can lead to market disruption, non-compliance with laws and potentially detrimental effects for participants, users and market operators who rely on the critical systems.

78 There are also high risks when a market participant outsources any of its critical systems. There have been instances where Australian market participants have experienced major system outages—for example, the failure of a middle and back office system due to a data corruption event where the outsourced service provider failed to follow standard procedures for system maintenance. The outage resulted in settlement failures and affected, among other things, financial monitoring, securities transactions, position and account ledgers, and reconciliations.

79 If a market operator or market participant has not been sufficiently engaged with the outsourced services and systems, there is a risk that they will have inadequate oversight of actual service levels. Where a market operator or market participant enters into an outsourcing arrangement with an offshore service provider, time zone differences may make it difficult for them to get urgent support during the trading day. These are just some factors that market operators and market participants need to carefully consider in their risk management of a potential service provider.

80 The requirement on market operators to provide notice to ASIC before entering into an outsourcing arrangement will allow us to monitor for emerging risks (including concentration risks) that may arise as a result of outsourcing. It is important for us to gather information about trends relating to emerging risks that might not otherwise be properly discerned.

81 If critical systems are outsourced, IOSCO recognises the importance of having policies and procedures in place to ensure that system modifications do not pose risks to the orderly functioning and integrity of the market.

82 The proposed rules are consistent with the IOSCO principles set out in IOSCO Report FR31/2015, IOSCO's *Principles for outsourcing by markets* and IOSCO's *Principles on outsourcing of financial services for market intermediaries*, February 2005.

83 In the 2005 IOSCO report, IOSCO outlines several outsourcing principles including:

(a) due diligence in the selection and monitoring of a service provider and service provider's performance;

(b) having contracts in place with a service provider which include provisions relating to the termination of the contract and appropriate exit strategies;

(c) having appropriate measures in place to ensure a service provider establishes and maintains emergency procedures and a plan for disaster recovery with periodic testing of backup facilities;

(d) taking appropriate steps to require that service providers protect proprietary and confidential information about the market participant and its clients from intentional or inadvertent disclosure to unauthorised individuals;

(e) having consideration for concentration risk relating to outsourced functions; and

(f) ensuring the market participant, its auditors and the regulator have prompt access to the books and records of the service providers relating to the outsourced activities.

Risk management—Data and cyber risk

84 Market operators and market participants hold or receive a range of information including their own data and data received from participants, market operators, service providers and their clients. For market operators this may also include 'market information' when a market is responsible for a company announcement platform (e.g. listed or quoted products on ASX, Chi-X, NSX and SSX). This information may include market-sensitive, confidential and personal data. Market operators and market participants must protect this information from theft, loss or corruption.

85 Data held will vary in volume and complexity depending on the operations and structure of the market operator or market participant. Globally, there is increased reliance on digital operations and services such as online trading and robo-advice, resulting in larger and more complex data sets being generated that are critical to the effective operation of market operators and market participants.

86 Data analytics is used to optimise operations, enhance services and gain a competitive advantage in the market. Data analytics, in the form of risk analytics, is also being used to support market operators and market participants in their risk and compliance activities. Through this process of

analysis, new data sets containing strategic or commercially sensitive content may be generated.

87 Cyber attacks on market operators and market participants may impact on the security, confidentiality, integrity and availability of access to data. Such attacks can also affect investor confidence in the integrity of the markets they invest in. Examples of the types of cyber attacks intended to be covered by the proposed rules include theft, destruction or manipulation of data, system outages and denial of service attacks requiring ransom at the extreme. These attacks may facilitate, for example, identify theft and other harms.

88 Cyber attacks have the potential to disrupt the operation of a market operator or a market participant's critical systems and affect the fair and orderly operation of, and investor confidence in, the market. We are aware that there are ongoing penetration attempts across the industry. Recently there has been a growing number of share sale frauds, where client identification and account details are stolen and share accounts and the shares/funds in those accounts are accessed and transferred (stolen). We have published an information sheet for market participants providing specific guidance on how to limit the risk of share sale fraud: see Information Sheet 237 *Protecting against share sale fraud* (INFO 237).

89 Cybersecurity has been an ASIC priority over recent years. We have worked with market operators, participants and listed companies (among other financial services institutions) to undertake a cyber health check using the US National Institute of Standards and Technology (NIST) framework: see Report 429 *Cyber resilience: Health check* (REP 429) and Report 555 *Cyber resilience of firms in Australia's financial markets* (REP 555). We are doing a refresh of these reviews and expect to publish a report in the coming period. We have also issued cyber resilience good practices.

90 Internationally, there has been recognition of the importance of data privacy and security. As set out in Section A of this paper, the European Union and the United States have both introduced rules (the EU GDPR and SEC Reg SCI respectively) designed to ensure the integrity, confidentiality and security of data.

91 In Australia, the *Privacy Amendment (Notifiable Data Breaches) Act 2017* amends the *Privacy Act 1988* (Privacy Act) to introduce a mandatory notifiable data breaches scheme for entities regulated by the Privacy Act. The scheme came into effect on 22 February 2018 and includes an obligation to notify individuals whose personal information is involved in a data breach that is likely to result in serious harm.

92 For those entities that are also ADIs, APRA has issued guidance on managing data risk: see, for example, Prudential Practice Guide CPG 235 *Managing data risk*.

93 There are currently no specific market integrity rules requiring market operators and market participants to have adequate arrangements to ensure the confidentiality, integrity and security of data obtained, held or used. The proposed rules complement existing obligations in place here and abroad and will bolster ASIC's regulatory and enforcement toolkit in this area.

Proposal

B4 We propose introducing rules that require:

(a) market operators and market participants to have adequate arrangements to ensure the confidentiality, integrity and security of data obtained, held or used by a market operator or market participant in connection with their operations or services, including:

(i) controls, including automated controls, designed to prevent unauthorised access to data;

(ii) controls for identifying, assessing, managing and monitoring unauthorised access to data; and

(iii) arrangements designed to prevent the theft, loss or corruption of data;

(b) market operators and market participants to have adequate arrangements to ensure the availability of access to data obtained, held or used by a market operator or market participant in connection with their operations or services, including arrangements for backup and the timely recovery of data in the event of theft, corruption or loss of the data;

(c) market operators to notify ASIC in writing, as soon as practicable on becoming aware of any unauthorised access to or use of:

(i) their critical systems that affect the effective functioning of those systems; and

(ii) market-sensitive, confidential or personal data; and

(d) market participants to maintain, for a period of at least seven years after the relevant event, records of any unauthorised access to or use of:

(i) their critical systems that affect the effective functioning of those systems; and

(ii) market-sensitive, confidential or personal data.

Your feedback

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

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.

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.

Rationale

94 Notification requirements for market operators allow ASIC to gather information about potential weaknesses and persistent or recurrent problems resulting in cyber or data risk. This information will also allow ASIC to provide necessary industry alerts or guidance.

95 The proposed rule is consistent with sound practice 2 which is set out in IOSCO Report FR32/2015 and relates to the protection of data, systems and client privacy. IOSCO encourages all market participants to consider whether, as part of the business continuity plan or otherwise, they have addressed the need to protect data and client privacy, particularly from cyber attacks. This would include measures to address the risk of potential loss or compromising the firm's and investors' information or assets due to cyber attacks.

96 IOSCO Report FR31/2015 details sound practices to protect market operators' critical systems against cyber attacks that include establishing, implementing and updating robust cybersecurity programs—for example:

(a) governance practices such as appropriate controls to restrict access to critical systems and identification of responsible personnel;

(b) appropriate escalation and communication procedures;

(c) penetration and vulnerability testing;

(d) data storage and integrity safeguards, such as the use of offsite storage facilities or backup centres, encryption, passwords and network segregation, and anti-virus and anti-malware software; and

(e) policies and procedures to monitor for suspicious network activity, including intrusion detection, firewalls and audit trails regarding access to critical systems.

97 The proposed rules give effect to the IOSCO principles and sound practices and address the data and cybersecurity risks that are escalating in Australia and abroad.

Incident management and business continuity arrangements

98 An unexpected interruption to the usual operation of a critical system or major event that causes significant disruption to market operations or services may result in disruption for other market users. Having appropriate business continuity, backup and disaster recovery arrangements can minimise the effects that a disruption or outage can have on services for the entity as well as other market operators, participants or market users who are dependent on the market operator or participant for their critical systems.

99 There are some existing expectations for market operators and participants in relation to incident management and business continuity arrangements, but they are partly in guidance rather than rules.

(a) *Market operators* should have robust continuity planning, backup and disaster recovery arrangements: see RG 172. They are also required to:

(i) notify ASIC of breaches under s792A of the Corporations Act, including those relating to sufficient technological resources and maintaining a fair, orderly and transparent market (s792B(1) of the Corporations Act); and

(ii) notify ASIC, other market operators and market participants of certain technical problems that may interfere with the fair, orderly or transparent operation of any market (Rule 9.1.3 of the Securities Markets Rules). There is currently no equivalent rule for futures market operators.

(b) *Market participants* should already undertake incident management reviews and tests to meet their general obligations under the Corporations Act. Further:

(i) ASX Clear participants are also required to maintain adequate disaster recovery and business continuity arrangements; and

(ii) those operating a crossing system must also notify ASIC of issues that materially affect the efficiency or proper functioning of a crossing system (Rule 5A.2.3 of the Securities Markets Rules).

100 It is important for continuity across all market operators and across all participants that clear, consistent rules apply. The proposed rules require market operators and market participants to establish, maintain and implement incident management plans for dealing with incidents and major events that can disrupt the operation of their critical systems.

Proposal

B5 We propose introducing rules that:

(a) define an 'incident' and a 'major event';

(b) require market operators and market participants to establish, maintain and implement plans for dealing with incidents (incident management plans) and major events (business continuity plans);

(c) require market operators and market participants to design their incident management and business continuity plans to enable:

(i) continuation of the usual operation of their critical systems, operations and services during an incident or major event; or

(ii) if continuation of the usual operations of critical systems, operations and services is not possible, the timely and orderly restoration of operations following the incident or major event;

(d) require market operators' and market participants' incident management plans and business continuity plans to be appropriate to the nature, scale and complexity of the critical systems, operations, services and their structure and location;

(e) require market operators and market participants to identify and address in their incident management plans and business continuity plans:

(i) the types of incidents and major events that may impact their critical systems, operations and services;

(ii) the potential impact incidents and major events may have on their critical systems, operations and services;

(iii) the classification of types of incidents and major events according to potential severity of the impacts;

(iv) escalation procedures;

(v) the actions, arrangements and resources required to achieve continuation or restoration of the usual operation of critical systems, operations and services, including specific time objectives to achieve this outcome; and

(vi) procedures for communicating during an incident or major event with persons that may be affected by the incident or major event to ensure they are adequately informed about the nature and impact of, and steps being taken to manage, the incident or major event; likely timing for restoration of critical systems, operations and services; and

(vii) any relevant operational dependencies that may affect the matters in (i) to (vi) above;

(f) require market operators and market participants to have adequate arrangements to ensure they can carry out incident management or business continuity plans for any outsourced critical systems;

(g) require market operators to notify ASIC as soon as they become aware of an incident or major event that may interfere with the fair, orderly or transparent operation of any market and notify other market operators, operators of clearing and settlement facilities and participants that may be affected. A subsequent report must be provided detailing the circumstances and steps taken to manage the incident or major event;

(h) require market participants to notify ASIC as soon as they become aware of a major event and, within seven days of the notification, provide a report to ASIC detailing the circumstances of the major event and steps taken to manage the major event;

(i) require market operators and market participants to review and test their incident management and business continuity arrangements:

  (i) at a frequency and in a manner appropriate to the nature, scale and complexity of their critical systems, operations and services, structure and location; and each time there is a material change to the critical systems, operations or services, structure or location; and in the case of the business continuity plans, at a minimum once every three months for market operators and once every 12 months for market participants; and

  (ii) update the incident management plans and business continuity plans as required; and

(j) require market operators and market participants to document:

  (i) incident management and business continuity plans;

  (ii) the scope and results of reviews and testing performed; and

  (iii) maintain that documentation for at least seven years.

Your feedback

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

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.

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

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

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.

Rationale

101 The multi-market environment in Australia means incidents or major events experienced by market operators or market participants can have flow-on effects to other market operators or other market participants who require access to these systems to carry out their activities. Therefore, in the event of a problem that disrupts services for other market users, it is essential that

these users are notified and informed. A lack of communication during system disruptions can create uncertainty and a lack of confidence in the market system. It also makes it difficult for other market users to appropriately manage their risks in response to the disruption.

102 There is currently no equivalent rule in the Futures Markets Rules to Rule 9.1.3 of the Securities Markets Rules, which requires market operators to notify ASIC, other market operators and market participants as soon as they become aware of technical issues that may interfere with the fair, orderly or transparent operation of any market. It is our intention that the proposed incident management and business continuity rule will replace Rule 9.1.3 and ensure continuity across all market operators and participants.

103 We expect market operators to already have systems in place to identify incidents that interfere with the fair, orderly or transparent operation of any market or major events. Such incidents may include, for example, interruption to price formation systems or failure of a system that results in the market operator being unable to meet one of its other licensee obligations. It is important that market operators notify ASIC immediately when these incidents occur to prevent the risk of contagion.

104 Notification from market participants as soon as they become aware of a major event and lodgement, within seven days of notification, of a report detailing the circumstances of the major event and steps taken to manage the major event, allows ASIC to monitor any trends relating to incidents that interfere with the operation of markets that would otherwise not be properly discerned.

105 The proposed rule is consistent with principles 2–6 of the joint forum business continuity plan principles set out in IOSCO Report FR31/2015 and IOSCO Report FR32/2015. These principles provide that:

(a) financial industry participants should incorporate the risk of a major operational disruption into their approaches to business continuity management (principle 2);

(b) financial industry participants should develop recovery objectives that reflect the risk they represent to the operation of the financial system (principle 3);

(c) financial industry participants should include in their business continuity plans procedures for communicating within their organisations and with relevant external parties in the event of a major operational disruption (principle 4);

(d) financial industry participants' communication procedures should address communications with financial authorities in other jurisdictions in the event of major operational disruptions with cross-border implications (principle 5); and

(e) financial industry participants should test their business continuity plans, evaluate their effectiveness, and update their business continuity management (principle 6).

106 The proposed rule reflects IOSCO sound practice and is consistent with the joint forum's view, set out in IOSCO Report FR32/2015, that all market intermediaries should:

(a) be required to have written business continuity plans identifying procedures relating to an emergency or significant business disruption; and

(b) update these plans in the event of a material change to their operations, structure, businesses or locations, and conduct annual reviews to determine whether any modifications are necessary.

Governance arrangements and adequate resources

107 We propose a rule that requires market operators to have governance arrangements and adequate financial, technological and human resources to support all of the arrangements outlined in the above proposals.

Proposal

B6 We propose to introduce a rule that requires market operators and market participants to:

(a) have governance arrangements and adequate financial, technological and human resources to comply with all the obligations in these proposed rules; and

(b) have arrangements for their board and senior management to have oversight of the establishment, maintenance, implementation, review, testing and documentation of their incident management plans and business continuity plans.

Your feedback

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.

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.

Rationale

108 Business continuity management is essential to ensuring that a participant can maintain its critical systems in the face of disruptions. It is appropriate that market operators and market participants ensure that oversight and accountability for business continuity is held at the highest levels within their organisations. This approach is also consistent with ASIC's broader governance strategic priority for greater board and senior executive oversight of, and accountability for, critical functions and consumer outcomes.

109 The proposed rule is consistent with:

(a) principle 1 of the joint forum business continuity plan principles set out in IOSCO Report FR32/2015, which provides that an organisation's board of directors and senior management are collectively responsible for the organisation's business continuity; and

(b) principle 1 of the joint forum principles set out in IOSCO Report FR31/2015, which provides that financial industry participants should have effective and comprehensive approaches to business continuity management. An organisation's board of directors and senior management are collectively responsible for the organisation's business continuity. IOSCO also states that clarity around the governance of business continuity plans and their implementation is important.

Fair access to the market—Market operator rule only

110 As market operators increasingly adapt to technological innovations, they need to consider how the availability of technology affects participants and users of the market, other stakeholders and the efficiency and fairness of the wider Australian financial system.

111 There is guidance in RG 172 that market operators should provide access to their market and services on reasonable commercial terms and on a non-discriminatory basis. We propose to embed this expectation in rules.

Proposal

B7 We propose introducing a rule (for market operators only) that requires a market operator to provide access to their market and to their associated products, data and services:

(a) on reasonable commercial terms; and

(b) on a non-discriminatory basis.

Your feedback

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.

Rationale

112 The proposed rule is intended to mitigate the risks of technological innovations in markets being made available in an unfair way, while supplementing the market operator's obligations to operate a fair, orderly and transparent market. Fair access is access provided on reasonable commercial terms (including price and non-price terms) and on a non-discriminatory basis. To fulfil these aims, terms on which access is available should be transparent (i.e. expressed in reasonably plain language, presented clearly and readily available to participants and other users of the market affected by the terms).

113 For example, market data and the proximity to a market's matching engine have become key commercial offerings by market operators in the current high-speed automated trading environment. It is important that these and other services are made available in a fair way to anyone that seeks access.

Trading controls—Market operator rule only

114 It is important that market operators have appropriate mechanisms in place to maintain a fair and orderly market. This includes the capacity to manage messages entering the market's matching engine.

115 We already expect certain securities market operators to have in place execution risk controls that will minimise the incidence of anomalous priced orders and transactions executing in the extreme trade range: Chapter 8 of the Securities Markets Rules.

116 There is an existing requirement for market participants that operate crossing systems to have controls that enable the suspension, limitation or prohibition of the entry of orders in the crossing system (Rule 5A.5.2 of the Securities Markets Rules). Proposal 8 is intended to apply the same obligation to market operators.

Proposal

B8 We propose introducing a rule (for market operators only) that 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 where required for the purposes of ensuring the market is fair, orderly and transparent.

Your feedback

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.

Rationale

117 This type of 'kill switch' functionality to manage the orders of individual participants has proven important in markets—for example, the incident in the United States where principal trading firm, Knight Capital, flooded the market with errant orders. Both Knight Capital and the stock exchange were unable to easily switch off the flow.

118 The proposed rule will create consistency between the obligations of market operators and market participants and embed existing expectations.

C Regulatory and financial impact

119 In developing the proposals in this paper, we have carefully considered their regulatory and financial impact. On the information currently available to us we think they will strike an appropriate balance between:

(a) ensuring resilient market operators and market participants that do not adversely affect the integrity and efficiency of Australian financial markets or create systemic risks in the Australian financial system; and

(b) providing an appropriate level of flexibility and consistency with global industry practice.

120 Before settling on a final policy, we will comply with the Australian Government's regulatory impact analysis (RIA) requirements by:

(a) considering all feasible options, including examining the likely impacts of the range of alternative options which could meet our policy objectives;

(b) if regulatory options are under consideration, notifying the Office of Best Practice Regulation (OBPR); and

(c) if our proposed option has more than minor or machinery impact on business or the not-for-profit sector, preparing a Regulation Impact Statement (RIS).

121 All RISs are submitted to the OBPR for approval before we make any final decision. Without an approved RIS, ASIC is unable to give relief or make any other form of regulation, including issuing a regulatory guide that contains regulation.

122 To ensure that we are able to properly complete any required RIS, please give us as much information as you can about our proposals or any alternative approaches, including:

(a) the likely compliance costs;

(b) the likely effect on competition; and

(c) other impacts, costs and benefits.

See 'The consultation process', p. 4.

Key terms

Term	Meaning in this document
ADI	Authorised deposit-taking institution
APRA	Australian Prudential Regulation Authority
ASIC	Australian Securities and Investments Commission
ASX	ASX Limited (ACN 008 624 691) or the exchange market operated by ASX Limited
ASX 24	The exchange market operated by Australian Securities Exchange
ASX Group	ASX, Australian Securities Exchange, ASX Clear, ASX Clear (Futures) and ASX Settlement
ASX outage	On 19 September 2016, ASX experienced a hardware failure in its equities trading system, ASX Trade. The initial technology failure triggered a number of events that delayed the opening of the ASX market and caused it to close early
Australian market licence	An Australian market licence under s795B of the Corporations Act that authorises a person to operate a financial market
Chi-X	Chi-X Australia Pty Limited (ACN 129 584 667) or the exchange market operated by Chi-X
Corporations Act	*Corporations Act 2001* (Cth), including regulations made for the purposes of that Act
financial market	As defined in s767A of the Corporations Act. It encompasses facilities through which offers to acquire or dispose of financial products are regularly made or accepted
Futures Markets Rules	ASIC Market Integrity Rules (Futures Markets) 2017—rules made by ASIC under s798G of the Corporations Act
GDPR	General Data Protection Regulation (EU) 2016/679
INFO 237 (for example)	An ASIC information sheet (in this example numbered 237)
IOSCO	International Organization of Securities Commissions
market integrity rules	Rules made by ASIC, under s798G of the Corporations Act, for trading on domestic licensed markets
market operator (or market licensee)	The operator of a financial market. A market operator may be referred to as a 'market licensee' where they are the holder of an Australian market licence

Term	Meaning in this document
market participant	A participant of a market Note: Participant has the meaning given by s761A of the Corporations Act.
NSX	National Stock Exchange of Australia Limited or the exchange market operated by NSX Note: NSX was formerly known as Stock Exchange of Newcastle Limited.
Part 7.4 (for example)	A part of the Securities Markets Rules (in this example numbered 7.4), unless otherwise specified
RBA	Reserve Bank of Australia
Reg SCI	Regulation Systems Compliance and Integrity
REP 509	An ASIC report (in this example numbered 509)
RG 265 (for example)	An ASIC regulatory guide (in this example numbered 265)
Rule 5.5.2	A rule of the Securities Markets Rules (in this example numbered 5.5.2), unless otherwise specified
s792A	A section of the Corporations Act (in this example numbered 792A), unless otherwise specified
Securities Markets Rules	ASIC Market Integrity Rules (Securities Markets) 2017—rules made by ASIC under s798G of the Corporations Act

List of proposals and questions

Proposal	Your feedback
B1 We propose introducing rules that: (a) define 'critical system' to mean functions, infrastructure, processes or systems which in the event of failure to operate effectively, would or would be likely to cause significant disruption to the market operator's or market participant's market-related operations and services; (b) require market operators and market participants to have adequate arrangements in place to ensure the resilience, reliability, integrity and security of their critical systems; (c) require critical systems arrangements to include: (i) identifying the critical systems; (ii) identifying, assessing, managing and monitoring risks to the resilience, reliability, integrity and security of the critical systems; (iii) ensuring the critical systems have sufficient and scalable capacity for ongoing and planned operations and services; (iv) preventing unauthorised access to or use of critical systems; (v) managing the implementation of new critical systems and changes to existing critical systems; (vi) dealing with an incident or major event affecting the critical systems; and (vii) managing outsourcing arrangements in relation to critical systems; (d) require market operators and market participants to: (i) review their critical systems arrangements following each material change to their critical systems, and at least annually; and (ii) change the critical systems arrangements as required to ensure they continue to comply with the above obligations; and	B1Q1 Do you agree with the definition of 'critical systems' and 'critical systems arrangements'? In your response, please give detailed reasons for your answer. 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? 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? 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. 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.

Proposal	Your feedback
(e) require market operators and market participants to: (i) document their critical systems arrangements; (ii) document the scope and results of reviews of their critical systems arrangements; (iii) document any changes to the critical systems arrangements; and (iv) maintain that documentation for a period of at least seven years.	
B2 We propose introducing rules that: (a) require market operators and market participants to ensure their critical systems arrangements remain adequate following the implementation of a new critical system or a change to an existing critical system; (b) require additional arrangements that include: (i) testing new critical systems or changes to the existing critical system before implementation; (ii) communicating with anyone that may be materially affected by the implementation to ensure they are adequately informed about the nature, timing and impact of the implementation before it occurs; (iii) ensuring, to the extent reasonably practicable, that anyone materially affected by the implementation is adequately prepared for the implementation before it occurs; and (iv) providing written notice of the proposed implementation to ASIC in a reasonable time before the implementation (market operators only).	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? B2Q2 Do you agree with our proposed rule? If you disagree, please give detailed reasons why. 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.
B3 We propose introducing rules that: (a) define an 'outsourcing arrangement' as an arrangement under which a third party provides, supports or operates a critical system; (b) require market operators and market participants to conduct due diligence prior to entering into an outsourcing arrangement to ensure the service	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. B3Q2 Do you agree with the definition of 'outsourcing arrangement'? In your response, please give detailed reasons for your answer.

Proposal	Your feedback
provider has the ability to provide the services effectively; (c) require market operators and market participants to ensure that an outsourcing arrangement is covered by a legally binding written contract with the service provider that: (i) sets out the nature, scope and quality of services to be provided; (ii) requires a service provider to obtain approval before outsourcing any of the services already outsourced to them to another party and before making any other material change to the manner in which the services covered by the outsourcing arrangement are provided; and (iii) includes termination provisions, including a provision for the orderly transfer of services following termination of a contract; (d) requires market operators and market participants to: (i) monitor the service provider's performance in providing the outsourced services and ensure it has the ability and capacity to continue to provide those services effectively; (ii) have in place arrangements to identify and manage any conflicts of interest involving the service provider or related party; (iii) in relation to any outsourced critical systems, have in place adequate arrangements to ensure they can comply with their obligations under the Corporations Act and market integrity rules; (iv) ensure that they and their auditors can promptly, upon request, access books, records and other information relating to the critical systems from the service provider; (v) ensure that ASIC has the same access to all books, records and other information relating to the critical systems and maintained by the service provider, that ASIC would have if not for the outsourcing arrangement; and	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? 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. 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.

Proposal	Your feedback
(vi) ensure that for each outsourcing arrangement, the market operator's and market participant's board and senior management have confirmed they have complied with their obligations above and have made a written attestation to that effect; (e) requires market operators and market participants to: (i) comply with all of the above requirements in a manner appropriate to the nature, complexity, risks and materiality of the outsourcing arrangement; and (ii) in determining whether the service provider has the ability and capacity to provide the outsourced services, consider the extent to which the service provider is providing the same or similar services to other market operators or market participants; and (f) requires a market operator to give written notice to ASIC before entering into an outsourcing arrangement.	
B4 We propose introducing rules that require: (a) market operators and market participants to have adequate arrangements to ensure the confidentiality, integrity and security of data obtained, held or used by a market operator or market participant in connection with their operations or services, including: (i) controls, including automated controls, designed to prevent unauthorised access to data; (ii) controls for identifying, assessing, managing and monitoring unauthorised access to data; and (iii) arrangements designed to prevent the theft, loss or corruption of data; (b) market operators and market participants to have adequate arrangements to ensure the availability of access to data obtained, held or used by a market operator or market participant in connection with their operations or services, including arrangements for backup and the timely recovery of data in the event of theft, corruption or loss of the data;	B4Q1 Do you agree with the proposed rules? If not, please give detailed reasons why you disagree. 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. 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.

Proposal	Your feedback
(c) market operators to notify ASIC in writing, as soon as practicable on becoming aware of any unauthorised access to or use of: (i) their critical systems that affect the effective functioning of those systems; and (ii) market-sensitive, confidential or personal data; and (d) market participants to maintain, for a period of at least seven years after the relevant event, records of any unauthorised access to or use of: (i) their critical systems that affect the effective functioning of those systems; and (ii) market-sensitive, confidential or personal data.	
B5 We propose introducing rules that: (a) define an 'incident' and a 'major event'; (b) require market operators and market participants to establish, maintain and implement plans for dealing with incidents (incident management plans) and major events (business continuity plans); (c) require market operators and market participants to design their incident management and business continuity plans to enable: (i) continuation of the usual operation of their critical systems, operations and services during an incident or major event; or (ii) if continuation of the usual operations of critical systems, operations and services is not possible, the timely and orderly restoration of operations following the incident or major event; (d) require market operators' and market participants' incident management plans and business continuity plans to be appropriate to the nature, scale and complexity of the critical systems, operations, services and their structure and location; (e) require market operators and market participants to identify and address in their	B5Q1 Do you agree with the definition of 'incident' and 'major event'? In your response, please give detailed reasons for your answer. 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. B5Q3 Do you agree with the frequency of reviewing and testing incident management and business continuity plans? B5Q4 Do you agree with the specific arrangements required in an incident management plan or business continuity plan? 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.

Proposal	Your feedback
incident management plans and business continuity plans: (i) the types of incidents and major events that may impact their critical systems, operations and services; (ii) the potential impact incidents and major events may have on their critical systems, operations and services; (iii) the classification of types of incidents and major events according to potential severity of the impacts; (iv) escalation procedures; (v) the actions, arrangements and resources required to achieve continuation or restoration of the usual operation of critical systems, operations and services, including specific time objectives to achieve this outcome; and (vi) procedures for communicating during an incident or major event with persons that may be affected by the incident or major event to ensure they are adequately informed about the nature and impact of, and steps being taken to manage, the incident or major event; likely timing for restoration of critical systems, operations and services; and (vii) any relevant operational dependencies that may affect the matters in (i) to (vi) above; (f) require market operators and market participants to have adequate arrangements to ensure they can carry out incident management or business continuity plans for any outsourced critical systems; (g) require market operators to notify ASIC as soon as they become aware of an incident or major event that may interfere with the fair, orderly or transparent operation of any market and notify other market operators, operators of clearing and settlement facilities and participants that may be affected. A subsequent report must be provided detailing the circumstances and steps taken to manage the incident or major event;	

Proposal	Your feedback
(h) require market participants to notify ASIC as soon as they become aware of a major event and, within seven days of the notification, provide a report to ASIC detailing the circumstances of the major event and steps taken to manage the major event; (i) require market operators and market participants to review and test their incident management and business continuity arrangements: (i) at a frequency and in a manner appropriate to the nature, scale and complexity of their critical systems, operations and services, structure and location; and each time there is a material change to the critical systems, operations or services, structure or location; and in the case of the business continuity plans, at a minimum once every three months for market operators and once every 12 months for market participants; and (ii) update the incident management plans and business continuity plans as required; and (j) require market operators and market participants to document: (i) incident management and business continuity plans; (ii) the scope and results of reviews and testing performed; and (iii) maintain that documentation for at least seven years.	
B6 We propose to introduce a rule that requires market operators and market participants to: (a) have governance arrangements and adequate financial, technological and human resources to comply with all the obligations in these proposed rules; and (b) have arrangements for their board and senior management to have oversight of the establishment, maintenance, implementation, review, testing and documentation of their incident management plans and business continuity plans.	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. 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.

Proposal	Your feedback
B7 We propose introducing a rule (for market operators only) that requires a market operator to provide access to their market and to their associated products, data and services: (a) on reasonable commercial terms; and (b) on a non-discriminatory basis.	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.