



**ASIC**  
Australian Securities &  
Investments Commission

REGULATORY GUIDE 266

# Guidance on ASIC market integrity rules for participants of futures markets

August 2022

## About this guide

This guide is for market participants subject to the *ASIC Market Integrity Rules (Futures Markets) 2017* and *ASIC Market Integrity Rules (Capital) 2021*.

It gives guidance on how market participants can comply with their obligations under these rules.

### 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 guide was issued in August 2022 and is based on legislation and regulations as at the date of issue.

Previous version

- Superseded Regulatory Guide 266, issued May 2018

### Disclaimer

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

Examples in this guide are purely for illustration; they are not exhaustive and are not intended to impose or imply particular rules or requirements.

# Contents

<b>A</b>	<b>Overview</b> .....	<b>5</b>
	Supervision of trading on domestic licensed financial markets .....	5
	ASIC market integrity rules .....	5
	Communicating with ASIC .....	6
	Scope of this regulatory guide .....	6
	Related guidance .....	7
<b>B</b>	<b>Supervision of trading on domestic licensed financial markets</b> .....	<b>8</b>
	ASIC's supervisory responsibilities .....	8
	How ASIC works together with market licensees .....	9
	Status of notifications, consents, waivers, etc., given before 1 August 2010 .....	10
<b>C</b>	<b>ASIC market integrity rules</b> .....	<b>11</b>
	ASIC market integrity rules .....	11
	Waivers .....	12
<b>D</b>	<b>Communicating with ASIC</b> .....	<b>14</b>
	Forms .....	14
	Contacting ASIC .....	15
	When to contact ASIC .....	16
	Notifying ASIC of reportable situations .....	17
<b>E</b>	<b>Risk management</b> .....	<b>18</b>
	Risk management requirements for market participants .....	18
	Setting and documenting limits .....	19
	Terminal connections .....	23
	Accessing terminal connections .....	24
<b>F</b>	<b>Trust account reconciliation reporting</b> .....	<b>26</b>
	Trust account reconciliation reporting .....	26
<b>G</b>	<b>Capital requirements</b> .....	<b>27</b>
	Scope, application and waivers .....	27
	Lodging forms and returns .....	27
	ASX guidance materials on capital .....	27
<b>H</b>	<b>Good fame and character requirement</b> .....	<b>29</b>
<b>I</b>	<b>Supervisory policies and procedures</b> .....	<b>30</b>
<b>J</b>	<b>Foreign participants: Minimum presence requirements</b> .....	<b>31</b>
<b>K</b>	<b>Suspicious activity reporting</b> .....	<b>33</b>
	What suspicious activity must be reported? .....	33
	Compliance with Part 3.6 .....	43
<b>L</b>	<b>Crossing systems</b> .....	<b>47</b>
	Scope and application .....	47
	Notifying ASIC of intention to operate a crossing system .....	48
	Monthly reporting to ASIC on trading activity and system changes .....	49
	Public disclosure about crossing system operations .....	49
	Disclosure to crossing system clients .....	51
	Fair treatment of users .....	56
	Monitoring and suspicious activity reporting .....	57
	Systems and controls .....	60
<b>M</b>	<b>Technological and operational resilience</b> .....	<b>62</b>
	Scope and application .....	62
	Critical business services .....	63

Information security .....	75
Business continuity plans .....	79
Governance .....	84
<b>Appendix 1: Procedures, determinations and practice notes .....</b>	<b>85</b>
<b>Appendix 2: Superseded guidance .....</b>	<b>86</b>
<b>Key terms .....</b>	<b>87</b>
<b>Related information.....</b>	<b>89</b>

## A Overview

### Key points

We are responsible for supervising trading on Australian domestic licensed financial markets.

As part of our supervisory responsibilities, we make market integrity rules and monitor compliance by market participants with those rules.

This regulatory guide gives guidance on the obligations of participants of futures markets in relation to:

- risk management for house accounts;
- supervisory policies and procedures;
- minimum presence requirements for foreign market participants;
- client detail record keeping;
- crossing systems;
- suspicious activity reporting;
- capital requirements; and
- technological and operational resilience of critical business services.

### Supervision of trading on domestic licensed financial markets

- RG 266.1 We are responsible for supervising the activities and the conduct of business by market participants in relation to domestic licensed markets (i.e. financial markets operated by persons licensed under s795B(1) of the *Corporations Act 2001* (Corporations Act)).
- RG 266.2 We are also responsible for supervising compliance with the Corporations Act and for making and supervising compliance with market integrity rules.
- RG 266.3 Australian market licensees are responsible for the operation of their markets and for monitoring and enforcing compliance with their markets' operating rules, which include their listing rules.

### ASIC market integrity rules

- RG 266.4 Under Pt 7.2A of the Corporations Act, we are able to make market integrity rules dealing with activities and conduct in relation to domestic licensed financial markets, including the activities and conduct of market participants. We are also responsible for granting waivers from the obligation to comply with a provision of the market integrity rules.

## Communicating with ASIC

- RG 266.5 Market participants can contact ASIC directly to ensure that market integrity matters are known and addressed in an efficient and timely manner.
- RG 266.6 You may contact ASIC by direct email or by telephone to the relevant ASIC teams to communicate issues and queries about markets, trading and participant conduct. For contact details see RG 266.44–RG 266.48. See Table 3 for a list of email addresses you can use to contact ASIC about different market- and participant-related matters.
- RG 266.7 In Table 2 we have listed some of the information which must be provided to ASIC under the market integrity rules.

## Scope of this regulatory guide

- RG 266.8 This regulatory guide provides guidance for market participants on the *ASIC Market Integrity Rules (Futures Markets) 2017* and *ASIC Market Integrity Rules (Capital) 2021*.

Note 1: In this guide, ‘Futures Markets Rules’ refers to the *ASIC Market Integrity Rules (Futures Markets) 2017*. The Futures Markets Rules replaced the *ASIC Market Integrity Rules (ASX 24 Market) 2010*, the *ASIC Market Integrity Rules (FEX Market) 2013* and *ASIC Market Integrity Rules (Competition in Exchange Markets) 2011*. The Futures Markets Rules can be downloaded from the [Federal Register of Legislation](#).

Note 2: In this guide, ‘Capital Rules’ refers to the *ASIC Market Integrity Rules (Capital) 2021*. The Capital Rules replaced the *ASIC Market Integrity Rules (Futures Markets – Capital) 2017*. The Capital Rules can be downloaded from the [Federal Register of Legislation](#).

Note 3: Guidance on the *ASIC Market Integrity Rules (Securities Markets) 2017* for market participants can be found in [Regulatory Guide 265](#) *Guidance on ASIC market integrity rules for participants of securities markets* (RG 265).

- RG 266.9 The guide also explains how we expect participants to comply with requirements about:
- (a) risk management;
  - (b) supervisory policies and procedures;
  - (c) minimum presence requirements for foreign participants;
  - (d) crossing systems;
  - (e) suspicious activity reporting;
  - (f) client detail record keeping;
  - (g) capital requirements; and
  - (h) technological and operational resilience of critical business services.
- RG 266.10 This guide does not cover the operating rules of market operators or clearing and settlement (CS) facility operators.

## Related guidance

RG 266.11 Table 1 identifies other regulatory guides that may be relevant to market participants.

Note: Guidance on various obligations under the Futures Markets Rules that apply to market operators can be found in [Regulatory Guide 172](#) *Financial markets: Domestic and overseas operators* (RG 172).

**Table 1: Related guidance**

Topic	ASIC regulatory guide
Our guidance for participants of securities markets subject to the Securities Markets Rules	<a href="#">Regulatory Guide 265</a> <i>Guidance on ASIC market integrity rules for participants of securities markets</i> (RG 265)
The disciplinary framework for the market integrity rules, the function of the Markets Disciplinary Panel (MDP), and the policies that the MDP will take into account when making decisions about alleged contraventions of the market integrity rules	<a href="#">Regulatory Guide 216</a> <i>Markets Disciplinary Panel</i> (RG 216)
Notifying ASIC of a range of conduct by Australian financial services (AFS) licensees known as 'reportable situations': see s912DAA	<a href="#">Regulatory Guide 78</a> <i>Breach reporting by AFS licensees and credit licensees</i> (RG 78)
Our approach to supervising compliance with AFS licensing obligations	<a href="#">Regulatory Guide 104</a> <i>AFS licensing: Meeting the general obligations</i> (RG 104) and <a href="#">Regulatory Guide 105</a> <i>AFS licensing: Organisational competence</i> (RG 105)

## B Supervision of trading on domestic licensed financial markets

### Key points

We are responsible for supervising trading on Australian domestic licensed financial markets.

We take a risk-based approach to surveillance of compliance with the market integrity rules and market participants' obligations under the Corporations Act.

### ASIC's supervisory responsibilities

RG 266.12 We are responsible for supervising market participants, market operators and other prescribed entities for compliance with the market integrity rules. This is in addition to our role in supervising compliance by market participants with the market misconduct provisions of the Corporations Act (e.g. the prohibitions against insider trading, market manipulation and making false and misleading statements) and with the general obligations of AFS licensees.

Note 1: For our approach to supervising compliance with the general obligations of AFS licensees under s912A of the Corporations Act, see [RG 104](#) and [RG 105](#).

Note 2: Guidance on market operators' obligations under the Securities Markets Rules can be found in [RG 172](#).

Note 3: Our supervisory responsibilities do not extend to foreign-based markets that are licensed to operate in Australia under s795B(2) or to financial markets that are exempt from being licensed.

### Supervision of compliance with market integrity rules

RG 266.13 We take a risk-based approach to surveillance of compliance with the market integrity rules and market participants' obligations under the Corporations Act. In doing so, we consider the *Objectives and principles of securities regulation* set out by the International Organization of Securities Commissions (IOSCO).

Note: IOSCO, [Objectives and principles of securities regulation](#) (PDF 187 KB), report, 10 June 2010.

RG 266.14 We perform risk assessments of participants and, where necessary, conduct targeted surveillance of suspected misconduct.

RG 266.15 We are responsible for any investigation and action in relation to an alleged breach of the market integrity rules.



### **SFE procedures, determinations and practice notes**

- RG 266.16 In assessing a market participant's compliance with the market integrity rules, we will seek to follow relevant published interpretation as contained in old Sydney Futures Exchange (SFE) procedures, determinations and practice notes. The old SFE procedures, determinations and practice notes that remain relevant are listed in the appendix.
- RG 266.17 In some instances, we have incorporated content from the SFE procedures, determinations and practice notes into the ASIC market integrity rules.

### **Market surveillance**

- RG 266.18 To promote market integrity, we monitor on-market trading activity, including activity in relation to futures market contracts, through a variety of computerised systems.
- RG 266.19 Our Market Surveillance team makes inquiries of market operators, participants, listed entities, clients and others, using compulsory powers where necessary.

### **Disciplinary process**

- RG 266.20 The disciplinary process for breaches of the market integrity rules is contained in [RG 216](#). The MDP exercises ASIC's power to issue infringement notices and accept court enforceable undertakings relating to breaches of the market integrity rules. RG 216 provides guidance on the processes by which matters will be referred to, and dealt with by, the MDP.

## **How ASIC works together with market licensees**

- RG 266.21 Australian market licensees are responsible for the operation of their markets and are required to set operating rules for their markets. These operating rules govern how trading can take place on the market and may, where relevant, deal with entities trading on the market's official list. Market licensees are responsible for monitoring and enforcing compliance with their operating rules.

Note: Guidance on market licensee obligations under the Corporations Act and, for domestic licensees, under the Securities Markets Rules and Futures Markets Rules, can be found in [RG 172](#).

- RG 266.22 ASIC and market licensees conduct site visits of market participants and, where appropriate, share information on supervisory practices.

## Status of notifications, consents, waivers, etc., given before 1 August 2010

RG 266.23 Unless ASIC determines that it should be amended or revoked, any written:

- (a) waiver, exemption, consent, recognition, accreditation, approval, determination or notification given by a market operator to a participant under the operating rules of a market, where those rules are incorporated into the market integrity rules; and
- (b) notification or certification given by market participants to market operators under the operating rules of a market, where those rules are incorporated into the market integrity rules,

is grandfathered and taken to be given by ASIC so as to continue in its existing form, and continue to have the same effect as given under the operating rules: reg 10.15.04 of the *Corporations Regulations 2001* (Corporations Regulations).

Note: Rule 1.6.1 of the Futures Markets Rules provides additional transitional arrangements to ensure the continuity of the status of notifications and certifications given by a market participant to ASIC in accordance with the market integrity rules in force immediately prior to 7 May 2018.

## C ASIC market integrity rules

### Key points

The market integrity rules are made by ASIC and apply to market operators, market participants, other prescribed entities and financial products traded on a licensed market.

We will consult on future amendments to the market integrity rules as required.

We are responsible for supervising compliance with the market integrity rules. We are also responsible for granting waivers from the obligation to comply with a provision of the market integrity rules.

### ASIC market integrity rules

- RG 266.24 We are able to make market integrity rules under Pt 7.2A of the Corporations Act dealing with the activities or conduct of:
- (a) licensed markets;
  - (b) persons in relation to licensed markets; and
  - (c) persons in relation to financial products traded on licensed markets.
- RG 266.25 The market integrity rules are legislative instruments and are subject to parliamentary scrutiny and possible disallowance by Parliament.

### Ministerial consent to market integrity rules

- RG 266.26 We may not make a market integrity rule unless we have the written consent of the Minister. An exception applies for making emergency rules that are necessary, or are in the public interest, to protect people dealing in a financial product.

### Future review and amendment to the market integrity rules

- RG 266.27 We will review the market integrity rules from time to time to make any adjustments required as a result of our experience in administering the rules; developments in the market and the international regulatory environment; and feedback from market operators, participants and clients.
- RG 266.28 We expect to consult on any future amendment of these rules.

## Waivers

### Power to grant a waiver of a market integrity rule

RG 266.29 We are able to grant waivers from the obligation to comply with a provision of the market integrity rules.

RG 266.30 Any such waiver may be general, or limited to a particular case or category, and may be limited by such conditions as we think fit. If conditions are imposed on a waiver, all of the conditions must be complied with for the waiver to be effective. Failure to comply with a condition imposed on a waiver is a contravention of Rule 1.2.2. Further, failure to comply with a condition on a waiver may amount to a possible breach of the relevant market integrity rule waived.

Note: In this guide, 'Chapter 4', 'Part 4.2' and 'Rule 4.2.1' (for example) refer to a chapter, part or rule (respectively) of the Futures Markets Rules, unless otherwise specified.

RG 266.31 We will make a waiver by way of legislative instrument. All legislative instruments, including waivers, are registered on the [Federal Register of Legislation](#) and are publicly available.

RG 266.32 We may withdraw, by legislative instrument, a waiver at any time. We will not grant a waiver retrospectively.

### Approach to considering a market integrity rule waiver

RG 266.33 We will consider and determine all requests for a waiver of a market integrity rule on the basis of the facts, circumstances and merits of each request. In determining whether such a request should be granted, we will take into account commercial considerations against the need to maintain the integrity of the market.

RG 266.34 Where appropriate, we may grant a waiver to a class of persons.

### The process of requesting a waiver

RG 266.35 Any request for a waiver must be in writing. It should also include details of the market integrity rule to be waived, the person or class of persons seeking the waiver, the requested start date and duration of the waiver, the rationale for the waiver, all relevant facts and circumstances in support of the request, and any other relevant information.

RG 266.36 Market participants may be refused a request if they fail to address all of the relevant issues. Similarly, failure to supply relevant information may cause a delay in finalising the request.

RG 266.37 Should a commercially time-sensitive situation arise, we can consider such requests on an urgent basis, providing the participant has clearly

demonstrated that the urgency results from factors beyond their reasonable control and that those factors could not reasonably have been foreseen. Self-imposed deadlines will not be a sufficient basis for urgent consideration.

RG 266.38 Applications for waivers should be submitted through the [ASIC Regulatory Portal](#). Participants will need to pay fees for their application. We have provided details about payment options in the portal. For more information, see [how to apply for relief](#).

### **Publication of waivers**

RG 266.39 All waivers will be publicly available on the [Federal Register of Legislation](#).

RG 266.40 We may also publish notice of a waiver on our website. We maintain a public [register of waivers](#) on our website that contains details of:

- (a) the date a waiver takes effect;
- (b) the person or class of persons relieved from the obligation in the market integrity rule;
- (c) the provision of the market integrity rule to which the waiver applies;
- (d) brief reasons for the waiver; and
- (e) any conditions that apply to the waiver.

## D Communicating with ASIC

### Key points

Market participants can contact ASIC directly to ensure that market integrity matters are known and addressed in an efficient and timely manner.

Market participants should use the forms available on the [ASIC Regulatory Portal](#) to submit certain information to us as required under the market integrity rules.

Other contact points include direct email and telephone access to the relevant ASIC teams to communicate issues and queries about markets, trading and participant conduct.

Breaches of the market integrity rules and/or provisions of the Corporations Act should be reported in accordance with the reportable situations procedures set out in [RG 78](#).

### Forms

- RG 266.41 Details about the type of information that is required to be submitted to ASIC in writing are contained in the market integrity rules.
- RG 266.42 Market participants should use the forms available on the [ASIC Regulatory Portal](#) to submit certain information to us as required under the market integrity rules. If you encounter issues while using the portal, contact [market.participants@asic.gov.au](mailto:market.participants@asic.gov.au).
- RG 266.43 Table 2 lists some of the matters market participants will need to notify ASIC about. Note that this list is not exhaustive.

**Table 2: What market participants must notify ASIC about**

<b>All market participants</b>	Reportable situations (s912DAA)
<b>Futures markets participants</b>	Trust account reconciliation breaches (Part 2.3) Suspicious activity reports (Rule 3.6.1) Crossing systems and suspicious activity reports (Chapter 5) Investigations into participants (Part 2.1) Becoming aware of a major event (Rule 8B.4.1(6))

## Contacting ASIC

RG 266.44 The market integrity rules require market participants to provide ASIC with information and other notifications in certain circumstances. Information should be provided in the manner detailed in the relevant market integrity rule.

### Written applications and requests

RG 266.45 Requests and applications should be made to ASIC using the relevant form on the [ASIC Regulatory Portal](#). If you encounter issues while using the portal, contact [market.participants@asic.gov.au](mailto:market.participants@asic.gov.au).

### ASIC Regulatory Portal

RG 266.46 Market participants can submit a range of applications and notifications using the forms available on the [ASIC Regulatory Portal](#). Where a form is available on the portal, participants should use the portal to make the application or notification.

### Telephone hotline

RG 266.47 Market participants can directly contact the relevant ASIC teams by calling our markets-related hotline on 1300 029 454 between 9 am and 5 pm Eastern Standard Time on market trading days. The hotline is for communicating with ASIC about live markets trading issues, non-live markets queries, general participant queries, notifications and exemptions. Participants can also call ASIC's Client Contact Centre on 1300 300 630.

### Email

RG 266.48 There are three email addresses set up for use by market participants for market- and participant-related matters: see Table 3 for details.

**Table 3: ASIC email addresses for use by market participants**

Email address	To be used for:	Examples of information, applications and notifications
<a href="mailto:feedback.breach@asic.gov.au">feedback.breach@asic.gov.au</a>	Reportable situations under s912D of the Corporations Act	Queries regarding reportable situations Market participants must lodge notifications of reportable situations under s912DAA via the <a href="#">ASIC Regulatory Portal</a> . Further guidance is given in <a href="#">RG 78</a>
<a href="mailto:markets@asic.gov.au">markets@asic.gov.au</a>	Matters relating to markets and trading	Concerns or queries about trading anomalies Queries about unexplained market events Concerns about misconduct in the market
<a href="mailto:market.participants@asic.gov.au">market.participants@asic.gov.au</a>	Participant-related matters	General participant queries

## When to contact ASIC

- RG 266.49 As stated above, we are responsible for supervising trading activities by market participants to ensure market integrity. As such, we can be contacted about conduct and activities that occur on domestic licensed financial markets.
- RG 266.50 Australian market licensees retain responsibility for the operation of their markets. Queries about the operations and processes of markets should be directed to the relevant market operator.
- RG 266.51 In general terms, if your issue relates to an obligation or conduct covered by the market integrity rules or provisions of the Corporations Act, you should contact ASIC. The following examples indicate the sorts of matters that might arise and who to contact.

### Example 1: Expiry of a futures contract

Participant A has a trading-related query about the expiry of a futures market contract.

- Where the query is about the delivery or process of the futures market contract, Participant A should contact the operator of the market on which the futures market contract is traded.
- Where the query is about possible manipulation in relation to the futures market contract or market misconduct, Participant A should contact ASIC.

### Example 2: Crossings

Participant A has a trading-related query about conducting crossings.

- Participant A should contact the relevant market operator to confirm what products, times and procedures apply as this is an operational issue.
- Where the query is about the interpretation of specific Futures Markets Rules (e.g. rules relating to wash trading, pre-negotiation or block trades), Participant A should contact ASIC.

### Example 3: Market manipulation

Participant A has a trading-related query about possible market manipulation by one of their clients.

- Participant A should contact ASIC.

### Example 4: Trade cancellations

Participant A has a trading-related query about trade cancellations.

- Participant A should contact the relevant market operator.



## Notifying ASIC of reportable situations

RG 266.52 Breaches (or likely breaches) of market integrity rules may constitute reportable situations for AFS licensees under s912D. If certain breaches of the market integrity rules are required to be reported under s912DAA, market participants need to report them to ASIC. The process for notifying ASIC of reportable situations under s912DAA and reporting significant breaches of market integrity rules to ASIC is the same.

RG 266.53 Guidance on how to notify ASIC of a reportable situation by AFS licensees under s912DAA is set out in [RG 78](#). You must report to ASIC using the prescribed form on the [ASIC Regulatory Portal](#).

Note: See RG 78 for further guidance on the process for notifying ASIC of reportable situations, and how we deal with these notifications.

## E Risk management

### Key points

Market participants must meet certain risk management requirements for their house accounts, including setting and documenting appropriate limits, and requirements relating to terminal connections.

### Risk management requirements for market participants

RG 266.54 Market participants that are principal traders have not traditionally accessed futures markets directly and, in those cases, their order and position limits have been set by the market participant that provides them with access to the market. This is because the market participant that provides the principal trader with access to the market must meet certain risk management obligations (including setting order and position limits) for the principal trader as its client: Rule 2.2.1.

RG 266.55 There are now an increasing number of principal traders accessing futures markets directly, rather than as clients of another market participant. There has also been an increase in automation and innovation in electronic trading more generally, including proprietary trading.

Note: A principal trader is a market participant that trades only on its own behalf.

RG 266.56 To deal with these changes occurring in market structure and the electronic market environment, Rule 2.2.1 requires all market participants that execute trades on behalf of a house account on a futures market to meet certain risk management requirements: see Table 4.

Note: The term ‘house account’ is defined in Rule 1.4.3.

**Table 4: Risk management—House account requirements**

Requirement	Description
Order and/or position limits	<p>A market participant must demonstrate prudent risk management procedures by setting and documenting appropriate predetermined order and/or position limits on each of its house accounts, including a volume per order limit, an aggregate loss limit and an aggregate net session limit</p> <p>These limits must be:</p> <ul style="list-style-type: none"> <li>• based on the market participant’s analysis of its financial resources or other relevant factors; and</li> <li>• input into trading platform account maintenance by the market participant’s risk manager</li> </ul>

Requirement	Description
Maximum price change limits	<p>A market participant must set and document maximum price change limits in relation to house accounts</p> <p>These limits must be input into trading platform account maintenance by the market participant's risk manager</p>
System requirements	<p>A market participant's order system for execution of trades on the house account must have the capability for:</p> <ul style="list-style-type: none"> <li>• setting limits; and</li> <li>• rejecting orders that are in excess of the limits set</li> </ul>
Amendment of limits	<p>A market participant may amend the predetermined order and/or position limits based on its analysis of financial resources or other relevant factors for house accounts</p>
Terminal connections	<p>Where a market participant has connected to a terminal for the purposes of allowing trading for a house account, it:</p> <ul style="list-style-type: none"> <li>• is responsible under the rules for any orders entered through the terminal on behalf of the house account; and</li> <li>• must promptly take all steps necessary to terminate such a connection when notified to do so by ASIC</li> </ul>
Accessing terminal connections	<p>Before connecting to a terminal for the purposes of allowing trading for a house account, and at all times while so connected, a market participant must:</p> <ul style="list-style-type: none"> <li>• have the necessary skills, facilities and procedures to operate such a facility;</li> <li>• understand the risks and obligations attached to the use of such a facility;</li> <li>• ensure that each order so placed, and any order system, complies with the rules;</li> <li>• provide appropriate controls on access to passwords of the market participant and its employees to such systems; and</li> <li>• ensure appropriate controls are implemented for the security of its premises and physical access of the market participant and its employees to such systems</li> </ul>

Note: [ASIC Market Integrity Rules \(Futures Markets\) Class Waiver 2018/313](#) provides a conditional waiver from the aggregate loss limit requirement in specified circumstances.

## Setting and documenting limits

RG 266.57 A market participant must demonstrate prudent risk management procedures. This includes, but is not limited to, setting and documenting:

- (a) appropriate predetermined order and/or position limits on each of its house accounts, including a volume per order limit, an aggregate loss limit and an aggregate net session limit, based on the market participant's analysis of its financial resources or other relevant factors; and
- (b) maximum price change limits (Rules 2.2.1(1)(ab) and (b)).

Note: [ASIC Market Integrity Rules \(Futures Markets\) Class Waiver 2018/313](#) provides a conditional waiver from the aggregate loss limit requirement in specified circumstances.

- RG 266.58 The limits determined in Rules 2.2.1(1)(a), (ab) and (b) must be input by a market participant's risk manager into trading platform account maintenance and will be established as preset accounts: Rule 2.2.1(1)(c). The 'risk manager' is the person responsible for managing risks within the market participant's business, and their role and responsibilities will depend on the nature, scale and complexity of the market participant's business.
- RG 266.59 A market participant may amend the predetermined order and position limits referred to in Rules 2.2.1(1)(ab) and (b) based on its analysis of financial resources or other relevant factors: Rule 2.2.1(e).
- RG 266.60 In addition to the limits referred to in Rules 2.2.1(1)(ab) and (b), a market participant's order system for execution of trades on the house account must also have the capability for:
- (a) setting limits that reflect prudent account risk management; and
  - (b) rejecting orders that are in excess of limits set by the market participant (Rule 2.2.1(1)(d)).

### Principal traders

- RG 266.61 A principal trader is a market participant that trades only on its own behalf. The principal trader is either:
- (a) a client of another market participant on a futures market where that other market participant permits the principal trader to connect to a terminal. The principal trader's orders are routed directly through the terminal onto the trading platform and are subject to the terminal's risk management system, but will usually bypass the market participant's order system (see RG 266.65–RG 266.67 and Figure 1);
  - (b) a client of another market participant on a futures market where the principal trader's orders are subject to the market participant's order system and the terminal's risk management system (see RG 266.68–RG 266.70 and Figure 2); or
  - (c) granted trading permission by ASX and given its own terminal (see RG 266.71–RG 266.74 and Figure 3).

Note: A 'terminal' (sometimes referred to as a 'gateway') is defined under Rule 1.4.3 as an automated order entry interface through which an order system routes orders to the trading platform of a market. An 'order system' is the software application for entering orders into the trading platform through a terminal.

- RG 266.62 In each of these scenarios, the principal trader has an obligation under Rule 2.2.1(1) to demonstrate prudent risk management procedures. This includes, but is not limited to, ensuring that the principal trader's order

system has the capability for setting limits that reflect prudent account risk management, and for rejecting orders that are in excess of those limits.

RG 266.63 However, when a principal trader engages in trading as set out in RG 266.61(a)–RG 266.61(b), the principal trader does not access the market directly and may not have the capability to set, document and input into trading platform account maintenance predetermined order or position limits on its house account. We have therefore granted [\*ASIC Market Integrity Rules \(Futures Markets\) Class Waiver 2018/312\*](#) (under Rule 1.2.1) for principal traders that engage in trading as set out in RG 266.61(a)–RG 266.61(b). This waiver relieves these principal traders from the obligation to comply with Rules 2.2.1(1)(ab), (b), (c) and (e).

RG 266.64 In these circumstances, the market participant that provides the principal trader with access to the market has obligations under Rule 2.2.1 to:

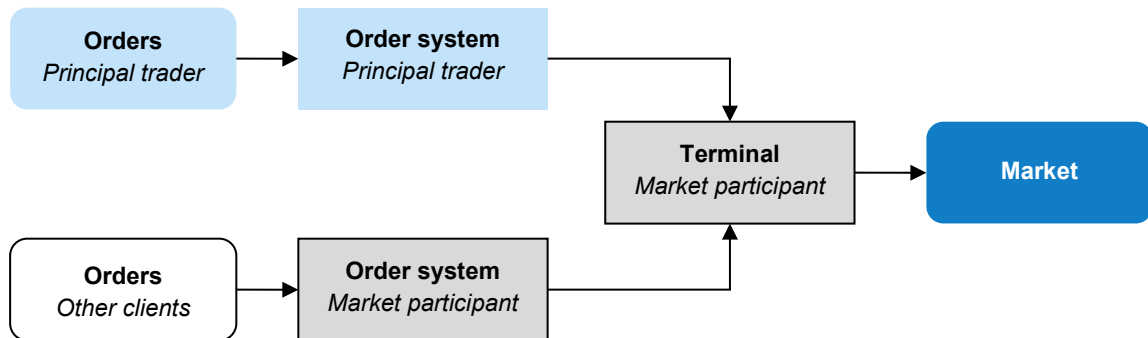
- (a) set and document appropriate predetermined order and/or position limits on each of its client accounts (including its client account for the principal trader) (Rule 2.2.1(1)(a));
- (b) set and document maximum price change limits (Rule 2.2.1(1)(b)); and
- (c) input the limits referred to in (a) and (b) above into trading platform account maintenance for each of its client accounts (including its client account for the principal trader) (Rule 2.2.1(1)(c)).

#### **Client of a market participant—Orders bypass market participant's order system**

RG 266.65 When a principal trader engages in trading as set out in RG 266.61(a) and Figure 1, the market participant responsible for access to the terminal has an obligation under Rule 2.2.1(1)(a) to set and document predetermined limits for the principal trader as its client, and an obligation under Rule 2.2.1(1)(b) to set and document maximum price change limits. The principal trader may rely on the relief in *ASIC Market Integrity Rules (Futures Markets) Class Waiver 2018/312*.

RG 266.66 The principal trader may set tighter and/or differing limits within its own order system at an individual trader or group level.

RG 266.67 The principal trader must document the limits that it has set in its own order system. The principal trader must ensure its order system complies with Rules 2.2.1(1)(d) and (f).

**Figure 1: Principal trader's orders bypass market participant's order system**

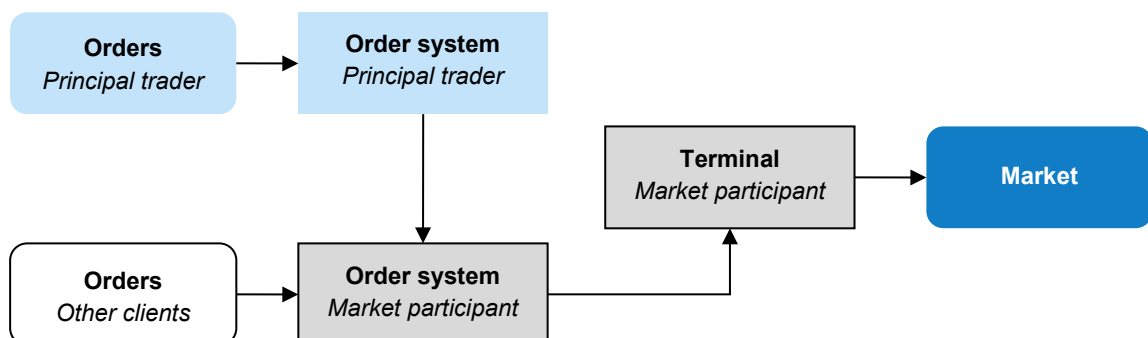
Note: See RG 266.61(a) for the processes set out in this flowchart (accessible version).

### Client of a market participant—Orders subject to market participant's order system

RG 266.68 When a principal trader engages in trading as set out in RG 266.61(b) and Figure 2, the market participant responsible for access to the terminal has an obligation under Rule 2.2.1(1)(a) to set and document predetermined limits for the principal trader as its client, and an obligation under Rule 2.2.1(1)(b) to set and document maximum price change limits. The principal trader may rely on the relief in *ASIC Market Integrity Rules (Futures Markets) Class Waiver 2018/312*.

RG 266.69 The principal trader's orders will also be subject to the limits set by the market participant in the market participant's order system. The principal trader may set tighter and/or differing limits within its own order system at an individual trader or group level.

RG 266.70 The principal trader must document the limits that the principal trader has set in its own order system. The principal trader must ensure that its order system complies with Rules 2.2.1(1)(d) and (f).

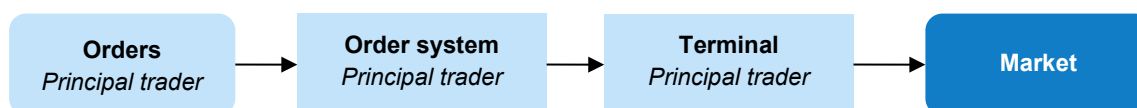
**Figure 2: Principal trader's orders are subject to market participant's order system**

Note: See RG 266.61(b) for the processes set out in this flowchart (accessible version).

### Granted trading permission by the market operator

- RG 266.71 When a principal trader engages in trading as set out in RG 266.61(c) and Figure 3, the principal trader has direct access to the risk management tools that are provided as part of the software associated with the terminal.
- RG 266.72 The principal trader has an obligation under Rule 2.2.1(1)(ab) to set and document predetermined limits for each of its house accounts, and an obligation under Rule 2.2.1(1)(b) to set and document maximum price change limits.
- RG 266.73 The principal trader may also set tighter and/or differing limits within its own order system at an individual trader or group level.
- RG 266.74 The principal trader must document the limits it has set in its order system. The principal trader must ensure its order system complies with Rules 2.2.1(1)(d) and (f).

**Figure 3: Principal trader granted trading permission by a market operator**



Note: See RG 266.61(c) for the processes set out in this flowchart (accessible version).

## Terminal connections

- RG 266.75 Any market participant, including a principal trader, who has connected to a terminal for the purposes of trading will be responsible under the Futures Markets Rules for any orders entered through the terminal: Rules 2.2.1(2)(a) and (ab).
- RG 266.76 We may give notice to a market participant requiring it to terminate a connection referred to in RG 266.75. As soon as a market participant receives notification, it must promptly take all steps necessary to terminate the connection: Rules 2.2.1(2)(b) and (c).

### Filters and filter parameters

- RG 266.77 As a market participant that has connected to a terminal is responsible for all orders entered through the terminal and must ensure those orders and the order system comply with the Futures Markets Rules (Rules 2.2.1(2)(a) and (ab) and Rule 2.2.1(4)(c)), we expect the market participant to apply appropriate filters and filter parameters to its order system.

- RG 266.78 What constitutes ‘appropriate’ will depend on the market participant’s order system capabilities; the nature, scale and complexity of its business; and the particular risks that the market participant has assessed as relevant to that business (including financial, reputational and regulatory risks).
- RG 266.79 Filters and filter parameters are pre-trade controls and the principal means by which trading messages are checked to ensure they comply with the rules. Filters are a set of rules that apply to an order system and determine automatically which trading messages (or series of related trading messages) meet a predefined set of criteria and can pass into the trading platform.
- RG 266.80 Filter parameters are the variables within each filter that can be changed to modify the operation of the filter without changing the rule to which the filter applies. The filter parameters result in trading messages being handled differently according to factors such as the type, source, size or price of an order, or its relationship with other orders. A filter parameter may apply at a number of different levels—for example, to particular financial products, representatives, authorised persons or clients, and to a dollar or margin value level.

## Accessing terminal connections

- RG 266.81 A market participant that connects to a terminal for the purposes of trading must, before connecting to the terminal and at all times while connected:
- (a) have the necessary skills, facilities and procedures to operate such a facility (Rule 2.2.1(4)(a));
  - (b) understand the risk and obligations attached to the use of such a facility (Rule 2.2.1(4)(b));
  - (c) ensure that each order placed through the terminal, and any order system, complies with the Futures Markets Rules (Rule 2.2.1(4)(c));
  - (d) provide appropriate controls (such as passwords) on any access by the market participant and its employees to such systems (Rule 2.2.1(4)(d)); and
  - (e) ensure appropriate controls are implemented for the security of its premises and physical access by the market participant and its employees to such systems (Rule 2.2.1(4)(e)).
- RG 266.82 We recognise that, given the differences in types of businesses conducted by market participants, there must be some degree of flexibility in determining what constitutes ‘appropriate’ controls for each market participant for the purposes of Rules 2.2.1(4)(d) and (e). The types of controls that a market participant must implement will depend on the nature, scale and complexity of its business, and the particular risks that the market participant has assessed as relevant to that business (including financial, reputational and regulatory risks).



**Example: Risk management for internet-based order systems**

XYZ Pty Ltd is a market participant that uses an internet-based order system to allow either clients or their principal traders to enter orders through a terminal into the trading platform. Each client or principal trader is granted remote access to the order system, allowing them to enter orders through the terminal 24 hours a day from their home computer or any other computer.

XYZ Pty Ltd must ensure that its order system and remote access to the system is subject to appropriate security measures such as passwords, firewalls and other security-related software.

XYZ Pty Ltd must also ensure that appropriate controls are implemented for the security of its premises and physical access of the market participants and its clients or principal traders to the order system. We would expect XYZ Pty Ltd to have appropriate policies and procedures in place outlining its security expectations for those who may be placing orders from locations other than the market participant's business premises.

## F Trust account reconciliation reporting

### Key points

Market participants are required to notify ASIC in writing of matters concerning client money reconciliations.

### Trust account reconciliation reporting

RG 266.83 All market participants holding client money (both clearing and non-clearing participants) must complete daily and monthly reconciliations of client money: Rules 2.3.2 and 2.3.3.

#### Daily reconciliation of client money

RG 266.84 Daily reconciliations are an essential part of a market participant's compliance processes for protecting client money. In an insolvency situation, client money can be at risk if it is not properly segregated or accounted for.

RG 266.85 Rule 2.3.4 requires a market participant to notify ASIC, in writing, within two business days if:

- (a) a trust account reconciliation has not been performed in accordance with Rule 2.3.2;
- (b) the reconciliation found the total deposits to be less than total third-party client money; or
- (c) the market participant is unable to reconcile its clients' segregated accounts under Rule 2.3.2.

RG 266.86 If the matter is a significant breach of the Futures Markets Rules, the notification should be submitted using the relevant form on the [ASIC Regulatory Portal](#): see RG 266.52–RG 266.53.

RG 266.87 If the matter is not reportable as a significant breach, the notification should also be submitted using the relevant form on the [ASIC Regulatory Portal](#).

#### Monthly reconciliation of client money

RG 266.88 All market participants holding client money (both clearing and non-clearing participants) must lodge a monthly reconciliation of client money with ASIC within one month after the end of each month: Rule 2.3.3. The monthly reconciliation should be lodged through the [ASIC Regulatory Portal](#).

## G Capital requirements

### Key points

The market integrity rules for capital and reporting do not apply if the market participant is a principal trader only, a clearing participant of an approved clearing facility or an authorised deposit-taking institution.

A market participant should lodge capital returns using the [ASIC Regulatory Portal](#).

### Scope, application and waivers

RG 266.89 This section provides guidance on the Capital Rules.

Note: In this guide, 'Capital Rules' refers to *ASIC Market Integrity Rules (Capital) 2021*.

RG 266.90 The Capital Rules set out the capital and reporting requirements for participants of futures and securities markets. The market integrity rules for capital and reporting do not apply if the market participant is a principal trader only, a clearing participant of an approved clearing facility or an authorised deposit-taking institution. A clearing participant must comply with the CS facility's capital and reporting requirements.

Note: In June 2021, ASIC made the Capital Rules. The Capital Rules replaced *ASIC Market Integrity Rules (Futures Markets – Capital) 2017* and *ASIC Market Integrity Rules (Securities Markets – Capital) 2017*.

### Lodging forms and returns

RG 266.91 A market participant should lodge capital returns using the [ASIC Regulatory Portal](#): Rule 9.4.2 of the Capital Rules.

RG 266.92 Market participants that belong to multiple futures markets (e.g. participants of both the ASX 24 market and the FEX market) only need to lodge one return.

### ASX guidance materials on capital

RG 266.93 Prior to 1 August 2011, the ASX Operating Rules set out capital requirements for market participants. These capital requirements were administered with the benefit of guidance materials issued by ASX Group—in particular, the *Capital Liquidity Handbook* and the *Capital Requirements Guidance*.

- RG 266.94 As such, we will take into account the *Capital Liquidity Handbook* and the *Capital Requirements Guidance* when interpreting the Capital Rules to the extent they are relevant.
- RG 266.95 In future, we may consider reviewing our policy position on these guidance materials in light of changes in the market or other factors. If so, we will consult with industry at that stage.

## H Good fame and character requirement

### Key points

Market participants are obliged to ensure that all persons involved in the business in connection with the relevant market are of good fame and character and high business integrity: Rule 2.2.3(1).

To satisfy itself that a person meets this requirement, a market participant should consider the factors in Rule 2.2.3(2)(b). This list is neither prescriptive nor exhaustive. A market participant may exercise its own discretion when making this assessment.

A person will not meet this requirement if they are disqualified from managing a corporation or insolvent under administration: Rule 2.2.3(2)(a).

- RG 266.96 A market participant must ensure that all persons involved in its business in connection with the relevant market are of good fame and character and high business integrity: Rule 2.2.3(1).
- RG 266.97 Under Rule 2.2.3(2)(b), when assessing whether a person is of good fame and character and high business integrity, a market participant should consider whether the person has been:
- (a) convicted of any offence;
  - (b) disciplined by or adversely mentioned in a report of a government or governmental authority or agency;
  - (c) adversely mentioned in a report of a market operator, a clearing facility, a settlement facility or any other exchange; or
  - (d) disciplined by a market operator, a clearing facility, a settlement facility or any other exchange.
- RG 266.98 Under Rule 2.2.3(2)(a), a person will not be of good fame and character if they are:
- (a) disqualified from managing a corporation under the Corporations Act (or under the law of another country); or
  - (b) an insolvent under administration (or its equivalent in another country).
- RG 266.99 Aside from the express circumstance in Rule 2.2.3(2)(a), none of the limbs in Rule 2.2.3(2)(b) will serve to determine that a person is not of good fame and character. Rule 2.2.3 does not prescribe the checks that a market participant must do in order to satisfy this requirement.
- RG 266.100 A market participant may exercise its own discretion to satisfy itself that a person is of good fame and character and high business integrity. The market participant may consider:
- (a) the facts and circumstances as a whole; and
  - (b) any procedural fairness and due process requirements relating to persons involved in its business in connection with the relevant market.

## I Supervisory policies and procedures

### Key points

Market participants must have appropriate supervisory policies and procedures in place to ensure compliance with the Futures Markets Rules, operating rules and Corporations Act.

Supervisory policies and procedures should be in writing and tailored to the nature, size and complexity of the market participant's business.

- RG 266.101 Rule 2.2.8 requires a market participant to have appropriate supervisory policies and procedures to ensure compliance by the market participant, and each person involved in its business as a market participant, with the Futures Markets Rules, operating rules and the Corporations Act.
- RG 266.102 A distinction can be drawn between compliance procedures and supervisory procedures. Compliance procedures generally cover the applicable rules and policies and describe prohibited practices. Supervisory procedures document the supervisory system that has been established to ensure that the compliance procedures are being followed, and to prevent and detect prohibited practices.
- RG 266.103 We expect a market participant to be able to demonstrate that it has established, maintained and continues to enforce supervisory policies and procedures that are tailored to the nature, size and complexity of its business. A market participant should also undertake periodic reassessment of its supervisory policies and procedures in light of changes to its business.
- RG 266.104 We expect a market participant's supervisory policies and procedures to be in writing and to be designed to reasonably supervise the business and each person involved in the business.
- RG 266.105 We also expect a market participant to maintain evidence that supervisory policies and procedures have been implemented and carried out, and make this available to ASIC on request. A market participant should be able to demonstrate that it has allocated sufficient personnel and system resources to implement the supervisory policies and procedures.

## J Foreign participants: Minimum presence requirements

### Key points

To facilitate enforcement action against foreign market participants on the futures markets that do not hold an AFS licence, Part 2.4 of the Futures Markets Rules imposes minimum presence requirements on those foreign market participants.

- RG 266.106 Under the Corporations Act, market participants must comply with the market integrity rules that apply to the market(s) on which they trade. This includes foreign market participants—that is, those participants that are foreign entities and are not required to hold an AFS licence.
- RG 266.107 Part 2.4 of the Futures Markets Rules imposes minimum presence requirements on foreign market participants of futures markets if those foreign market participants do not hold an AFS licence. This is to facilitate enforcement action in Australia for breaches by foreign market participants of the relevant market integrity rules, the *Australian Securities and Investments Commission Act 2001* (ASIC Act), the Corporations Act more broadly, the *Corporations (Fees) Act 2001*, the *ASIC Supervisory Cost Recovery Levy Act 2017* and the *ASIC Supervisory Cost Recovery Levy (Collection) Act 2017*.
- RG 266.108 Our ability to take effective enforcement action is fundamental to the supervision of financial markets and ensuring that markets are fair and efficient. The Corporations Act already facilitates enforcement actions against those market participants that are foreign entities that hold an AFS licence.
- RG 266.109 To facilitate enforcement action in Australia, a foreign market participant of a futures market must execute and lodge with ASIC a deed that contains certain provisions. This deed is for the benefit of, and is enforceable by, ASIC (and other persons referred to in s659B(1) of the Corporations Act) and continues to apply even if the foreign market participant has ceased to be a market participant of a futures market in Australia.
- RG 266.110 The deed must be irrevocable (except with the prior written consent of ASIC) and provide that the foreign market participant will:
- (a) submit to the non-exclusive jurisdiction of the Australian courts in legal proceedings (whether brought in the name of ASIC or the Crown or otherwise) that are conducted:
    - (i) by ASIC (including under s50 of the ASIC Act); and

- (ii) for proceedings relating to a financial services law, by any entity referred to in s659B(1);

Note: The entities referred to in s659B(1) (which permits certain entities to commence court proceedings relating to a takeover bid or a proposed takeover bid) are certain Commonwealth, state and territory entities. We have referred to 's659B(1) entities' here and in the Futures Markets Rules, rather than replicating the s659B(1) list of entities.

- (b) comply with any order of an Australian court for any matter relating to the activities or conduct of the foreign market participant in relation to the relevant futures market, or in relation to financial products traded on the relevant futures market, including but not limited to any matter relating to its obligations under the:
  - (i) ASIC Act;
  - (ii) Corporations Act;
  - (iii) *Corporations (Fees) Act 2001*;
  - (iv) *ASIC Supervisory Cost Recovery Levy Act 2017*; and
  - (v) *ASIC Supervisory Cost Recovery Levy (Collection) Act 2017*;
- (c) if the foreign market participant is not registered under Div 2 of Pt 5B.2 of the Corporations Act, appoint a local agent (a natural person or a company) that is resident in this jurisdiction and authorised to accept service of process and notices on behalf of the foreign market participant;
- (d) notify ASIC of any change to the agent or the name and address of the agent (if the agent is a company, the address will be the registered office of the company);
- (e) accept service on the agent as service of process on the foreign market participant in relation to any legal proceedings conducted by ASIC, the Crown or otherwise;
- (f) ensure that the deed applies even if the foreign market participant ceases to be a market participant; and
- (g) comply with any additional terms notified by ASIC to the foreign market participant (Rule 2.4.1(2)).

RG 266.111 The original deed must be dated and it must be signed by a person authorised by the foreign market participant to do so on its behalf. If the foreign market participant is an unincorporated entity, the foreign market participant must provide an authority for the person to sign the deed.



## K Suspicious activity reporting

### Key points

Under Rule 3.6.1, a market participant must notify ASIC if it has reasonable grounds to suspect that a person has placed an order or entered into a transaction:

- while in possession of inside information; or
- which has the effect of creating or maintaining an artificial price or a false or misleading appearance in the market or price for trading in financial products.

See RG 266.113–RG 266.120.

We do not expect a market participant to actively seek to detect reportable matters: see RG 266.121–RG 266.132.

A market participant should have a clear, well-understood and documented process for complying with its obligations under Rule 3.6.1: see RG 266.147–RG 266.151.

Notifying ASIC of a reportable matter under Rule 3.6.1 does not relieve market participants from compliance with other obligations, including notifying ASIC of reportable situations under s912DAA of the Corporations Act and other reporting requirements to AUSTRAC: see RG 266.152–RG 266.161.

Where a market participant has reported information to AUSTRAC under anti-money laundering (AML) reporting legislation, it is not required to notify ASIC of the same information under Rule 3.6.1: see RG 266.158.

- RG 266.112 This section provides guidance on a market participant’s obligations under Part 3.6 of the Futures Markets Rules. This includes guidance on the obligations for market participants operating a crossing system on a financial market in this jurisdiction.

Note: The obligations of a futures market participant under Part 3.6 of the Futures Markets Rules are equivalent to the obligations of a securities market participant under Part 5.11 of the Securities Markets Rules.

### What suspicious activity must be reported?

- RG 266.113 Under Rule 3.6.1, a market participant must notify ASIC in writing, as soon as practicable, if it has reasonable grounds to suspect that:
- (a) a person has placed an order or entered into a transaction on a market while in possession of inside information; or

- (b) a transaction, or an order transmitted to a trading platform of a market, has or is likely to have the effect of:
  - (i) creating an artificial price for trading in financial products on a market;
  - (ii) maintaining at a level that is artificial (whether or not it was previously artificial) a price for trading in financial products on a market;
  - (iii) creating or causing the creation of a false or misleading appearance of active trading in financial products on a market; or
  - (iv) creating or causing the creation of a false or misleading appearance with respect to the market, or price, for trading in financial products on a market.

These are collectively referred to as ‘reportable matters’ in this guide.

Note: Rule 5.4.2 sets out the obligations of a crossing system operator in relation to reportable matters. As noted in RG 266.227, the guidance in this section applies to crossing system operators’ obligations to report suspicious activity on a crossing system.

- RG 266.114 Market participant notifications under Rule 3.6.1 provide ASIC with a valuable supplementary source of market intelligence which, when combined with other information available to ASIC, helps us to focus our investigations and resources.
- RG 266.115 Rule 3.6.1 requires a market participant to notify ASIC in writing with details of the relevant transaction or order, and the reasonable grounds it has to suspect there is a reportable matter: see RG 266.133–RG 266.140 for guidance on the meaning of ‘reasonable grounds to suspect’ and RG 266.165–RG 266.167 for guidance on the content of notifications under Rule 3.6.1.
- RG 266.116 The obligation to notify ASIC in writing under Rule 3.6.1 arises whether or not a market participant has knowledge of all the details surrounding the transaction or order, the identity of any insider (if the reportable matter relates to a person trading with inside information) or the intention of any party to a transaction or order (if the reportable matter relates to the effect on a market).
- RG 266.117 Market participants also have an obligation to submit suspicious matter reports (SMRs) to the Australian Transaction Reports and Analysis Centre (AUSTRAC) under s41 of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (AML/CTF Act) and s16 of the *Financial Transaction Reports Act 1988* (FTR Act) (collectively referred to in this guide as ‘AML reporting legislation’). To avoid double reporting, Rule 3.6.1(2) provides that, where a market participant has reported information to AUSTRAC under AML reporting legislation, it is not required to notify ASIC of the

same information under Rule 3.6.1(1): see RG 266.157–RG 266.161 for further information about the interaction between Rule 3.6.1 and the AML reporting legislation.

- RG 266.118 Under Rule 3.6.2, a market participant must not disclose to any person that it has notified ASIC of a reportable matter, nor disclose the information contained in the notification: see RG 266.168 for further information about Rule 3.6.2, including exceptions to the rule.
- RG 266.119 Under Rule 3.6.1, a market participant is not required to form a view about whether a person has, or would have, a defence available if prosecuted for a contravention of any provision of the Corporations Act or any market integrity rule, or about whether all the elements of insider trading or market manipulation exist.
- RG 266.120 A market participant will need to decide on a case-by-case basis whether there are reasonable grounds to suspect there is a reportable matter. Table 5 and Table 6 provide guidance on when we would generally expect a market participant to consider notifying ASIC under Rule 3.6.1. These examples are not intended to provide an exhaustive list. There will be situations that do not fall squarely within any of the examples included in this guide where there would be reasonable grounds to suspect that a reportable matter has occurred.

### **Obligation to report, not actively investigate**

- RG 266.121 We do not expect a market participant to actively seek to detect reportable matters for the purposes of Rule 3.6.1. Rather, the rule requires market participants to report activity they become aware of in the ordinary course of their client and proprietary trading activities.
- RG 266.122 The obligation under Rule 3.6.1 is to report information that is known. The obligation under Rule 3.6.1 does not require a market participant to put in place new surveillance arrangements to detect circumstances that may trigger a reporting obligation.
- RG 266.123 As part of its arrangements to comply with its current obligations under the law, a market participant will have in place existing trading safeguards and monitoring mechanisms. These may include system alerts, and procedures and processes which, at a minimum:
- (a) enable it to consider the circumstances of an order set out in Rule 3.1.2(3) to prevent the submission of orders that have the effect of, or are likely to have the effect of, creating a false or misleading appearance of active trading in a contract or with respect to the market for, or the price of, a contract (Rule 3.1.2);
  - (b) for AFS licensees, ensure that it complies with, and takes reasonable steps to ensure that its representatives comply with, the financial services laws (s912A(1)(c) and (ca) of the Corporations Act).

- RG 266.124 Some market participants may also be subject to obligations under the AML/CTF Act to collect ‘know your customer’ information and conduct ‘ongoing customer due diligence’. We expect that these existing processes will, in some circumstances, be a source of information that a market participant should take into account in determining whether a reportable matter exists (e.g. details of a client’s investment profile or a client’s financial means—see Table 5 and Table 6).
- RG 266.125 If a market participant becomes aware of information, in the course of its business activities and in the course of complying with its existing obligations, that gives rise to reasonable grounds to suspect there is a reportable matter, the market participant must notify ASIC. Not all knowledge, by itself, gives rise to a reportable matter. Table 5 and Table 6 give some examples of information that, by itself, or in combination with certain other information, may give rise to a reportable matter. We do not expect market participants to make specific external inquiries to gather information for the purposes of Rule 3.6.1.

#### **Information in different parts of the organisation**

- RG 266.126 Where information in different parts of a market participant’s business would collectively give rise to a reportable matter, we will take into account whether:
- (a) the information has in fact come together; and
  - (b) it is reasonable to expect the information to have come together (e.g. in the compliance function of the market participant’s business).
- RG 266.127 Once information has come together, we would expect a market participant to notify ASIC in accordance with Rule 3.6.1. Market participants will need to consider which parts of the organisation are required to escalate potentially reportable matters to those responsible for compliance. At a minimum, we expect the trading function of the market participant to escalate potential reportable matters to those responsible for compliance with Rule 3.6.1: see RG 266.145.

#### **Retrospective review**

- RG 266.128 We expect a market participant to notify ASIC of orders or transactions that meet the Rule 3.6.1 criteria at the time they occur. We also expect that the Rule 3.6.1 criteria may be met as a result of information that the market participant becomes aware of after an order has been placed or a transaction entered into (e.g. price-sensitive announcements).
- RG 266.129 Where a market participant conducts retrospective spot checks in the ordinary course of ensuring compliance with its obligations, and discovers information that may give rise to reasonable grounds to suspect there is a reportable matter (e.g. Client A’s trading is inconsistent with its trading history and investment or risk profile, and Client A has made a large profit),

we expect the market participant, at a minimum, to identify this matter for internal escalation and active determination about whether to notify ASIC.

- RG 266.130 Where a market participant has received a notice to produce books or information to ASIC and, through this exercise, becomes aware of particular orders or transactions that may give rise to reasonable grounds to suspect there is a reportable matter, we expect the market participant to identify this matter for internal escalation and determine whether to notify ASIC.
- RG 266.131 We do not expect a market participant to retrospectively review all orders or transactions in light of subsequent events, or information that it later becomes aware of, to detect potentially reportable matters under Rule 3.6.1.
- RG 266.132 The operation of Rule 3.6.1 is not intended to affect current processes that may be conducted by a market participant for other reasons (e.g. post-trade analysis). However, if post-trade analysis reveals any indicators of a reportable matter (see Table 5 and Table 6), a market participant should ensure that the indicators are considered further to determine whether it should notify ASIC under Rule 3.6.1 and/or take any further internal action themselves.

### **What does ‘reasonable grounds to suspect’ mean?**

- RG 266.133 A market participant must notify ASIC if it has reasonable grounds to suspect there is a reportable matter. Establishing ‘reasonable grounds to suspect’ requires both a suspicion and just cause for that suspicion.
- RG 266.134 The test is satisfied by circumstances that would create an actual apprehension or fear that a reportable matter exists. The suspicion has to be honest and reasonable, and must be based on facts that would create suspicion.
- RG 266.135 In *Queensland Bacon Pty Ltd v Rees* (1966) 115 CLR 266, Kitto J described (at 303) a suspicion of something as being:
- ... more than a mere idle wondering whether it exists or not; it is a positive feeling of actual apprehension or mistrust amounting to a ‘slight opinion, but without sufficient evidence’.

This case was applied by the High Court in *George v Rockett* (1990) 170 CLR 104 at 106.

- RG 266.136 A reasonable suspicion can exist without the market participant conducting exhaustive and conclusive investigations into the matter and, as stated above, we do not expect a market participant to conduct external inquiries for this purpose: see RG 266.125. Nor do we expect a market participant to undertake extensive legal analysis to determine whether a contravention of the Corporations Act or market integrity rules has occurred: see RG 266.138.
- RG 266.137 In some instances, there may be legitimate reasons or trading strategies behind conduct that, based on a system alert, suggests that a reportable matter exists. For example, clients may legitimately request the cancellation of

their orders if they believe the market is falling. However, this may be a less plausible explanation if orders are repeatedly entered into the market and cancelled. A market participant will need to exercise judgement in determining whether it should notify ASIC.

### **How much analysis is required?**

- RG 266.138 A market participant is not required to form any view on whether a breach of the Corporations Act or market integrity rules has occurred. We do not expect a market participant to engage in detailed legal analysis to determine whether a particular law applies to the facts, whether an exception may apply in the circumstances, or whether it is aware of the knowledge or intention of the relevant person.
- RG 266.139 We expect all employees of a market participant to have some level of familiarity with, and knowledge of, the laws prohibiting insider trading and market manipulation, corresponding to the nature of their role in the organisation. We would expect that certain indicators of a reportable matter are referred to a compliance officer to ascertain whether a reporting obligation exists under Rule 3.6.1.
- RG 266.140 As a general rule, a market participant should exercise common sense and judgement when deciding whether to notify ASIC. We do not expect a market participant to notify ASIC every time a system alert is generated.

### **Some indicators of reportable matters**

- RG 266.141 In RG 266.142, we provide some indicators that may give rise to a reportable matter. In most cases, one indicator alone will not give rise to reasonable grounds to suspect that a reportable matter has occurred. In most instances, a combination of two or more indicators may lead the market participant to decide there are reasonable grounds to suspect a reportable matter. Table 5 and Table 6 set out our guidance on combinations of indicators that may give rise to reasonable grounds to suspect a reportable matter. A market participant will need to decide, in the context of complying with its other obligations (see RG 266.125), whether further review is necessary after observing one or more indicators. Clear policies and procedures detailing when further review should be conducted will help market participants to comply with Rule 3.6.1.
- RG 266.142 Examples of indicators that a market participant may wish to take into account when considering whether a reportable matter exists include (but are not limited to):
- (a) unusual or unexpected activity—for example:
    - (i) transactions that do not appear to make economic sense;
    - (ii) large volumes of orders or trades;
    - (iii) orders inconsistent with previous investment behaviour or investment profiles;

- (iv) unusually high profits within a short time period; and
- (v) financial commitments entered into by a client that appear beyond the client's means;
- (b) unusual concentration of trading or repetition of trading;
- (c) knowledge of client relationships (e.g. that a client is related to a director of the company that releases a price-sensitive announcement);
- (d) use of multiple accounts for no apparent reason, or accounts in the names of family members or corporate entities with no apparent business purpose or other purpose;
- (e) rapid purchase and sale of derivative products;
- (f) buying and selling derivative products with no discernible purpose;
- (g) instructions to place an order immediately or urgently;
- (h) trades modifying the valuation of a position without affecting the size of the position;
- (i) trades modifying the valuation of an underlying financial instrument to create a price impact on a related derivative;
- (j) orders or trades made outside volume limits, bid–offer spread parameters or any other applicable trading parameters; and
- (k) trading that takes place before the release of a price-sensitive announcement or research report, or ahead of a large house or client order ('front running').

RG 266.143 Table 5 and Table 6 provide detailed examples of how a review of some indicators may lead to reasonable grounds to suspect there is a reportable matter. These examples are not intended to be an exhaustive list of circumstances in which a reportable matter may arise. While Table 5 and Table 6 refer to trading in shares, the indicators are equally relevant for trading in all financial products.

RG 266.144 The presence of one or more of the indicators described in Table 5 and Table 6 is not necessarily conclusive. Conversely, the absence of any of the indicators does not indicate that a reportable matter does not exist. A market participant needs to exercise its own judgement in evaluating whether the presence of certain facts gives rise to reasonable grounds to suspect there is a reportable matter.

RG 266.145 At an individual trader level in a market participant's business, it may be that only one or two of these indicators are visible to the trader. This may, for example, result from the internal separation of a market participant's business as part of its compliance program. We would expect that, in these instances, where the trader has reason to question whether a reportable matter exists, the trader should escalate their observations to the person responsible for compliance. In the normal course of carrying out their responsibilities, the relevant compliance officer would:

- (a) assess these observations in light of all the information they possess; and

- (b) determine, in accordance with the market participant's policies and procedures, whether there are reasonable grounds to suspect there is a reportable matter.

RG 266.146 Once a notification is made, we will consider the information provided and may make further inquiries where appropriate. If a market participant notifies us of a reportable matter, it must not disclose to others that it has done so, except in limited circumstances: see RG 266.168.

**Table 5: Indicators that may combine to give rise to reasonable grounds to suspect that a person is trading while in possession of inside information—Rule 3.6.1(1)(a)**

Primary indicator	Other indicators
Orders or transactions are inconsistent with a client's or trader's recent prior trading history or risk profile	<p>On its own, trading that is inconsistent with a client's or trader's prior trading history or risk profile may not give rise to a reportable matter</p> <p>However, if there are other indicators present, this may give rise to reasonable grounds to suspect that a person is trading while in possession of inside information</p> <p>Other indicators may include:</p> <ul style="list-style-type: none"> <li>• the type of financial product that is the subject of the order or transaction;</li> <li>• the amount invested (including whether this is out of proportion with the client's monetary means or earning capacity);</li> <li>• the risk profile of the client;</li> <li>• the size of the order;</li> <li>• the length of time the security is held;</li> <li>• a significant increase in profit in the client's or trader's account; and</li> <li>• a significant increase in the particular market participant's representative's commission</li> </ul> <p>For example, an order or transaction may give rise to reasonable grounds to suspect a reportable matter if a client places large orders inconsistent with the client's investment profile</p>
An order or transaction occurs immediately before a price-sensitive announcement	<p>Without further knowledge or information, the order or transaction may not give rise to reasonable grounds to suspect that a person is trading while in possession of inside information</p> <p>However, if there are other indicators present, this may give rise to reasonable grounds to suspect that a person is trading while in possession of inside information</p> <p>Other indicators may include the knowledge that the client is connected to (or the compliance officer is aware that the trader is connected to) the company or government department the subject matter of the announcement (front running)</p> <p>For example, the client may be an officer or employee of the company, or the trader may have been involved in providing professional advice to the company</p>



Primary indicator	Other indicators
An order is placed or a transaction entered into immediately after a client opens a new account	<p>Without further knowledge or information, the order or transaction may not give rise to reasonable grounds to suspect that a person is trading while in possession of inside information</p> <p>However, if there are other indicators present, this may give rise to reasonable grounds to suspect that a person is trading while in possession of inside information</p> <p>Other indicators may include instructions for the order to be carried out urgently, without reference to the price at which the order is to be executed</p>
A client or trader opens simultaneous positions in related derivatives (e.g. contracts for difference (CFDs) or options)	<p>Without further knowledge or information, the orders or transactions may not give rise to reasonable grounds to suspect that a person is trading while in possession of inside information</p> <p>However, if there are other indicators present, this may give rise to reasonable grounds to suspect that a person is trading while in possession of inside information</p> <p>Other indicators may include:</p> <ul style="list-style-type: none"> <li>• the trading in the derivatives is inconsistent with the client's or trader's prior trading history or risk profile; and</li> <li>• the trading takes place just before a price-sensitive announcement</li> </ul>
A trading account receives a large transfer of money before an order is placed or a transaction entered into	<p>Without further knowledge or information, the orders or transactions may not give rise to reasonable grounds to suspect that a person is trading while in possession of inside information</p> <p>However, if there are other indicators present, this may give rise to reasonable grounds to suspect that a third party is trading while in possession of inside information and attempting to disguise their own trading by trading through another account or person</p> <p>Another indicator may be that the authorisation on the account has recently changed</p>
A trader is an employee of the market participant and an order is placed, or transaction entered into, ahead of house or client orders in the same security	<p>Without further knowledge or information, the orders or transactions may not give rise to reasonable grounds to suspect that a trader may be profiting from the effect of the house or client orders in the relevant futures contract (front running)</p> <p>However, if there are other indicators present, this may give rise to reasonable grounds to suspect that a person is trading while in possession of inside information</p> <p>Other indicators may include:</p> <ul style="list-style-type: none"> <li>• the employee has not received internal consent for the trade;</li> <li>• the security and size of the order are inconsistent with the employee's prior trading history (as far as the market participant is aware); and</li> <li>• the trading is accompanied by the trader taking simultaneous positions in related derivatives</li> </ul>

Primary indicator	Other indicators
Trading takes place before the release of a research report that has been prepared by the market participant	<p>Without further knowledge or information, the orders or transactions may not give rise to reasonable grounds to suspect that a trader may be profiting from the effect of the house or client orders on the price of the security (front running)</p> <p>However, if there are other indicators present, this may give rise to reasonable grounds to suspect that a person is trading while in possession of inside information</p> <p>Other indicators may include:</p> <ul style="list-style-type: none"> <li>• the employee has not received internal consent for the trade; and</li> <li>• no effective information barriers are in place between the market participant's business units</li> </ul> <p>A market participant may have a research of sales division that prepares research reports that will be released to the public. A trader may intend to profit from the effect that the release of the report will have on the price of the securities that are discussed in the research report (front running)</p>

Note: If the market participant is an AFS licensee, it may also be required to make an assessment about whether a significant breach report is to be made to ASIC under s912D of the Corporations Act.

**Table 6: Indicators that may combine to give rise to reasonable grounds to suspect that an order or transaction may affect market integrity—Rule 3.6.1(1)(b)**

Primary indicator	Other indicators
<p>An order is placed:</p> <ul style="list-style-type: none"> <li>• near the close of the trading day; or</li> <li>• on the last day of the month, quarter, half year or financial year</li> </ul>	<p>The order forms part of a trading pattern where the client or trader regularly chooses to buy high or sell low at the close. This may be a reportable matter where the order would, if executed, represent a significant increase or decrease from the previous trade price ('price support', 'marking the close' or 'window dressing')</p> <p>Other indicators include:</p> <ul style="list-style-type: none"> <li>• the client or trader chooses not to buy or sell at other times of the trading day when better prices are available;</li> </ul> <p>In addition, the client or trader may already hold existing positions in the futures contracts or related derivatives, and have an interest in maintaining the price of the futures at a certain level</p>
An order is placed near the expiry date of related derivatives (e.g. options)	<p>As a general rule, the market participant is not expected to investigate whether a client holds positions in related derivatives. A trader executing a client's order may not be able to 'see' if a client holds, or has open positions in, related derivatives because of the way in which the market participant's business is structured, or the way the client has structured their investments</p> <p>This may raise an early warning signal if the market participant is aware that the client holds positions in related derivatives such as an option that is close to expiry. The order would, if executed, represent a significant increase or decrease from the previous trade price of the underlying futures contract, and thereby increase or decrease the value of the related derivatives. As a result, the client or trader makes a profit or avoids a loss</p>
A client or trader places matched orders—prearranged trades	<p>The order is for a large volume in a futures contract which is relatively illiquid. Immediately after the client's order is placed, an order for a similar volume at the same price is placed on the opposite side of the market. The effect is that the order is executed unusually quickly, given the size of the order and the limited liquidity in the futures contract. This may indicate that the trade is a 'wash trade'</p> <p>We note that this may not always be indicative of suspicious conduct, as legitimate prearranged trading of large volumes must be in accordance with the prearranged trading rules</p>

Primary indicator	Other indicators
A client or trader places multiple orders on the same side of the market at different price levels, which are just behind the best bid or ask	<p>These orders may be intended to create a false or misleading appearance of buying or selling demand ('layering the order book')</p> <p>This may be more suspicious if the client or trader subsequently submits an order on the other side of the market. Once this latter order is executed, the client or trader rapidly removes the initial multiple orders</p>

Note: Rule 3.6.1 does not require the market participant to be aware of the intention of any party to the transaction or order before it notifies ASIC.

## Compliance with Part 3.6

- RG 266.147 To help ensure compliance with the obligation to notify ASIC of reportable matters, a market participant should have a clear, well-understood and documented process for:
- identifying indicators of reportable matters;
  - ensuring that employees escalate potentially reportable matters to compliance staff, who are made aware of the indicators identified;
  - determining whether indicators of reportable matters give rise to an obligation to report; and
  - notifying ASIC in writing of reportable matters.
- RG 266.148 A market participant will need to consider how best to keep these documents or records (e.g. they may be kept electronically). Keeping documents and records (particularly of the determinations made in RG 266.147(c)) will help market participants demonstrate to ASIC compliance with the obligation under Rule 3.6.1.
- RG 266.149 These records may be kept in a similar manner to a register for identifying, recording and reporting reportable situations: see [RG 78](#) at RG 78.136. However, this is not the only method that market participants can use to demonstrate compliance.
- RG 266.150 In enforcing Rule 3.6.1, we intend to focus on instances where market participants are obliged to notify us, but wilfully or recklessly disregard this obligation.
- RG 266.151 We will consider whether a market participant's policies and procedures have been followed, as well as whether the policies are adequate, when deciding whether a market participant has failed to report a reportable matter. Where internal policies and procedures are followed strictly but the market participant is not adequately reporting reportable matters to ASIC, the market participant may need to review its policies and procedures to ensure they are effective.

### How does this relate to other breach reporting obligations?

- RG 266.152 Section 912DAA requires AFS licensees to notify ASIC if there are reasonable grounds to believe that a reportable situation has arisen: see [RG 78](#) for more detail.
- RG 266.153 The obligation to report suspicious conduct under Rule 3.6.1 is in addition to the reportable situations obligations imposed on AFS licensees under s912DAA.
- RG 266.154 In contrast to the breach reporting obligation, Rule 3.6.1 requires notification to ASIC of information relating to the trading activities of clients, other market participants or any other person.
- RG 266.155 In addition, the obligation under Rule 3.6.1 applies to all market participants, not all of whom are AFS licensees (e.g. some foreign market participants are exempt from holding an AFS licence).
- RG 266.156 The reporting obligations in s912DAA and Rule 3.6.1 are distinct. A notification under Rule 3.6.1 does not relieve a market participant that is an AFS licensee from its obligation to report under s912DAA. There may be instances where a reportable matter is notified to ASIC in the first instance, and then, after further inquiry to determine whether it is also a reportable situation by the AFS licensee under s912D, the AFS licensee also notifies ASIC of the reportable situation. In these instances, when submitting a reportable situation notification, it will assist ASIC if market participants advise, in their reportable situation notification, that a suspicious activity report has been made to ASIC and state the date of the suspicious activity report.

### How does this relate to reporting obligations to AUSTRAC?

- RG 266.157 A market participant may have an obligation under AML reporting legislation to submit an SMR to AUSTRAC if it forms a suspicion on reasonable grounds relating to insider trading or market manipulation. Many of these cases may also give rise to reasonable grounds to suspect there is a reportable matter that must be reported to ASIC under Rule 3.6.1(1).
- RG 266.158 To avoid double reporting, Rule 3.6.1(2) provides that, where a market participant has reported information to AUSTRAC under AML reporting legislation, it is not required to notify ASIC of the same information under Rule 3.6.1(1). ASIC has access to SMRs lodged with AUSTRAC.
- RG 266.159 It is important to note that market participants cannot discharge their obligation to report under AML reporting legislation by reporting to ASIC.
- RG 266.160 Market participants should refer to [How to comply and report: guidance and resources](#) on the AUSTRAC website—in particular, [Who and what we regulate: designated services and reporting entities](#) and [Reporting](#)—for more information about their obligations under AML reporting legislation.

RG 266.161 We expect that the processes and procedures that a market participant has in place to comply with Rule 3.6.1 may not be the same as those it has in place to comply with the AML reporting legislation.

### **When must market participants notify ASIC?**

RG 266.162 A market participant must notify ASIC under Rule 3.6.1 as soon as practicable and via the [ASIC Regulatory Portal](#). We would expect that this is within three business days of determining that there is a reportable matter.

RG 266.163 We expect a market participant's internal systems to ensure that the relevant staff are aware of potentially suspicious activity in a timely and efficient manner.

### **What should the notification contain?**

RG 266.164 Notification to ASIC under Rule 3.6.1 must contain details of the transaction or order (to the extent known to the market participant) and the reasons the market participant suspects there is a reportable matter.

RG 266.165 As a general guide, we would expect a notification to contain:

- (a) if known, the name and contact details of the person suspected of trading while in possession of inside information, or who placed the order or entered into the transaction that has, or is likely to have, one of the effects set out in Rule 3.6.1(b);
- (b) the details of the order or transaction that is the subject of the notification, including the contract, market, time of placement, price and volume;
- (c) the recent trading history of the client if the reportable matter arises partly because a market participant considers an order or transaction is inconsistent with a client's recent trading history (i.e. for the previous three months);
- (d) information on the client's investment profile and risk profile if the reportable matter arises partly because a market participant considers an order or transaction is inconsistent with a client's investment or risk profile; and
- (e) a snapshot of specific trading or order book activity that illustrates the context of the order or transaction that is the subject of the notification.

RG 266.166 As stated in RG 266.158, where information that would otherwise be required to be contained in the notification to ASIC under Rule 3.6.1 has already been reported to AUSTRAC under the AML reporting legislation, a market participant may, but has no obligation to, notify ASIC of the same information: Rule 3.6.1(2).

## Confidentiality

- RG 266.167 Under Rule 3.6.2, a market participant must not disclose that it has notified ASIC of a reportable matter under Rule 3.6.1, nor disclose the information contained in the notification. This rule does not preclude a market participant from communicating that it has obligations under Rule 3.6.1 generally, or from communicating to a client or trader that it has concerns about the conduct of that person, which may constitute an offence under the law or which may expose the market participant to risk.

## Qualified privilege

- RG 266.168 A market participant notifying ASIC under Rule 3.6.1 has qualified privilege under s1100A for the notification. Section 89 states that, where a person has qualified privilege, that person is not, in the absence of malice, liable to an action for defamation. Qualified privilege under the Corporations Act does not affect any right, privilege or immunity that a person may otherwise have: s89(3).

Note: Section 1100A(1)(a) refers to information that a person is required to give under Ch 7 of the Corporations Act. Section 761H provides that, in Ch 7, a reference to a provision of Ch 7 includes (unless a contrary intention appears) a reference to other instruments made for the purposes of Ch 7.

- RG 266.169 A market participant that has qualified privilege under s1100A for the notification is also not liable for any action based on breach of confidence in relation to the notification: s1100A(3).
- RG 266.170 This protection extends to the officers, employees and representatives of a market participant: s1100D.

## L Crossing systems

### Key points

A participant of the ASX 24 market that operates a crossing system for financial products able to be traded on that market must:

- make certain notifications to ASIC and users of the crossing system, and make information about the operation of the crossing system publicly available on a website;
- provide fair treatment to all users of a crossing system;
- monitor activity on the crossing system, report significant breaches of its user obligations and operating procedures to ASIC, and report suspicious activity to ASIC; and
- have controls to ensure the efficiency and integrity of the crossing system.

### Scope and application

- RG 266.171 Chapter 5 of the Futures Markets Rules and this section of the guide apply to participants of the ASX 24 market that operate crossing systems (unless otherwise specified in the relevant rule).
- RG 266.172 A ‘crossing system’ is defined as any automated service provided by a market participant that matches or executes client orders with orders of:
- (a) the market participant;
  - (b) other clients of the market participant; or
  - (c) any other person whose orders access the automated service,
- otherwise than on an order book of a licensed market (Rule 1.4.3).
- RG 266.173 A full list of [crossing systems that are registered with ASIC](#) is available on our website.
- RG 266.174 The guidance in this section sets out our expectations in relation to crossing systems that are currently permitted to operate in the futures markets—for example, systems that automate mechanisms to facilitate pre-negotiated business orders under Part 3.3, block trades under Part 3.4 or exchange for physical transactions under Part 3.5. Some of the guidance in this section also anticipates the evolution of crossing systems in the futures markets.

## Notifying ASIC of intention to operate a crossing system

RG 266.175 A market participant that operates, or proposes to operate, a crossing system must lodge a crossing system initial report with ASIC no later than 20 business days before beginning to operate the crossing system. Table 7 sets out the details required to be included in a crossing system initial report.

**Table 7: Reporting requirements to be provided to ASIC about the nature of a crossing system**

Matters	Rule 5.1.1 reporting requirement	Guidance on details of information
Date of commencement	The date on which the crossing system began operating, or will begin to operate, in this jurisdiction	No further guidance
Clients	Access to the crossing system, including the criteria for determining persons who are eligible to use the crossing system and whether the crossing system transmits orders to other crossing systems, or receives orders from other crossing systems	For example, retail clients, wholesale clients and buy-side only
Matching process	How orders are prioritised and matched, and transactions are executed or matched off-market, on the crossing system	For example, if the crossing of orders is done on price–time priority, size priority or some other basis
Price determination	How the price for transactions on the crossing system is determined	For example, at the midpoint of the best available bid and offer on the order books of licensed markets
Fee structure	The fees, commissions, rebates or other charges paid by or to the market participant and users of the crossing system	This includes incentives paid by or to the market participant and/or users of the crossing system
Principal trades	Whether the market participant that operates the crossing system deals as principal (e.g. house account) with clients on the crossing system and, if so, the arrangements the market participant has in place for the management of conflicts of interest that may arise between the market participant and those clients	This includes all dealings as principal ('principal' has an extended meaning under Rule 1.4.3)
Reporting to a licensed market	The name(s) of the market(s) to which transactions executed or matched off-market on the crossing system are reported  Where more than one market is named, the circumstances in which each market is used for reporting transactions executed or matched off-market on the crossing system	For example, ASX 24



Matters	Rule 5.1.1 reporting requirement	Guidance on details of information
Life of an order	Whether orders on the crossing system are purged at the end of the day or remain on the crossing system until matching or execution on the crossing system next resumes. If the orders are not purged, the period of time they remain on the crossing system	No further guidance
RG 266.176	Under Rules 5.2.1(4) and 5.2.2(4), crossing system operators are also required to give ASIC a copy of the disclosures they make about their crossing systems to the public and to their clients: see RG 266.180–RG 266.200 for further information about publicly available crossing system information and non-public crossing system information. The information in these disclosures to the public and to clients is more detailed than the information required to be lodged with ASIC in a crossing system initial report.	
RG 266.177	A crossing system operator may fulfil its obligation to lodge a crossing system initial report under Rule 5.1.1 by giving ASIC copies of the more detailed disclosures under Rules 5.2.1 and 5.2.2 no later than 20 business days before the crossing system commences operation.	

## Monthly reporting to ASIC on trading activity and system changes

- RG 266.178 A crossing system operator that operates a crossing system must submit a monthly report to ASIC in certain circumstances: Rule 5.1.2. A monthly report must be submitted if there have been any changes during that calendar month to the information last provided to ASIC in the operator's crossing system monthly report or crossing system initial report: Rule 5.1.2(a).
- RG 266.179 Under Rule 5.1.2(b), the report must be prepared within 20 business days of the end of the calendar month and must be provided to ASIC as soon as practicable after it has been prepared.

## Public disclosure about crossing system operations

- RG 266.180 Under Rule 5.2.1, a crossing system operator must make available on a publicly accessible website the information listed in columns 1 and 2 of Table 8. More detailed guidance about what we expect a crossing system operator to disclose is provided in column 3.

**Table 8: Public disclosure requirements for crossing system operators**

Type of information	Publicly available crossing system information	Guidance
Operator	The code identifying the crossing system	The full legal name of the crossing system operator should be identified in addition to a code that uniquely identifies the crossing system. We may publish on our website the codes assigned to and applicable to specific crossing systems
Start date	The date the crossing system began to operate in this jurisdiction	Where a crossing system has been decommissioned or replaced by another crossing system, the market participant should disclose the date the system originally commenced operating, the date it ceased operating and the date the new crossing system commenced operating
Products	The types of financial products traded on the crossing system	For example, equity index future, other futures market contracts
Access criteria	The criteria used to determine eligibility to use the crossing system	Crossing system operators should consider including: <ul style="list-style-type: none"> <li>(a) the minimum requirements (e.g. technical capabilities) and the process for gaining access to the system; and</li> <li>(b) whether access arrangements for the crossing system are uniform across all users and, where they differ, provide details (e.g. whether some users are permitted to have direct access to the crossing system)</li> </ul>

### Making the information publicly available

RG 266.181 Rule 5.2.1(1) requires a crossing system operator to make the information available on a website that is publicly available and free to access.

RG 266.182 We expect the information to be made available on the crossing system operator's website using a constant, stable deep link where the web address does not change even when the information on the website changes.

### Updating the information

RG 266.183 When a crossing system operator implements a change to the operation of the crossing system described in Table 8, it must update the website within one business day: Rule 5.2.1(3). We do not expect short-term 'pilot' changes to be updated. However, when the final version is launched, the website should be updated within one business day.

RG 266.184 Crossing system operators should ensure that it is made clear on the website when the information was last updated and what information has been changed by an update.

## Notifying ASIC of the information and the website address

- RG 266.185 Rule 5.2.1(4) requires a crossing system operator to provide ASIC with a copy of the information that it has made publicly available and to provide ASIC with each update to the information within one business day of making the information available on its website. In fulfilling this requirement, we expect a crossing system operator to submit the relevant form on the [ASIC Regulatory Portal](#).
- RG 266.186 [Publicly available crossing system information](#) is also accessible via links on our website.

## Disclosure to crossing system clients

- RG 266.187 It is important that clients of a market participant that operates a crossing system understand the operating procedures of the crossing system. Rule 5.2.2 requires a crossing system operator to provide the following information to a client before accepting an order from them for the first time:
- (a) a copy of the publicly available crossing system information outlined in Table 8, or inform the client of the web address where the information is available (Rule 5.2.2(1)(a)); and
  - (b) the non-public crossing system information outlined in columns 1 and 2 of Table 9 (Rule 5.2.2(2)).

Note: A more detailed description of the non-public crossing system information we expect a crossing system operator to disclose to its clients is provided in column 3 of Table 9.

- RG 266.188 Each time a crossing system operator makes a change to the publicly available crossing system information or the non-public crossing system information, it must inform each of its clients of the change before it accepts an order from the client: Rules 5.2.2(1)(b) and (3).
- RG 266.189 We expect that the information provided by each crossing system operator should be standardised and consistent (i.e. not tailored for individual clients). However, it may differ for different groups of clients (e.g. wholesale and retail clients).
- RG 266.190 A crossing system operator only needs to provide the information outlined in Table 9 to a client in relation to its own crossing system. We do not expect it to provide this information in relation to other crossing systems that a client's order may access.

**Table 9: Non-public client disclosure requirements for crossing system operators**

Type of information	Non-public crossing system information	Guidance
User obligations	A description of the obligations imposed on users of the crossing system by the operator of the crossing system	<p>Crossing system operators should consider including:</p> <ul style="list-style-type: none"> <li>(a) how users are expected to access the crossing system and enter orders into the crossing system;</li> <li>(b) technical specifications users must comply with;</li> <li>(c) controls for maintaining the efficiency and integrity of the crossing system; and</li> </ul> <p>Note: A crossing system operator has obligations under Rule 5.5.2 in relation to the efficiency and integrity of its crossing system.</p> <ul style="list-style-type: none"> <li>(d) circumstances where access may be suspended or constrained (e.g. during a system failure) and any trading protocols or behavioural expectations when users access and use the crossing system</li> </ul>
Order types	A description of the order types available to those who have access to the crossing system, including a description of the characteristics of each order type	<p>Crossing system operators should consider including:</p> <ul style="list-style-type: none"> <li>(a) how the order types work, how price is determined for each order type and whether certain order types affect the order queue priority in the crossing system;</li> <li>(b) for each order type, whether it is available to all users who have access to the crossing system and, if not, the types of users that can use the order type and on what terms; and</li> <li>(c) whether the order type interacts with an exchange market or another crossing system (e.g. a shadowing arrangement)</li> </ul>
Operations	<p>A description of the operation of the crossing system—including, but not limited to:</p> <ul style="list-style-type: none"> <li>(a) how orders are managed, including how prices are determined and cancellations are managed;</li> <li>(b) details of any different treatment or arrangements for certain users or order types;</li> <li>(c) the circumstances in which principal orders may interact with other orders in the crossing system, and the nature of the principal orders (e.g. proprietary desk or market maker);</li> </ul>	<p>Crossing system operators should consider including:</p> <ul style="list-style-type: none"> <li>(a) the hours of operation of the crossing system;</li> <li>(b) how orders are prioritised and matched on the crossing system (e.g. price–time priority or some other basis);</li> <li>(c) how order and trade cancellations are managed;</li> <li>(d) how a system outage is managed, including the execution venues an order may be routed to in the event of a system outage or system stress (see RG 266.201–RG 266.205);</li> <li>(e) attributes of orders that may be controlled by users (e.g. minimum order quantity, opting out of certain types of order flow such as principal flow or liquidity providers);</li> <li>(f) details of any different treatment or arrangements for certain users or order types. Where one or a group of users have access to certain features of a crossing system and others do not, the details should be included;</li> </ul>

Type of information	Non-public crossing system information	Guidance
Operations (cont.)	<p>(d) whether orders of related bodies corporate of the operator enter the system and, if so, how conflicts (arising because orders of related bodies corporate enter the crossing system) are managed; and</p> <p>(e) how any other conflicts of interest that may arise are managed</p>	<p>(g) the circumstances in which principal (e.g. house account) orders (including orders of a related body corporate) may interact with other orders in the crossing system, and the nature of the principal orders (e.g. proprietary desk, market maker);</p> <p>(h) the arrangements for managing conflicts of interest that may arise in relation to the crossing system;</p> <p>(i) the licensed market(s) to which transactions are reported (i.e. ASX 24);</p> <p>(j) whether orders on the crossing system are purged at the end of the trading day or remain on the crossing system until matching or execution next resumes. If orders are not purged, the period of time they remain on the crossing system; and</p> <p>(k) how system failures are managed, including when users will be informed and how users' orders will be managed during system failures</p>
Fees	<p>The fees imposed for orders to gain access to the crossing system, or to be matched or executed in the crossing system, and an indication whether those fees differ from (e.g. by being in addition to) the market participant's standard fees</p>	<p>Crossing system operators should consider including:</p> <p>(a) disclosure of fees charged by a crossing system operator to allow another crossing system to gain access to the crossing system;</p> <p>(b) disclosure where there are different fees for different types of users (e.g. liquidity providers) and a description of how the different fee arrangements apply in relation to the type of use of the crossing system—we do not expect the actual fee to be disclosed; and</p> <p>(c) where there are no additional fees beyond standard commission, this should be disclosed</p> <p>Where fees are part of a commission sharing arrangement, and the commission does not depend on a particular execution venue, then the commission sharing arrangements do not need to be disclosed</p>

RG 266.191 When describing the operation of the crossing system we expect there to be sufficient detail to enable a client to identify the key features of the system's operations.

RG 266.192 We expect that, where retail clients use a crossing system, the disclosure to them about the matters in Table 9 is clear, concise and effective.

### Providing the information to clients

RG 266.193 A crossing system operator must provide a document containing non-public crossing system information to each client before accepting an order from the client for the first time: Rule 5.2.2(2)(a).

- RG 266.194 It is not necessary for clients to acknowledge or consent to this disclosure. We consider that the disclosure may be made in printed or electronic form, including via email with hyperlinks or references to a website. This is the same approach as for Financial Services Guides in [Regulatory Guide 221 Facilitating digital financial services disclosures](#) (RG 221).
- RG 266.195 Where a client asks for the non-public crossing system information in hard copy form (e.g. if they do not have access to electronic communications), we expect the crossing system operator to provide it to them in this form.

### Updating the information

- RG 266.196 A crossing system operator must update its non-public crossing system information within one business day of implementing changes to the operation of the crossing system where those changes affect the accuracy of information disclosed under Rule 5.2.2(3) and described in Table 8 and Table 9. A crossing system operator must provide the updated information to clients before accepting an order from the client after the update has been made. Clients only need to be notified about final system changes: see RG 266.183.
- RG 266.197 We expect that the notification will be made when there is a material change to the crossing system, particularly when it affects a client's use of the crossing system. For example, in relation to how orders are managed:
- (a) we expect clients to be notified when the change affects the order types available, how the price of an order is determined, or how the priority of orders is determined; and
  - (b) we would not expect clients to be notified when there are technical changes to the crossing system—for example, enhancement to the speed at which it operates—which do not affect the logic of how, for example, price or priority is determined.
- RG 266.198 A crossing system operator should consider providing advanced notice to its clients about planned changes to its crossing system where there are material changes to the way a user may access the crossing system or to the execution outcome (e.g. price) a user may expect to obtain from the crossing system.
- RG 266.199 Where the update is provided on a website, we expect that steps should be taken to ensure that clients are aware of the new information on the website. This may be done through an email with a hyperlink to the website, or through another form of written documentation (paper or electronic).

## Notifying ASIC of the information

- RG 266.200 Rule 5.2.2(4) requires a crossing system operator to provide ASIC with the non-public information that has been made available to its clients and each update to the information within one business day. In fulfilling this requirement, we expect a crossing system operator to submit the relevant form on the [ASIC Regulatory Portal](#).

## Notifications of crossing system outages

- RG 266.201 Rule 5.2.3 requires crossing system operators to notify ASIC and all users with orders in the crossing system at the time where a system outage may materially affect the efficiency or proper functioning of the crossing system. Examples of matters that may be considered material include:

- (a) when orders can no longer be entered, amended or cancelled in the crossing system; or
- (b) when the matching facility in the crossing system ceases to function efficiently.

- RG 266.202 We do not expect a crossing system operator to notify clients where, under the non-public disclosure requirements in Rule 5.2.2, it has disclosed to clients:

- (a) how it will route an order that may be in the crossing system at the time of the outage; and
- (b) when it has discretion to on-route an order that may be in the crossing system at the time of the outage.

Note: See Table 9.

- RG 266.203 To meet the requirements of Rule 5.2.3, a crossing system operator should consider putting in place policies and procedures that clearly outline the steps to be followed if the crossing system experiences an outage. The policies and procedures should outline the period of time before the procedures are enacted and the process of notifying ASIC and users with orders in the crossing system.

- RG 266.204 These notifications may be made by any means that the crossing system operator determines is most efficient, including through the use of a standardised email to all users. ASIC should be notified using the relevant form in the ASIC regulatory portal.

- RG 266.205 If a crossing system experiences an outage, and there are orders from another market participant that are affected by the outage, the notification should be made to the other market participant. This is because the crossing system operator may not know the contact details of the underlying clients, and the market participant responsible for these clients is in the best position to take action that is in its clients' best interests.

## Fair treatment of users

### Fair treatment of all users of a crossing system

- RG 266.206 Rule 5.3.1(1) requires a crossing system operator to ensure that:
- (a) the crossing system is operated by a common set of procedures that balances the interest of all users; and
  - (b) the procedures do not unfairly discriminate between crossing system users.
- RG 266.207 This is to ensure that users are treated in a fair and impartial manner and that retail clients are treated fairly compared to wholesale and principal users.
- RG 266.208 The requirement to treat users fairly does not prevent a crossing system operator from providing less favourable treatment for its own use of the crossing system or that of a related body corporate (Rule 5.3.1(2))—for example, providing client orders with time priority over principal orders.
- RG 266.209 In complying with Rule 5.3.1, we expect a crossing system operator to develop a common set of operating procedures that address the matters in Table 8 and Table 9.

### Fairness and priority in dealing

- RG 266.210 Rules 5.3.2 and 5.3.3 relate to fairness and priority when dealing with client orders in a crossing system.
- RG 266.211 Rule 5.3.3(1)(h) specifies that a crossing system operator's principal orders are not to be knowingly interposed between orders of its clients that would otherwise have crossed in its crossing system. We consider that a crossing system that systematically matches client orders with principal orders, without considering client orders that are available to match, would be inconsistent with these requirements.

### Opting out of a crossing system

- RG 266.212 Under Rule 5.3.4, a crossing system operator must permit a user of the crossing system to opt out of having their orders sent to the crossing system or another market participant's crossing system. The crossing system operator must not impose any additional operational or administrative requirements as a consequence of a client electing to opt out.
- RG 266.213 Additional operational or administrative requirements include requiring users who opt out to contact the crossing system operator on a trade by trade basis through a different mechanism to their usual broking arrangements.



## Monitoring and suspicious activity reporting

### Monitoring the use of a crossing system

- RG 266.214 Rule 5.4.1 requires a crossing system operator to monitor the use of its crossing system for compliance with:
- (a) the obligations that the crossing system operator has imposed on the user in relation to the crossing system as discussed under ‘User obligations’ in Table 9; and
  - (b) the operating procedures of the crossing system as described in Table 9.
- RG 266.215 The monitoring that we expect a crossing system operator to undertake will vary depending on the nature, size and complexity of the crossing system and the crossing system operator’s business. The types of factors that may warrant higher levels of monitoring include, for example, whether:
- (a) it is possible for one or more users to directly access and enter orders into the crossing system;
  - (b) there are liquidity providers active in the crossing system or otherwise large volumes of order messages; and
  - (c) there is principal trading in the crossing system.
- RG 266.216 Where the crossing system is large and complex and there are large volumes of orders, the crossing system operator should consider monitoring activity in real time or at least having in place adequate filters and controls that it monitors in real time. This will enable a crossing system operator to effectively meet its responsibilities to ensure the efficiency and integrity of its crossing system and meet the requirement to have appropriate controls in place: see RG 266.227–RG 266.231.
- RG 266.217 Post-trade monitoring may be adequate where a crossing system:
- (a) has a simple order and matching process;
  - (b) has relatively low order and trade volumes; and
  - (c) does not have clients directly accessing the system.
- RG 266.218 Any monitoring (whether manual or automated, real-time or post-trade) could include, for example, monitoring:
- (a) whether users have complied with their user obligations and the operating procedures;
  - (b) for spikes in order and trading volumes that may affect the efficiency and integrity of the crossing system;
  - (c) the use of order types that may be inconsistent with their intended purpose as outlined in the crossing system’s operating procedures and disclosures made to clients (see ‘Order types’ in Table 9);

- (d) activity that has interfered with, or is likely to interfere with, the efficiency and integrity of the crossing system (see RG 266.227–RG 266.231);
- (e) where there is principal trading in the crossing system, that principal orders are not receiving more favourable outcomes than client orders; and
- (f) where a crossing system promotes itself as providing a specific benefit (e.g. being a ‘safe harbour’ from high-frequency traders or an execution venue of ‘natural liquidity’), that activity in the crossing system is consistent with such disclosures.

RG 266.219 We expect that a crossing system operator’s monitoring activity will help the crossing system operator to determine whether the filters and controls it has put in place ensure the efficiency and integrity of its crossing system: see RG 266.227–RG 266.231.

#### **Managing breaches identified through monitoring activity**

RG 266.220 A crossing system operator must also take action to ensure that any breaches identified as part of its monitoring activities do not recur: Rule 5.4.1(1)(c). To comply with Rule 5.4.1(1)(c), we expect crossing system operators to have policies and procedures for managing suspected breaches. The policies and procedures may include:

- (a) documenting inquiries made on suspected breaches, and the results of these inquiries;
- (b) actions that may be taken for certain types of breaches; and
- (c) internal escalation policies and procedures and external and internal notifications to be made in relation to types of breaches.

#### **Notifying ASIC of breaches**

RG 266.221 Rule 5.4.1(2) requires a crossing system operator to notify ASIC, as soon as practicable, of all significant breaches it identifies during the course of its monitoring activities. In assessing what constitutes a ‘significant’ breach, a crossing system operator is not limited to considering a potential breach of the Corporations Act or market integrity rules. The crossing system operator should assess:

- (a) the types of users that access the crossing system and whether the activity or conduct of concern was targeted against particular types of users;
- (b) the nature of the activity or conduct of concern (e.g. whether it is repetitive);
- (c) the potential profitability of the activity or conduct of concern; and

- (d) any potential effects on the efficiency and integrity of the crossing system, and other execution venues. We do not expect a significant breach of the commercial terms between the crossing system operator and client to be reported to us.

RG 266.222 A crossing system operator must give ASIC written notification of the breach as soon as practicable: Rule 5.4.1(2). We would expect to be notified within three business days of determining that there is a notifiable matter. This is consistent with our expectations for suspicious activity reporting.

### **Record keeping**

RG 266.223 Rule 5.4.1(3)(a) requires a crossing system operator to maintain records that document its monitoring activities for a period of seven years. We expect these records to include:

- (a) details of the monitoring activities the crossing system operator has undertaken; and
- (b) results of the monitoring activities, including details of inquiries made and any communications that have been sent to clients, internal management and ASIC about the monitoring activities.

RG 266.224 A crossing system operator must also maintain records of breaches that it has identified for a period of seven years: Rule 5.4.1(3)(b).

### **Reporting suspicious activity in a crossing system**

RG 266.225 A market participant that operates a crossing system is required by Rule 5.4.2 to notify ASIC if it has reasonable grounds to suspect that a person has placed an order, or entered into a transaction, on a crossing system operated by the market participant:

- (a) while in possession of inside information; or
- (b) which has or is likely to have the effect of:
  - (i) creating an artificial price for trading in financial products on a financial market operated in this jurisdiction;
  - (ii) maintaining at a level that is artificial (whether or not it was previously artificial) a price for trading in financial products on a financial market operated in this jurisdiction;
  - (iii) creating or causing the creation of a false or misleading appearance of active trading in financial products on a financial market operated in this jurisdiction; or
  - (iv) creating or causing the creation of a false or misleading appearance with respect to the market for, or price for trading in, financial products on a financial market operated in this jurisdiction.

- RG 266.226 The guidance in Section K on suspicious activity reporting obligations relating to orders placed or transactions entered into on a market applies to operators of a crossing system for reportable matters on a crossing system.

## Systems and controls

### Efficiency and integrity controls

- RG 266.227 Rule 5.5.1 requires a crossing system operator to have:
- (a) appropriate automated filters designed to ensure the efficiency and integrity of its crossing system (Rule 5.5.1(1)); and
  - (b) controls that enable the immediate suspension or cancellation of orders in a series of related orders (Rule 5.5.1(2)).
- RG 266.228 In relation to the obligation in Rule 5.5.1(1), filters are pre-trade controls that establish points at which orders are tested and, by exception, where the system may determine an action other than passing them directly into the crossing system. In practical terms, an automated filter can usually do one of four things in relation to any given order (depending on the settings of the filter parameters):
- (a) pass the order into the crossing system;
  - (b) pass the order into the crossing system but identify it as an exception on exception reports generated by the system for subsequent analysis;
  - (c) pass the order to an appropriate person for review—this could include personnel on an electronic trading desk—and a decision as to whether the order may be submitted to the crossing system or routed to another execution venue; or
  - (d) reject the order outright.
- RG 266.229 We recognise that, given the differences in the types of business conducted by crossing system operators, there must be some degree of flexibility in determining what constitutes ‘appropriate’ filters for each crossing system operator. The types of filters will depend on the crossing system operator’s capabilities; the nature, scale and complexity of its business; and the particular risks that the crossing system operator has assessed as relevant to that business (including financial, reputational and regulatory risks).
- RG 266.230 The requirement in Rule 5.5.1(2) relates to controls that enable a crossing system operator to effectively implement automated controls to limit a series of related orders from interfering with the efficiency and integrity of the crossing system. For example, this may be required if a user has flooded a crossing system with orders which have substantially slowed the system down so that it no longer operates efficiently. Such controls enable a

crossing system operator to target its response to orders which may substantially disrupt the service it offers to other users.

RG 266.231 In addition to having appropriate automated filters and controls, we expect a crossing system operator to consider the resources it may need to cope with the effects of stressed market conditions on its crossing system, including the adequacy of any disaster recovery and capacity management with respect to its crossing system operations. In managing client orders in the event of stressed market conditions, this may include switching to a back-up site or bypassing the crossing system and routing to another execution venue (e.g. a licensed exchange market). Whatever the case, these arrangements should not result in a worse outcome for the crossing system operator's clients.

## M Technological and operational resilience

### Key points

Market participants must have adequate arrangements to ensure the resilience, reliability, integrity and security of their critical business services.

If a market participant engages a service provider to provide, operate or support one or more of its critical business services, they must have additional safeguards to ensure the operational resilience of those services.

Market participants must have adequate arrangements to ensure the confidentiality, integrity and availability of information obtained, held or used by the participant. They must also have adequate arrangements to ensure the availability of access to data obtained, held or used by the market participant, including arrangements designed to provide for the backup of data and the timely recovery of data in the event of any theft, corruption or loss of the data.

Market participants must have robust business continuity plans to effectively respond to events that could cause significant disruption to their operations or materially impact their services. These plans must be regularly reviewed, updated and tested.

It is essential for market participants to have appropriate governance arrangements and adequate financial, technological and human resources to comply with these obligations. This includes, but is not limited to, oversight by the board or senior management of the establishment, implementation, maintenance, review, testing and documentation of business continuity plans.

### Scope and application

- RG 266.232 Chapter 8B of the Futures Markets Rules and this section of the guide apply to all futures market participants. Similar rules also apply to participants of the securities markets. Guidance for securities market participants can be found in [RG 265](#).
- RG 266.233 While the rules apply to market participants, the obligations set out sound practices that have more general applications. Other AFS licensees should consider applying the principles in the rules to their business.
- RG 266.234 AFS licensees should also consider [RG 104](#), which provides further information about ensuring adequacy of resources to provide financial services: see RG 104.89–RG 104.100.

## Critical business services

RG 266.235 Part 8B.2 of the Futures Markets Rules requires market participants to implement an appropriate framework for ensuring the resilience, reliability, integrity and security of their critical business services.

### Definition of critical business services

RG 266.236 ‘Critical business services’ means functions, infrastructure, processes or systems (and the resources on which these functions, infrastructure, processes or systems depend) that, in the event of failure to operate effectively, would or would be likely to:

- (a) cause significant disruption to the market participant’s operations, activities and conduct in connection with each market of which they are a participant (participant operations); or
- (b) materially impact the market participant’s services provided in connection with each market of which they are a participant (participant services).

RG 266.237 Market participants must identify the critical business services relevant to their business: Rule 8B.2.1(2)(a). We expect market participants to determine which services are critical in the context of their own businesses and consider the nature, scale and complexity of their operations. The factors that may be considered in identifying critical business services include the criticality of a service to users or the market participant, the impact on users or the market participant in the event of prolonged disruption, and any dependencies that third-party businesses may have on a service. Market participants may determine the criticality of their business services based on their operational risk appetite, with defined indicators and limits.

RG 266.238 In defining critical business services, we have provided examples of what we consider likely to be critical business services for market participants: see the definition of critical business services and related note in Rule 8B.1.2.

Critical business services generally include functions, infrastructure, processes and systems that deliver or support:

- (a) order acceptance;
- (b) routing and entry;
- (c) clearing and settlement of transactions;
- (d) payments and deliveries of securities and funds;
- (e) accounting for and reconciling client money;
- (f) trust accounts;
- (g) securities and funds;
- (h) provision of trade confirmations; and
- (i) regulatory data reporting to market operators.

- RG 266.239 Relevant infrastructure that delivers or supports critical business services may include telephony, power and e-communication services.
- RG 266.240 The rules do not apply to CS participants (but do apply to market participants that are also CS participants). However, market participant functions, infrastructure, process and systems that provide information to, or that interface with, CS participants for the purposes of clearing and settling transactions would likely be critical business services.

Note: For further information on determining the criticality of services, market participants may wish to refer to IOSCO, *Market intermediary business continuity and recovery planning* (PDF 321 KB), final report, December 2015 and the International Standard [ISO 22301:2019](#) *Security and resilience—Business continuity management systems—Requirements*.

### **Adequate arrangements for critical business services**

- RG 266.241 Market participants must have adequate arrangements for their critical business services. Adequate arrangements should ensure the resilience, reliability, integrity and security of critical business services: Rule 8B.2.1(1). These arrangements would generally include, but are not limited to, policies, procedures and organisational resources (including financial, human and technological resources). The arrangements should be commensurate with the nature, scale and complexity of the services offered: see [RG 104](#) at RG 104.21–RG 104.22.
- RG 266.242 At a minimum, a market participant must have arrangements for:
- (a) identifying critical business services;
  - (b) identifying, assessing, managing and monitoring for any risks to the resilience, reliability, integrity and security of critical business services (see RG 266.243–RG 266.246);
  - (c) ensuring critical business services have sufficient and scalable capacity for the market participant’s ongoing and planned operations and services (RG 266.247–RG 266.253);
  - (d) preventing unauthorised access to or use of critical business services (see RG 266.300);
  - (e) managing the implementation of new critical business services and of changes to existing critical business services (RG 266.254–RG 266.269);
  - (f) dealing with a major event (RG 266.319–RG 266.343); and
  - (g) managing outsourcing arrangements for critical business services (RG 266.270–RG 266.296).



## Identifying, assessing, managing and monitoring risks to critical business services

- RG 266.243 Market participants must have critical business services arrangements for identifying, assessing, managing and monitoring for any risks to the resilience, reliability, integrity and security of their critical business services: Rule 8B.2.1(2)(b). To identify and assess risks, market participants should have adequate risk management systems: see RG 104.59–RG 104.66. Market participants should also have effective compliance measures to manage or mitigate those risks: see RG 104.23–RG 104.32 and Chapter C of RG 104. A market participant’s risk management systems and compliance measures will depend on the nature, scale and complexity of its business and its risk profile.
- RG 266.244 A director or senior manager of a market participant should have appropriate oversight of the risk management framework and compliance measures. This includes reporting to the governing body: see RG 104.50–RG 104.53.
- RG 266.245 A market participant regulated by APRA may instead develop and maintain a risk management framework as required by Prudential Standard [CPS 220 Risk management](#) to ensure compliance with Rule 8B.2.1(2)(b).
- RG 266.246 A market participant’s critical business services arrangements should also identify key interdependencies that may exist between critical business services. Market participants should also consider the risks associated with aged systems and assets.

## Sufficient and scalable capacity

- RG 266.247 Market participants should have arrangements for ensuring their critical business services have sufficient and scalable capacity for the participant’s ongoing and planned operations and services: Rule 8B.2.1(2)(c).

## Human capacity

- RG 266.248 Market participants should have sufficient human resources to conduct their business and provide their services properly. What is ‘sufficient’ will depend on the nature, size and complexity of the market participant. As a market participant’s businesses may change over time, a market participant should keep under review whether it still has sufficient human resources, including the right balance of skill sets.
- RG 266.249 We consider having sufficient human resources means:
- (a) having enough staff for the size of the business;
  - (b) having staff (including directors, secretaries and senior management) with the right skills, knowledge, competence, expertise and integrity to

ensure the market participant can operate their business properly and comply with its obligations;

- (c) when outsourcing any senior management or executive function, exercising due diligence and taking care to ensure that the outsourcing provides the market participant with the requisite skills, knowledge and competence;
- (d) being able to monitor and supervise the business appropriately; and
- (e) being able to meet current and anticipated future operational needs.

RG 266.250 To ensure market participants have sufficient and scalable capacity for their ongoing and planned operations and services, market participants should also undertake robust continuity planning, capacity planning and stress testing. Where market participants have outsourced their critical business services, we expect them to consider these principles as part of their management of the outsourced services: for more information about outsourcing of critical business services, see RG 266.270–RG 266.296.

#### **System capacity management and stress testing**

RG 266.251 Market participants should have sufficient system capacity to accommodate reasonably foreseeable volumes of trading activity.

RG 266.252 Systems should be adaptable to manage trading behaviours and scalable to allow for changes in response to elevated message levels and/or stressed market conditions that might breach their capacity. Stress testing of capacity, infrastructure, computers and applications should be conducted regularly and in line with a market participant's change management arrangements.

#### **Monitoring and review**

RG 266.253 To ensure that critical business services have sufficient and scalable capacity for the participant's ongoing and planned operations and services, market participants should periodically monitor and review their arrangements for systems testing, business continuity, capacity management and security. Market participants should remedy deficiencies and deal with identified problems in an appropriate and systematic way, as soon as reasonably possible.

#### **Review and change of critical business services arrangements**

RG 266.254 Review of a market participant's critical business services arrangements is fundamental to ensuring the continued resilience, reliability, integrity and security of a market participant's critical business services.

- RG 266.255 At a minimum, market participants must review their critical business services arrangements following each material change to their critical business services and at least once every 12 months: Rule 8B.2.1(3). However, it may be appropriate for larger and more complex businesses to review their arrangements more frequently.
- RG 266.256 A market participant's critical business services arrangements should be periodically reviewed to ensure they remain adequate and are within the risk appetite and risk tolerance levels of the market participant. Market participants must apply recommended changes to the critical business services arrangements arising from the review to ensure they continue to comply with the requirement to have adequate critical business services arrangements: Rule 8B.2.1(3). The monitoring and review of arrangements should be proportional to the nature, scale and complexity of the business: see [RG 104](#) at RG 104.21–RG.104.22.
- RG 266.257 We expect that the board or senior management of the market participant should have oversight of the review.

### **Documentation of arrangements**

- RG 266.258 Market participants must implement an appropriate framework for documenting their compliance with Rule 8B.2.1(4), including their critical business services arrangements, the scope and results of each review, and changes made to the arrangements. For guidance on how you can document your compliance measures, see [RG 104](#) at RG 104.23–RG 104.32.

### **Change management of critical business services**

- RG 266.259 Poor implementation of a new critical business service or a poorly managed material change to an existing critical business service may adversely affect clients, other market participants, market operators and the operators of licensed CS facilities. It can also affect the fair, orderly and transparent operation of the market.
- RG 266.260 Market participants must have adequate arrangements to ensure they continue to comply with Rule 8B.2.1(1) following the implementation of a new, or change to an existing, critical business service: Rule 8B.2.2. Adequate arrangements include, but are not limited to, testing of a new critical business service or material changes to an existing critical business service: Rule 8B.2.2(2)(a). The testing of new or material changes to existing critical business services should include testing of related changes to processes, technology, data and infrastructure, and consider the effect on stakeholders relying on the critical business service. Testing should occur before the live implementation of a new critical business service or material changes to an existing critical business service.

- RG 266.261 Adequate arrangements may also include implementation of a recovery point mechanism, where possible. Such a mechanism enables market participants to ‘roll back’ to a functional pre-change point, following the implementation of a new critical business service or material changes to an existing critical business service.
- RG 266.262 Market participants must have arrangements for communicating with persons who may be materially impacted by the implementation of a new critical business service, or a material change to an existing critical business service, to ensure they are adequately informed about the nature, timing and impact of the implementation a reasonable time before it occurs: Rule 8B.2.2(2)(b). What a reasonable time is will depend on the size, complexity and impact of the change, including the impact on clients and other third parties.
- RG 266.263 Market participants’ arrangements must also include arrangements for ensuring, to the extent reasonably practicable, that persons that may be materially impacted by the implementation or change are adequately prepared before it occurs: Rule 8B.2.2(2)(c). We expect that market participants will factor in the impact of the change on clients and other third parties, and allow sufficient time for any system or process changes that these persons need to make.

### **Material change**

- RG 266.264 When determining what constitutes a ‘material change’, market participants should consider the change in the context of the nature, scale and complexity of their business.
- RG 266.265 Material changes to critical business services could include, but are not limited to:
- (a) implementing a new critical business service or ceasing an existing critical business service;
  - (b) outsourcing a new or existing critical business service;
  - (c) bringing in-house a previously outsourced critical business service;
  - (d) making changes to an existing critical business service that may materially affect the users of the market participant’s services;
  - (e) implementing hardware upgrades and software updates that, in the event of an unsuccessful go-live:
    - (i) would or would be likely to cause significant disruption to the market participant’s operations or materially impact the participant’s services; or
    - (ii) may materially impact persons such as other market participants, market operators and the operators of licenced CS facilities; and

- (f) making changes that, in the event of an unsuccessful go-live, may require the activation of the market participant's business continuity plan.

RG 266.266 Adequate change management arrangements mitigate the risk of market disruptions and adverse impacts caused by failures of critical business services.

### Testing

RG 266.267 Market participants should have appropriate testing arrangements to ensure that their critical business services are functional and reliable. The testing methodologies should be designed to ensure that:

- (a) the operation of the critical business service complies with relevant regulatory obligations;
- (b) the controls embedded in the critical business service work as intended; and
- (c) the critical business service can continue to work effectively in stressed market conditions.

RG 266.268 Material stress scenarios may include significantly increased trading message volumes, constrained access to a market operator or other important service provider and/or market conditions that might strain a market participant's functions, infrastructure, processes and systems. Stress testing of capacity, infrastructure, computers and applications should be conducted to ensure market participants have sufficient capacity to accommodate reasonably foreseeable volumes of trading activity. Market participants that facilitate algorithmic, low-latency and high-message volumes should have a testing environment to enable them to adequately stress test this activity.

RG 266.269 When introducing or modifying a critical business service, relevant testing should be performed before going live. Examples of relevant testing may include, but are not limited to, the following:

- (a) *Functional testing*—This testing ensures that a system works as intended by verifying its features against its functional requirements.
- (b) *Connectivity testing*—This testing validates the continuity of network communications by verifying that the network is properly connected, with message traffic taking the desired route. For example, if a market participant plans to introduce a new order routing system, it could use a 'simulated trading environment' to make sure that the system is properly connected to relevant market operators and data providers.
- (c) *Conformance testing*—This testing is designed to determine whether a system meets predefined standards, and that quality assurance standards are being met. For example, standards can be the FIX protocols and specifications. Conformance testing should include interoperability

testing and confirmation of associated internal procedures. It should also include testing for compliance with the market participant's obligations under the Corporations Act and ASIC market integrity rules.

- (d) *Regression testing*—This testing detects potential problems in existing functional and non-functional areas of a system after changes and/or enhancements have been made. For example, when undertaking system enhancements, the market participant should review relevant legacy code and infrastructure to evaluate the compatibility of the system changes with existing software and hardware.

### Outsourcing of critical business services

- RG 266.270 Outsourcing occurs where a market participant uses a third party to perform tasks that it would ordinarily undertake itself. Outsourcing may also include tasks that the market participant does not have the capacity or resources to perform.
- RG 266.271 We recognise that market participants may enter into an arrangement with a third party (service provider) under which the service provider will provide, operate or support their critical business services (outsourcing arrangement).
- RG 266.272 The service provider may be a related party within the corporate group or an unrelated third party. Outsourced critical business services may be provided domestically, from an offshore location or a combination of both.
- RG 266.273 Critical business services that are commonly subject to an outsourcing arrangement include, but are not limited to:
- (a) order acceptance, routing and entry using trading platforms supplied by third-party vendors;
  - (b) clearing and settlement of transactions;
  - (c) accounting for or reconciling client money and trust accounts conducted by a third-party custodian; and
  - (d) regulatory data reporting.
- RG 266.274 Market participants that outsource tasks (including their critical business services) related to their AFS licence will remain responsible for complying with their licence obligations under s769B of the Corporations Act. [RG 104](#) provides further information for licensees on their obligations when outsourcing tasks: see RG 104.33–RG 104.36.

### Due diligence inquiries

- RG 266.275 Before entering into an outsourcing arrangement, market participants must conduct due diligence inquiries to ensure the service provider has the ability and capacity to provide the services effectively: Rule 8B.2.3(1)(a). When renewing or materially modifying an existing outsourcing arrangement,

market participants should make inquiries to ensure the service provider continues to have the ability and capacity to provide the services effectively.

- RG 266.276 Market participants should exercise due care, skill and diligence in the selection of service providers. This should include consideration of the service provider's technical, financial and human resources and capability. The participant should also consider the service provider's capability on information security, business resilience, continuity and disaster recovery, as well as any dependencies, conflicts and risks. Participants should be satisfied that the service provider has the ability and capacity to provide the services effectively, reliably, continuously and to a high standard.
- RG 266.277 The due diligence inquiries to be made under Rule 8B.2.3(1)(a) may be different depending on whether the outsourced arrangement is with a wholly-owned group entity or another third party. There may also be differences in the due diligence inquiries required depending on whether the wholly-owned group entity is based in Australia or on a cross-border basis. For example, in identifying the potential business, operational and other risks in an outsourcing arrangement with a wholly-owned group entity based in Australia, there may be more focus on the internal processes and procedures of the participant and the service provider.
- RG 266.278 Where the outsourced arrangement is with a wholly-owned group entity outside Australia, there may be more focus on the added risk that the overseas-based wholly-owned group entity may not be able to exercise the same level of oversight as if they were based in Australia—for example, due to time zone differences, language barriers and the fact that the overseas-based wholly-owned group entity may not be as familiar with Australian legislative requirements.
- RG 266.279 In outsourcing arrangements with other service providers (including with a related body corporate that is not a wholly-owned group entity) there may be more focus on the contractual arrangements between the participant and the service provider and validating, through appropriate reference checks, the competence and reliability of the service provider.
- RG 266.280 When outsourcing is undertaken on a cross-border basis (including with a wholly-owned group entity), market participants should consider any additional due diligence to address additional risks—for example, to maintain confidentiality of client information and whether any laws in the service provider's jurisdiction would obstruct or frustrate the ability of the market participant or ASIC to obtain prompt access to books and records.

### **Legally binding agreement**

- RG 266.281 Market participants must ensure that the outsourcing arrangement is contained in a legally binding agreement between the market participant and the service provider: Rule 8B.2.3(1)(b). The agreement must provide, among other things,

for the orderly transfer of services to the market participant or another service provider in the event of termination of the arrangement: Rule 8B.2.3(1)(b)(iv). The agreement should clearly define the ownership of intellectual property and provide specifications relating to the transfer of information to the market participant or the new service provider, as instructed by the market participant following the termination of the outsourcing arrangement. The agreement should also include an obligation for the service provider to assist and provide full support for the successful and complete transition following the termination of the outsourcing arrangement.

- RG 266.282 Additional safeguards can be implemented in the contractual arrangements between market participants and service providers. For example, market participants may also like to consider including provisions that:
- (a) terminate the contract if the service provider subcontracts services material to the outsourcing arrangement;
  - (b) allow the market participant to grant approval before the service provider subcontracts services material to the outsourcing arrangement;
  - (c) require the service provider to provide periodic assurance about the adequacy of their security controls and resilience capability;
  - (d) require the service provider to give a copy of its business continuity program to the market participant; and
  - (e) permit the market participant to make periodic onsite visits to the service provider's premises to assess whether it is meeting its obligations.

### **Monitor the performance of the service provider**

- RG 266.283 Market participants must monitor the performance of the service provider to ensure it is providing, and continues to provide, the services effectively and has the ability and capacity to continue to provide those services effectively: Rule 8B.2.3(1)(c). They are expected to have written supervisory procedures that set out how they will monitor and oversee the outsourced tasks provided by service providers.
- RG 266.284 The written supervisory procedures may be part of an overall framework for managing outsourcing arrangements. However, the framework should document, for each service provider, the required service level and have clearly defined metrics to measure the service level provided, including on emergency procedures, disaster recovery and contingency plans. This will also support the market participant's assessment of, and reporting to management on, the quality of tasks performed by the service provider.
- RG 266.285 Market participants should have measures for the service provider to identify, record and remediate instances of failure to meet contractual obligations or unsatisfactory performance and to report such instances to the market participant in a timely manner.



- RG 266.286 Market participants should have sufficient human resources to monitor the outsourced service provider. Market participants may also consider the use of internal and/or external auditors to monitor, assess and report on performance and controls over confidential information or client data.

### **Conflicts of interest**

- RG 266.287 Market participants must also have in place adequate arrangements to identify and manage any conflicts of interest which have been identified or could arise between the market participant and the service provider. This includes any conflicts involving subcontractors and related entities of the market participant, service provider and any subcontractor: Rule 8B.2.3(1)(d). The legally binding agreement between the service provider and the market participant must require a service provider to notify a market participant before it subcontracts services to another provider: Rule 8B.2.3(1)(b)(ii). Therefore, market participants should be able to identify and manage any potential conflicts of interests relating to subcontractors as they would ordinarily identify and manage potential conflicts relating to the service provider.

### **Access to books, records and other information**

- RG 266.288 Market participants must ensure that they and their auditors are able to promptly, on request, access books, records and other information of the service provider relating to the critical business services: Rule 8B.2.3(1)(f). They must also ensure that ASIC has the same access that it would have if not for the outsourcing arrangement: Rule 8B.2.3(1)(g). This may be achieved through specific terms in the legally binding outsourcing agreement with the service provider. The terms could prevent the service provider from deleting the records or otherwise making them unavailable, including in the event of non-payment of fees and charges by the market participant.
- RG 266.289 Market participants should test that their books, records and other information are readily accessible as expected. For example, market participants may do so by requesting, from time to time, access to certain books, records and other information of the service provider.
- RG 266.290 We expect that market participants will deal appropriately with any actions by service providers that breach outsourcing arrangements or compromise the participant's ability to comply with the market integrity rules and the law.
- RG 266.291 Where the outsourced tasks do not relate to critical business services, we encourage market participants to consider the appropriateness of applying the principles in Rule 8B.2.3 as a matter of good practice.

Note: APRA-regulated entities should also refer to Prudential Standard [CPS 231 Outsourcing](#), which includes information on outsourcing arrangements involving material business activities and IOSCO, [Principles on outsourcing](#) (PDF 639 KB), final report, October 2021.

**Attestation requirement**

- RG 266.292 Market participants must ensure, for each outsourcing arrangement, that the board or a director or senior manager have confirmed that they complied with the market participant's obligations in Rule 8B.2.3(1) and have made a written attestation to that effect: Rule 8B.2.3(1)(h). This attestation requirement applies to any outsourcing arrangement entered into after 10 March 2023 (including when an existing outsourcing arrangement is renewed or materially changed after 10 March 2023).
- RG 266.293 A market participant may use an internal governing body able to make decisions, approve or oversee a market participant's outsourcing arrangements to confirm whether a market participant has complied with the participant's obligations under Rule 8B.2.3(1). Examples of such a body are a steering or oversight committee for outsourcing, a risk management committee or an audit committee (at board or management level). In these examples, the written attestation may be made by a member of one of the above committees, or by a director of the market participant's board or a senior manager with relevant expertise and oversight.
- RG 266.294 The written attestation should be made each time a market participant enters into a new outsourcing arrangement with a service provider. This includes when a market participant renews or materially modifies an existing outsourcing arrangement with a service provider. Where a market participant has an existing outsourcing arrangement with a service provider that has no end date (e.g. an outsourcing arrangement within a wholly-owned group entity), we expect that the market participant will periodically comply with the written attestation requirement in Rule 8B.2.3(1)(h). The frequency of attestation may be informed by the risks involved with the outsourcing arrangement.
- RG 266.295 Market participants should regularly review and report to the board, director, senior manager or relevant governing body whether the outsourcing arrangement continues to comply with the participant's obligations in Rule 8B.2.3(1).

**Outsourcing involving cloud computing services**

- RG 266.296 We consider that using a cloud service provider is a form of outsourcing that involves specific risks and issues. Market participants should consider these risks and issues and apply appropriate safeguards to manage them. These risks and issues include, but are not limited to:
- (a) the shared responsibility model, which may require the allocation of roles and accountabilities between the market participant and the cloud service provider;
  - (b) different types of cloud services, including exposure to environments that are available to a range of entities (e.g. the 'public cloud' versus the 'private cloud');

- (c) the information security arrangements that are applied to information stored in the cloud;
- (d) the jurisdictions in which the cloud service provider's data centres are located;
- (e) the jurisdictions from which the cloud service provider's services are supported (e.g. there may be a 'follow-the-sun' service model) by technical staff;
- (f) the legal jurisdiction that applies to the contractual arrangements with the cloud service provider;
- (g) market participants', auditors' and regulators' access to data stored in the cloud, including any privacy limitations on accessing and using information about individual persons;
- (h) circumstances where the service provider is unable to provide an orderly transfer of services following unexpected termination of the outsourcing arrangement; and
- (i) the lack of visibility of the controls implemented by the cloud service provider.

Note: For further information on the use of cloud service providers, participants may wish to refer to the APRA information paper [Outsourcing involving cloud computing services](#) (PDF 836 KB), 24 September 2018.

## Information security

- RG 266.297 Market participants may hold or receive a range of information, including information received from their clients and external parties. This may include sensitive, confidential and personal information. Market participants must protect their information assets from unauthorised access, theft, loss or corruption. This helps to address concerns relating to cyber-attacks and privacy requirements.
- RG 266.298 Rules 8B.3.1(1) and (2) require market participants to have adequate arrangements to ensure the confidentiality, integrity and availability of information obtained, held or used by the market participant in relation to its operations and services. This includes:
- (a) arrangements to identify and document information assets that are integral to the provision of the participant's operations and services;
  - (b) controls (including automated controls) designed to prevent unauthorised access to information assets;
  - (c) controls for identifying, assessing, managing and monitoring for unauthorised access to information assets; and
  - (d) arrangements designed to protect information assets from theft, loss or corruption.

- RG 266.299 Information assets include information and information technology, including software, hardware and data (both soft and hard copy).
- RG 266.300 Market participants must also have arrangements for preventing unauthorised access to or use of their critical business services: Rule 8B.2.1(2)(d). These arrangements may include appropriate security policy frameworks that safeguard critical business services against unauthorised use, modification, damage or loss.
- RG 266.301 A market participant must maintain, for a period of at least seven years after the relevant event, records of any:
- (a) unauthorised access to or use of its critical business services that impacts the effective operation or delivery of those services; or
  - (b) unauthorised access to or use of market-sensitive, confidential or personal information: Rule 8B.3.1(5).
- RG 266.302 We do not expect a market participant to retain all of its IT logs (such as user activity logs) for at least seven years. However, when a market participant becomes aware of unauthorised access to or use of the above services or information, it should retain whatever written records it makes about the relevant event and, where possible, retain the relevant IT logs associated with the unauthorised access.

### **Roles and responsibilities**

- RG 266.303 A market participant should maintain an information security policy framework commensurate with its exposures to vulnerabilities and threats. A market participant should classify its information assets, including those managed by related parties and third parties, by criticality and sensitivity.
- RG 266.304 A market participant's information security arrangements should set out the responsibilities of all parties who have an obligation to maintain information security.
- RG 266.305 A market participant should clearly define the information security roles and responsibilities of:
- (a) the board;
  - (b) senior management;
  - (c) governing bodies; and
  - (d) individuals with responsibility for decision making, approval, oversight, operations and other information security functions.
- RG 266.306 A market participant should maintain an information security capability commensurate with the size and extent of threats to its information assets, and that enables the continued sound operation of the entity. To determine

the size and extent of threats, a market participant should consider the degree to which an information security incident affecting an information asset has the potential to impact market participant services and operations.

- RG 266.307 Those responsible for information security should ensure that the market participant maintains the information security capability in this manner.
- RG 266.308 A market participant should actively maintain its information security capability in response to changes in vulnerabilities and threats, including those resulting from changes to information assets or its business environment.

### **Controls in relation to information assets**

- RG 266.309 A market participant should have information security controls to protect its information assets, including those managed by related parties and third parties. The controls should be designed to prevent unauthorised access to information assets and to protect information assets from theft, loss or corruption. These controls should be commensurate with:
- (a) vulnerabilities and threats to the information assets;
  - (b) the criticality and sensitivity of the information assets;
  - (c) the stage at which the information assets are within their life cycle; and
  - (d) the potential consequences of an information security incident.
- RG 266.310 Market participants should consider implementing access controls to their information assets. Controls include, but are not limited to:
- (a) authorisation for remote access being determined on a user-by-user basis and business requirements;
  - (b) validation and review of access rights on a regular basis;
  - (c) traceable audit trails and logs for access to critical systems;
  - (d) multi-factor authentication for remote access; and
  - (e) ringfenced security, isolated networks or ‘air gaps’ for those critical systems that should not be accessed remotely.
- RG 266.311 Market participants that have adopted or expanded remote working arrangements should ensure supervision and controls remain effective for staff who are working remotely. They should also enhance supervision and controls where necessary to mitigate additional risks.
- RG 266.312 A market participant should test the effectiveness of its information security controls through a systematic testing program.

## Availability of access to data

- RG 266.313 Market participants must have adequate arrangements to ensure the availability of access to data obtained, held or used by the participant in its operations and services: Rule 8B.3.1(3).
- RG 266.314 We expect a market participant to have adequate arrangements and controls to ensure availability of access to data in the event of either physical or electronic information security incidents. Adequate arrangements include, but are not limited to:
- (a) access controls through encryption, firewalls, password and/or electronic keys, and network segregation;
  - (b) monitoring access to data through authentication mechanisms and generation of audit trails to detect unauthorised access;
  - (c) intrusion prevention and detection systems that allow the market participant to detect, analyse and alter possible cyber-security threats; and
  - (d) appropriate training programs educating staff on cyber-security threats.
- RG 266.315 We expect market participants' arrangements to include testing of information security controls in a manner that is appropriate to the nature, scale and complexity of the business.
- RG 266.316 Market participants who are AFS licensees must comply with their obligation to have adequate risk management systems: see s912A(1)(h). These participants should refer to [RG 104](#) for guidance on how to comply with this obligation: see RG 104.59–RG 104.66.
- RG 266.317 AFS licensees must also comply with the obligation to have adequate resources, including financial, technological and human resources, to provide the financial services covered by their licence: see s912A(1)(d). This includes having adequate technological resources to enable the licensee to maintain client records, maintain data integrity, and to protect confidential and other information. Licensees should refer to [RG 104](#) for guidance on how to comply with this obligation: see RG 104.97–RG 104.100.

Note: APRA-regulated entities should also refer to Prudential Standard [CPS 234 Information security](#), which includes requirements and guidance on information security.

## Backup and recovery of data

- RG 266.318 Market participants must have adequate arrangements to provide for the backup and timely recovery of data obtained, held or used by the market participant in the event of any theft, loss or corruption of the data: Rule 8B.3.1(4). Adequate arrangements may include, but are not limited to:
- (a) data backups that mirror data stored in the primary data centre;
  - (b) geographically separate secondary data centres and/or offsite storage;

- (c) assessment of the geographical area risks of the secondary data centre;
- (d) penetration testing of the backup site to prevent backups from compromise; and
- (e) technical recovery tests to ensure data backups can be recovered.

Note: For insight into what constitutes timely recovery of data, market participants may wish to refer to Section 2(d) of IOSCO, [Market intermediary business continuity and recovery planning](#) (PDF 321 KB), [CPS 234](#) and additional resources such as the [Information security manual](#) published by the Australian Cyber Security Centre (ACSC).

## Business continuity plans

- RG 266.319 A market participant must establish, implement and maintain business continuity plans for effectively responding to a major event. A major event is an event that would or would be likely to cause significant disruption to the market participant's operations or materially impact their services: Rule 8B.4.1(1). The plans must enable the continuity of the market participant's usual operations and services, including of critical business services, during a major event. Where continuity is not possible, the plans must enable the timely and orderly restoration of those usual operations following the event.
- RG 266.320 The plan implemented by the market participant should include clearly defined roles and responsibilities to ensure that the appropriate resources and correct processes are deployed in response to a major event.

### Identifying possible major events

- RG 266.321 Under Rule 8B.4.1(4), business continuity plans must identify and address, among other things:
- (a) the types of major events that may impact a market participant's operations and services; and
  - (b) their potential impact on the market participant's critical business services, operations and services, including classifying the potential severity of the impacts and the escalation procedures that are appropriate to the classification.
- RG 266.322 It must also be clear what actions, arrangements and resources are required, and specific objectives for the time taken, to provide continuity of operations or to quickly restore services. For example, this may involve teams triaging events according to pre-defined metrics and escalating the event to the appropriate crisis management team.

RG 266.323 Major events might include a significant internal system failure, a pandemic, a natural disaster, an outage of a critical infrastructure provider (such as a market operator or operator of a CS facility), the failure or corruption of a critical third-party service (such as a market data provider), or a significant cyber-security threat.

RG 266.324 A pandemic can have global impact for significant periods of time. While a pandemic may not cause physical damage to property and assets like a natural disaster, it can threaten the health of key personnel and demand a special level of consideration.

Note: For further guidance on the operational resilience of trading venues and market intermediaries during the COVID-19 pandemic, market participants may wish to refer to IOSCO, [Operational resilience of trading venues and market intermediaries during the COVID-19 pandemic & lessons for future disruptions](#) (PDF 654 KB), final report, July 2022.

RG 266.325 We expect market participants to undertake a business impact analysis to identify the potential likelihood of a major event occurring and the impact a major event may have on the market participant.

RG 266.326 We also expect market participants to map assets and dependencies (including third parties and financial market infrastructures) to identify potential impacts when a dependency is unavailable, so as to develop appropriate workaround actions.

### **Appropriate to the nature, scale and complexity of their business**

RG 266.327 We expect market participants to implement business continuity plans that are appropriate to the nature, scale and complexity of their business. Market participants operating on a regional or global scale are expected to have business continuity plans that address major events at the appropriate level:

- (a) *Local response to a major event*—when the event has a local impact only (e.g. a localised event that affects only part of a building or a single building), such as a fire at the primary site;
- (b) *Wide area response to a major event*—when the event affects both the primary site and alternative site within a region, such as an earthquake or wide area flooding;
- (c) *Regional response to a major event*—when the event affects two or more countries within a region, such as a pandemic, nuclear accident or the onset of war.

RG 266.328 Market participants should establish alternative sites for critical business services that have the same basic capabilities of primary sites including for required infrastructure, hardware and software (e.g. data centres). Any alternative site should be a safe distance from any primary site to mitigate any reasonably foreseeable event likely to impact the availability of all sites simultaneously.



- RG 266.329 In some cases, employees working remotely may be a resilient and workable alternative option. However, if this is not a solution for all employees and functions, business continuity plans should provide for an alternative location. Market participants should also consider the risks associated with remote working arrangements and implement appropriate controls to address these risks.

### **Communication during a major event**

- RG 266.330 A disruption or outage to a market participant's critical business services can impact:
- (a) their clients;
  - (b) other market participants;
  - (c) counterparties; or
  - (d) those dependent on the market participant for their critical business services, who require access to these services to carry out their activities.
- RG 266.331 Market participants' business continuity plans must include procedures for communicating during a major event with persons that may be impacted to ensure they are adequately informed: Rule 8B.4.1(4)(h). The communication must include the nature of the event, the steps that are or will be taken (and their likely timing) to manage the event, and the likely timing of the resumption of usual operations. The form of communication should be consistent with how the recipients would reasonably expect the market participant to communicate with them during such events.
- RG 266.332 A market participant's communication procedures should address required communications with financial authorities in other jurisdictions in the event of major operational disruptions with cross-border implications.

### **Notification of a major event**

- RG 266.333 Market participants must notify ASIC immediately on becoming aware of a major event: Rule 8B.4.1(6). We also request that ASIC is notified when operations return to normal.
- RG 266.334 The market participant must also give ASIC a written report within seven days. The report must set out the circumstances and the steps taken by the market participant to respond to the major event: Rule 8B.4.1(7). The following elements should be set out in the report:
- (a) the circumstances of the major event—including, for example:
    - (i) how it was identified;
    - (ii) the cause;

- (iii) the impact of the event on the usual operation of the critical business services; and
  - (iv) the affected parties (e.g. clients, other market participants, market operators or operators of licensed CS facilities); and
- (b) the steps taken to manage the major event—including, for example:
- (i) the escalation procedures for responding to the event, and the board members and senior management involved;
  - (ii) any changes to management structure or supervisory policies and procedures during or after the event;
  - (iii) the actions, arrangements and resources to respond to the event (including any documentation arising from the formation or invocation of a crisis management team or plan);
  - (iv) the timeframe for the expected return to normal operations; and
  - (v) any actions to remediate affected parties.

RG 266.335 Following submission of the written report to ASIC, we encourage market participants to notify ASIC if there are any significant changes to the matters outlined in the written report.

### **Review, update and testing of plans**

RG 266.336 Market participants must review, test and update their business continuity plans from time to time. At a minimum, to ensure the plans remain effective, market participants must review, test and update them:

- (a) each time there is a material change to the operations, services or critical business services, or to the participant's structure and location;
- (b) as soon as practicable after a major event; and
- (c) once every 12 months (Rule 8B.4.1(8)).

RG 266.337 Testing scenarios should be designed to cover a variety of major events and recovery scenarios. This should go beyond partial scenarios where only specific components of business continuity plans are tested (like offsite tests that only involve switching off the main system to operate the backup system). Better practice is that tests should incorporate full-scale simulated 'real life, end-to-end' scenarios that test all aspects of the business continuity plan, including the initial response and invocation, recovery and continuity, and return to normal operation phases.

RG 266.338 Business continuity testing should include market participants considering all the resources and facilities required to conduct the testing and confirming their availability—for example, physical infrastructure, equipment and personnel. Market participants should also consider the efficacy of a business continuity plan before testing—a full-scale test of a plan with limited development may itself lead to a disruption.

- RG 266.339 Whenever practical and useful, market participants should participate in industry-wide or cross-border testing with other intermediaries and stakeholders. Participants should conduct mock drills (simulation exercises) to test the effectiveness of their business continuity plan. Senior management should review results of business continuity plan assessments and, where appropriate, make the necessary changes to the business continuity plan.
- RG 266.340 Business continuity plans are generally temporary in nature. Prolonged use of these plans may require more frequent updates and testing. Further, the occurrence of a major event may warrant revisiting these plans and making more permanent changes to governance and oversight frameworks.
- RG 266.341 When reviewing their business continuity plans, market participants should conduct small-scale exercises to improve and increase understanding and effectiveness within the business.
- RG 266.342 Market participants should document the training exercises and note any observed problems or weaknesses in staff execution of the business continuity plan. Market participants should incorporate lessons learned from their reviews and testing of their business continuity plans in the updates.

### Documentation of plans and testing

- RG 266.343 Market participants must maintain documentation of their business continuity plans and the scope and results of all reviews and testing required under the rules: Rule 8B.4.1(9). The documentation must be maintained for a period of seven years from the date created or last amended, whichever is later. From time to time, we may request this documentation. Examples of documentation that should be maintained include, but are not limited to:
- (a) playbooks detailing responses to major events;
  - (b) terms of reference for crisis management committees;
  - (c) business continuity communication plans; and
  - (d) results of business continuity testing and failover resilience testing.

Note 1: Market participants may wish to refer to IOSCO, [Market intermediary business continuity and recovery planning](#) (PDF 321 KB), final report, December 2015 and IOSCO, [Thematic review on business continuity plans with respect to trading venues and intermediaries](#) (PDF 556 KB), final report, May 2021.

Note 2: Market participants should also consider certifying their business continuity plans against [ISO 22301:2019](#). APRA-regulated entities should also refer to Prudential Standard [CPS 232 Business continuity management](#).

## Governance

- RG 266.344 Market participants must have appropriate governance arrangements and adequate financial, technological and human resources to comply with their obligation under Chapter 8B of the Futures Markets Rules: Rule 8B.5.1(1).
- RG 266.345 We expect that oversight and accountability for critical business services and business continuity will come from the highest levels within market participants. Market participants must have arrangements for their board or senior management to oversee the establishment, implementation, maintenance, review, testing and documentation of the business continuity plans: Rule 8B.5.1(2).
- RG 266.346 We expect the persons with responsibility for oversight to be able to exert significant influence over the management of the business operations. Examples of appropriate levels of seniority include, but are not limited to:
- (a) a director of the organisation;
  - (b) a member of the board of the organisation; and
  - (c) individuals who make, or participate in making, decisions that affect the whole or a substantial part of the organisation.
- Note: See the definition of 'director' and 'senior manager' in s9 of the Corporations Act.
- RG 266.347 Whether a person might be considered as having the appropriate level of seniority will depend on the size and nature of the business. This may include a senior manager with responsibility for oversight of the relevant critical business service and/or business continuity plans.
- RG 266.348 We expect that the board or senior management will provide effective oversight and regularly assess whether the market participant has adequate financial, technological and human resources to comply with its obligations under Chapter 8B of the Futures Markets Rules.

## Appendix 1: Procedures, determinations and practice notes

RG 266.349 Table 10 lists the old SFE procedures, determinations and practice notes relevant to the ASIC market integrity rules.

**Table 10: Pre-existing SFE procedures, determinations and practice notes that are relevant to the ASIC market integrity rules**

Number	Title
PDP 1.13	Order records and accounting records
PDP 2.2.23	Order records and accounting records
PDP 2.2.25	Client documentation
PDP 2.2.26	Clients' segregated account obligations
PDP 2.2.28	Mandatory recording of information by the exchange and its participants
PDP 3.1.4	Market manipulation and misleading acts or practices regarding price
PDP 3.1.5	Market manipulation and misleading acts or practices regarding price
PDP 3.1.6	Entering orders without an intent to trade
PDP 3.1.7	Orders to be transmitted as soon as received
PDP 3.1.8	Orders to be transmitted and executed in the sequence received
PDP 3.1.9	Aggregation of orders
PDP 3.1.10	Disclosure
PDP 3.1.11	Withholding orders
PDP 3.1.12	Withdrawing orders
PDP 3.1.13	Pre-arrangement
PDP 3.1.14	Trading to the exclusion of others
PDP 3.1.15	Wash trades
PDP 3.1.17	Personal account trading
PDP 3.1.18	Dual trading prohibition
PDP 3.1.19	Trades to be allocated in sequence of order of receipt
PDP 3.2	Strategy trades
PDP 3.3	Pre-negotiated business
PDP 3.4	Block trades
PDP 3.5	Exchange for physical transactions

## Appendix 2: Superseded guidance

RG 266.350 This guide consolidates relevant guidance previously found in:

- (a) Superseded Regulatory Guide 214 *Guidance on ASIC market integrity rules for ASX and ASX 24 markets*, issued July 2010, reissued August 2010, February 2014, May 2015 and November 2015;
- (b) Superseded Regulatory Guide 223 *Guidance on ASIC market integrity rules for competition in exchange markets*, issued 4 May 2015;

Note: See also [Regulatory Guide 172](#) *Financial markets: Domestic and overseas operators* for guidance previously found in superseded Regulatory Guide 223.

- (c) Superseded Regulatory Guide 226 *Guidance on ASIC market integrity rules for capital and related requirements: ASX, ASX 24, Chi-X and APX markets*; and
- (d) Superseded Regulatory Guide 250 *Guidance on ASIC market integrity rules for risk management and other requirements: ASX 24 market*.

## Key terms

Term	Meaning in this document
AFS licence	An Australian financial services licence under s913B of the Corporations Act that authorises a person who carries on a financial services business to provide financial services  Note: This is a definition contained in s761A of the Corporations Act.
ASIC Act	<i>Australian Securities and Investments Commission Act 2001</i>
ASX 24	The exchange market formerly known as the Sydney Futures Exchange (SFE), operated by Australian Securities Exchange Limited
ASX 24 Operating Rules	ASX Limited's new operating rules, which replace the pre-existing SFE Operating Rules
Australian domestic licensed financial market	A financial market licensed under s795B(1) of the Corporations Act
Australian market licence	Australian market licence under s795B of the Corporations Act that authorises a person to operate a financial market
Capital Rules	<i>ASIC Market Integrity Rules (Capital) 2021</i> —rules made by ASIC under s798G of the Corporations Act
client	Has the meaning given by Rule 1.4.3
client account	Has the meaning given by Rule 1.4.3
Corporations Act	<i>Corporations Act 2001</i> , including regulations made for the purposes of the Act
CP 157 (for example)	An ASIC consultation paper (in this example numbered 157)
CPS 234 (for example)	An APRA Prudential Standard (in this example numbered 234)
deed	An instrument under seal containing a written contractual arrangement between ASIC and the foreign market participant that is enforceable by a court
FEX	FEX Global Pty Ltd
FEX market	The market operated by FEX
foreign market participant	A market participant that is a foreign entity and does not hold an AFS licence

Term	Meaning in this document
Futures Markets Rules	<i>ASIC Market Integrity Rules (Futures Markets) 2017</i> — rules made by ASIC under s798G of the Corporations Act
house account	Has the meaning given by Rule 1.4.3
IOSCO	International Organization of Securities Commissions
market integrity rules	Rules made by ASIC under s798G of the Corporations Act
market participant	A participant of a market
MDP (Markets Disciplinary Panel)	ASIC's Markets Disciplinary Panel, through which ASIC exercises its power to issue infringement notices and to accept court enforceable undertakings in relation to breaches of the market integrity rules
order system	Has the meaning given by Rule 1.4.3
principal trader	A market participant that trades only on its own behalf
RG 214 (for example)	An ASIC regulatory guide (in this example numbered 214)
Rule 2.2.1 (for example)	A rule of the <i>ASIC Market Integrity Rules (Futures Markets) 2017</i> (in this example numbered 2.2.1) unless otherwise specified
s912D (for example)	A section of the Corporations Act (in this example numbered s912D)
SFE Operating Rules	The operating rules of the Sydney Futures Exchange, now replaced by the ASX 24 Operating Rules
terminal	Has the meaning given by Rule 1.4.3
trading platform	Has the meaning given by Rule 1.4.3



## Related information

### Headnotes

ASX 24 market, crossing systems, foreign market participants, Futures Markets Rules, market integrity rules, market participants, minimum presence requirements, principal traders, risk management, supervisory policies and procedures, terminals

### Regulatory guides

[RG 78](#) *Breach reporting by AFS licensees and credit licensees*

[RG 104](#) *AFS licensing: Meeting the general obligations*

[RG 105](#) *AFS licensing: Organisational competence*

[RG 172](#) *Financial markets: Domestic and overseas operators*

[RG 216](#) *Markets Disciplinary Panel*

[RG 221](#) *Facilitating digital financial services disclosures*

[RG 265](#) *Guidance on ASIC market integrity rules for participants of securities markets*

### Legislation

AML/CTF Act, s41

ASIC Act, s50

*ASIC Supervisory Cost Recovery Levy Act 2017*

*ASIC Supervisory Cost Recovery Levy (Collection) Act 2017*

Corporations Act, Pts 5B.2 and 7.2A; s659B(1), 795B, 912A, 912D and 912DAA

*Corporations Amendment (Financial Market Supervision) Act 2010*

*Corporations (Fees) Act 2001*

Corporations Regulations, reg 10.15.04

FTR Act, s16

## Market integrity rules

Capital Rules, Rule 9.4.2.

Futures Markets Rules, Chapters 3, 5 and 8B; Parts 2.1–2.4 and 3.3–3.5; Rules 1.2.1–1.2.2, 1.4.3, 1.6.1, 2.2.1, 2.2.8, 2.3.2–2.3.4, 2.4.1, 5.1.1–5.1.2, 5.2.1, 5.2.2, 5.2.3, 5.3.1–5.3.3, 5.4.1–5.4.2 and 5.5.1–5.5.2.

## Consultation papers

[CP 157](#) *Proposed ASIC market integrity rules: FEX market*

[CP 166](#) *Market integrity rules for non-AFS licensee foreign participants and consequential amendments*

[CP 195](#) *Proposed amendments to ASIC market integrity rules: ASX 24 and FEX markets*

[CP 277](#) *Proposals to consolidate the ASIC market integrity rules*

[CP 302](#) *Proposed changes to ASIC's capital requirements for market participants*

[CP 314](#) *Market integrity rules for technological and operational resilience*

[CP 342](#) *Proposed amendments to the ASIC market integrity rules and other ASIC-made rules*

[CP 347](#) *Proposed amendments to the prohibition on order incentives in the ASIC market integrity rules*

## Waivers

[ASIC Market Integrity Rules \(Futures Markets\) Class Waiver 2018/312](#)

[ASIC Market Integrity Rules \(Futures Markets\) Class Waiver 2018/313](#)

## Other publications

ACSC, [Information security manual](#)

APRA, [CPS 220](#) *Risk management*

APRA, [CPS 231](#) *Outsourcing*

APRA, [CPS 232](#) *Business continuity management*

APRA, [CPS 234](#) *Information security*

APRA, [Outsourcing involving cloud computing services](#) (PDF 836 KB)

IOSCO, [\*Market intermediary business continuity and recovery planning\*](#) (PDF 321 KB)

IOSCO, [\*Objectives and principles of securities regulation\*](#) (PDF 187 KB)

IOSCO, [\*Operational resilience of trading venues and market intermediaries during the COVID-19 pandemic & lessons for future disruptions\*](#) (PDF 654 KB)

IOSCO, [\*Principles on outsourcing\*](#) (PDF 639 KB)

IOSCO, [\*Thematic review on business continuity plans with respect to trading venues and intermediaries\*](#) (PDF 556 KB)

[ISO 22301:2019](#) *Security and resilience—Business continuity management systems—Requirements*