REGULATORY GUIDE 266

Guidance on ASIC market integrity rules for participants of futures markets

September 2026

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 draft guide was issued in September 2026 and is based on legislation, regulations and market integrity rules as at the date of issue.

Previous versions

- Superseded Regulatory Guide 266, issued May 2018 and reissued August 2022

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

A Overview

Key points

ASIC is responsible for supervising domestic licensed financial markets in Australia: see RG 266.1–RG 266.3.

As part of our supervisory responsibilities, we make market integrity rules and monitor compliance by market participants with those rules: see RG 266.4.

This regulatory guide covers how to comply with those market integrity rules for participants on futures markets: see RG 266.5–RG 266.8.

Supervision of trading on domestic licensed financial markets

RG 266.1 We are responsible for supervising the activities and the conduct of 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.

Scope of this regulatory guide

RG 266.5 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 the *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 266.6 The guide also explains how we expect participants to comply with requirements about:

(a) governance and risk management;

(b) trading and trading systems;

(c) initial certification, material change and annual reviews of trading systems;

(d) crossing systems;

(e) suspicious activity reporting;

(f) capital requirements; and

(g) technological and operational resilience of critical business services.

RG 266.7 This guide does not cover the operating rules of market operators or clearing and settlement (CS) facility operators.

Related guidance

RG 266.8 Table 1 identifies other regulatory guides that may be relevant to market participants. This is not an exhaustive list.

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 *ASIC Market Integrity Rules (Securities Markets) 2017*	RG 265
The disciplinary process for breaches of all 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	Regulatory Guide 216 *Markets Disciplinary Panel* (RG 216)

Topic	ASIC regulatory guide
Notifying ASIC of a range of conduct by Australian financial services (AFS) licensees known as ‘reportable situations’: see s912DAA	Regulatory Guide 78 *Breach reporting by AFS licensees and credit licensees* (RG 78)
Our approach to supervising compliance with the AFS licensing obligations	Regulatory Guide 104 *AFS licensing: Meeting the general obligations* (RG 104) and Regulatory Guide 105 *AFS licensing: Organisational competence* (RG 105)
Guidance on an AFS licensee’s statutory obligation to manage conflicts of interest (s912A(1)(aa))	Regulatory Guide 181 *AFS licensing: Managing conflicts of interest* (RG 181)

B Supervision of trading on domestic licensed financial markets

Key points

We are responsible for supervising trading on Australian domestic licensed financial markets: see RG 266.9–RG 266.17

We take a risk-based approach to surveillance of compliance with the market integrity rules and market participants' obligations under the Corporations Act: see RG 266.18–RG 266.19

Market participants can communicate with ASIC through the ASIC Regulatory Portal, our markets-related telephone hotline or various dedicated email addresses: see RG 266.20–RG 266.21

ASIC's supervisory responsibilities

RG 266.9 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 or 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, see RG 104 and RG 105.

Note 2: Guidance on market operators' obligations under the Futures 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 266.10 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 266.11 We perform risk assessments of participants and, where necessary, conduct targeted surveillance of suspected misconduct.

RG 266.12 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 266.13 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 266.14 In some instances, we have incorporated content from the SFE procedures, determinations and practice notes into the ASIC market integrity rules.

Market surveillance

RG 266.15 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 266.16 Our market surveillance team makes inquiries of market operators, participants, listed entities, clients and others, using compulsory powers where necessary.

Disciplinary process

RG 266.17 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 266.18 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 266.19 ASIC conducts site visits of market participants and licensees and, where appropriate, shares information on supervisory practices.

Communicating with ASIC

ASIC Regulatory Portal

RG 266.20 Market participants can submit a range of applications and notifications using the transactions available on the ASIC Regulatory Portal. If a transaction is available on the portal, participants should use the portal to make the application or notification. If you encounter issues while using the portal, contact market.intermediaries@asic.gov.au

RG 266.21 Market participants should use the transactions available on the ASIC Regulatory Portal to submit certain information to ASIC, as required under the market integrity rules. 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

All market participants	Reportable situations (s912DAA)
Futures markets participants	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))

Note: In this guide, references to 'Chapter 3', 'Part 3.5' and 'Rule 3.5.10' (for example) are to that chapter, part or rule in the Futures Markets Rules (unless otherwise specified).

Telephone hotline

RG 266.22 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 Australian Eastern Standard Time (or Australian Eastern Daylight Time, as applicable) 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 266.23 We have set up three email addresses for use by market participants for market- and participant-related matters: see Table 3.

Table 3: ASIC email addresses for use by market participants

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

When to contact ASIC

RG 266.24 We are responsible for supervising trading activities by market participants to ensure market integrity: see RG 266.1–RG 266.3. As such, you can contact ASIC about conduct and activities that occur on domestic licensed financial markets.

RG 266.25 Australian market licensees retain responsibility for the operation of their markets. You should direct queries about the operations and processes of markets to the relevant market operator.

RG 266.26 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 266.27 Breaches (or likely breaches) of market integrity rules may constitute reportable situations for AFS licensees under s912D. If a breach of the market integrity rules must be reported under s912DAA, market participants need to report it 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 266.28 We have set out guidance on how to notify ASIC of a reportable situation under s912DAA 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.

C ASIC market integrity rules

Key points

We make market integrity rules which apply to market operators, market participants, other prescribed entities and financial products traded on a licensed market: see RG 266.29–RG 266.32.

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: see RG 266.33–RG 266.41

ASIC market integrity rules

RG 266.29 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 266.30 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 266.31 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 266.32 We will review and consult on 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.

Waivers

Power to grant a waiver of a market integrity rule

RG 266.33 We are able to grant market participants waivers from the obligation to comply with a provision of the market integrity rules.

RG 266.34 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 we impose conditions on a waiver, the market participant must comply with all of the conditions 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.

RG 266.35 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 266.36 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 266.37 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. Where appropriate, we may grant a waiver to a class of persons.

The process of requesting a waiver

RG 266.38 If you apply for a waiver, you must make your request in writing. You 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 266.39 We may refuse a request if you fail to address all of the relevant issues. Similarly, failure to supply relevant information may cause a delay in finalising the request.

RG 266.40 Should a commercially time-sensitive situation arise, we can consider such requests on an urgent basis. However, you must clearly demonstrate that the urgency results from factors beyond your reasonable control and that you could not have reasonably foreseen those factors. Self-imposed deadlines will not be a sufficient basis for urgent consideration.

RG 266.41 You should submit your applications for a waiver through the ASIC Regulatory Portal. You will need to pay a fee for your application. We have provided details about payment options in the portal. For more information, see how to apply for relief on the ASIC website.

D Governance and risk management requirements

Key points

This section provides guidance on complying with the governance, risk management and operational requirements in the market integrity rules. The requirements relate to:

- supervisory policy and procedures (see RG 266.45–RG 266.49);
- good fame and character requirements (see RG 266.50–RG 266.54);
- use of artificial intelligence (AI) and machine learning (see RG 266.55–RG 266.58);
- organisation and technical resources (see RG 266.59–RG 266.62);
- trading representatives (see RG 266.63–RG 266.66); and
- trading systems (see RG 266.67–RG 266.80).

Scope and application

RG 266.42 Market participants should maintain governance arrangements, risk management systems and supervisory procedures that are appropriate to their business. These arrangements, systems and procedures must also support compliance with the market integrity rules, market operating rules and other applicable provisions of the Corporations Act.

RG 266.43 Participants should adopt a structured and systematic approach to identifying, assessing and managing risk. This approach should be supported by practical supervisory policies, appropriate resources, and effective controls including over trading activity and trading systems.

RG 266.44 When determining the resources, governance arrangements and risk management systems appropriate to their business, market participants should consider the nature, scale and complexity of their participant services and operations.

Note: For further guidance on the general obligations for market participants that are also AFS licensees, see RG 104 and RG 105.

Supervisory policies and procedures

RG 266.45 Market participants must have appropriate supervisory policies and procedures to comply with the Corporations Act, relevant market integrity rules and market operating rules: see Rule 2.2.8.

RG 266.46 Market participants should have compliance policies and procedures that give their representatives clear and practical guidance on how their obligations apply. This guidance should cover behaviours that are expected and those that are not permitted. Compliance procedures that merely restate the law are insufficient. Market participants should integrate policies and procedures into day-to-day practice and reinforce them through supervision, training and appropriate resourcing. We consider that these steps will create a culture that encourages compliance.

RG 266.47 Supervisory policies and procedures should set out the arrangements used to ensure that the compliance procedures are being followed, and to prevent and detect prohibited practices. For example, supervisory procedures may specify the actions and reviews that should be undertaken by supervisory staff and the frequency of the supervisory reviews.

RG 266.48 At a minimum, a market participant's written supervisory procedures should specify:

(a) the supervisory staff responsible for supervision of the market participant's business operations and processes, identified by name, or title and position;

(b) the supervisory activities each supervisor is responsible for carrying out;

(c) the frequency with which the market participant requires those supervisory activities to be carried out;

(d) any supervisory activities which the supervisory staff may delegate to other persons, taking into account any need for specific qualifications; and

(e) the documentation that the market participant requires a supervisor to retain to demonstrate that their supervisory activities were carried out and the results of those activities.

RG 266.49 The board of a market participant should regularly assess its supervisory arrangements.

Good fame and character requirement

RG 266.50 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 4.4.1.

RG 266.51 Under Rule 4.4.1(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 266.52 Under Rule 4.4.1(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 266.53 Aside from the express circumstance in Rule 4.4.1(2)(a), none of the limbs in Rule 4.4.1(2)(b) will serve to determine that a person is not of good fame and character. Rule 4.4.1 does not prescribe the checks a market participant must perform to satisfy this requirement.

RG 266.54 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.

Use of AI and machine learning

RG 266.55 A market participant might use AI or machine learning in its business operations—for example, in trading systems, trading algorithms, surveillance, compliance, risk management or client-facing and operational processes. This may introduce additional risks due to increased system complexity, reduced transparency of model behaviour, and the potential for unintended outcomes when using AI or machine learning. These risks may be heightened in conditions of market stress.

RG 266.56 A market participant’s systems and controls include any AI or machine learning functionality used to comply with the market integrity rules. The participant should ensure that those systems and controls do not adversely affect the efficiency, integrity or proper functioning of a market and are subject to appropriate controls and oversight.

RG 266.57 Market participants that use AI or machine learning in their business (including in functions relevant to their market activities and compliance obligations) should implement governance and risk management arrangements that are commensurate with the nature, scale and complexity of that use. This includes:

(a) effective oversight by appropriately qualified staff with clear accountability for AI and machine learning use;

(b) appropriate controls, guardrails and limits to manage model behaviour and mitigate unintended outcomes; and

(c) processes to assess, validate and monitor systems that use AI and machine learning, including as part of existing testing, review and surveillance arrangements.

RG 266.58 Market participants should consider risks relating to data integrity, security and operational resilience. They should also consider whether it is appropriate in the circumstances to disclose their use of AI or machine learning to clients, market operators, ASIC or other relevant stakeholders.

Note: For more guidance relating to trading algorithms, including testing and AI and machine learning governance, see RG 266.110–RG 266.119.

Organisational and technical resources

RG 266.59 Trading participants must have and maintain 'necessary organisational and technical resources' to ensure that:

(a) trading does not interfere with the efficiency and integrity of a market or the proper functioning of a trading platform; and

(b) the trading participant complies at all times with the market integrity rules and the relevant market operating rules of which it is a Trading Participant.

Note: See Rule 2.2A.2.

RG 266.60 What is 'necessary' will depend on the nature, scale and complexity of the trading participant's business and activities. To meet the definition, the resources must be sufficient to ensure ongoing compliance with these obligations: see Rule 2.2A.2(b).

RG 266.61 Trading participants should allocate resources that can be reasonably expected to achieve compliance with these obligations. This includes:

(a) adequately trained staff who understand and apply compliance obligations;

(b) systems and controls to identify, escalate and address potential breaches; and

(c) effective governance, supervision and escalation arrangements and sufficient time and priority given to compliance matters.

RG 266.62 Trading participants should also have in place organisational and technical resources to comply with the trading obligations such as set out in Table 4.

Table 4: Examples of resources needed to comply with trading obligations

Obligation	Resources needed
Trading record requirements	Trading participants should have in place organisational and technical resources to automatically generate and maintain all trading records that are required to be kept. This includes those records required: • specifically under Rules 2.2.4 and 2.2.4A to 2.2.4D; and • generally under the Corporations Act. These records should be kept regardless of whether the order enters the trading platform or is rejected by the trading participant's trading system filter.
Capital requirements	A trading participant should have in place organisational and technical resources to ensure that, when it trades on its own behalf or on behalf of clients, it complies at all times with the risk-based capital requirements set out in Schedule 1A of the Capital Rules: Rule 8.2.1 of the Capital Rules. This requirement does not apply to a trading participant that is a principal trader only, a clearing participant of an approved clearing facility or an authorised deposit-taking institution.
Client order priority requirements	A trading participant should have in place organisational and technical resources to ensure it: • acts in accordance with client instructions and the client's best interests (Rule 3.1.13); • transmits orders as soon as they are received and in the order that they are received (Rules 3.1.4 and 3.1.5); and • does not aggregate orders unless permitted (Rule 3.1.16).
Client money requirements	A trading participant should have in place organisational and technical resources to segregate client money: Rule 2.2.6.
Account reconciliation requirements	A trading participant should have in place organisational and technical resources to reconcile client funds on a daily and monthly basis: Part 2.3.

Trading representatives

RG 266.63 A trading participant may authorise a trading representative to submit trading messages to the trading platform of a market on behalf of the participant. In these circumstances the trading participant must ensure that its trading representative is suitably qualified and has demonstrated to the participant their knowledge of the dealing rules of the markets that the trading participant operates on: Rule 2.2A.1(2).

RG 266.64 In addition, trading representatives may perform other important functions for which they should be trained and qualified. These functions include managing direct electronic access (DEA) users, post trade monitoring and surveillance functions and real time management of order exceptions requiring manual review. This is one aspect of the broader framework in Part 2.2A and Part 2.2B requiring trading participants to maintain appropriate resources and controls over trading activity.

RG 266.65 Market participants should consider implementing limits on the trading representative's access to the trading platform and the financial products in which the representative is authorised to trade. We consider that this will help the participant meet their obligations as an AFS licensee (e.g. the obligation to have adequate risk management systems under s912A(1)(h) of the Corporations Act).

RG 266.66 Trading participants may wish to consider:

(a) providing their trading representative with a copy of, or access to, the current documentation published by the market operator in relation to its trading platform (e.g. ASX24 Trade manuals); and

(b) providing or arranging training for, and testing of, the trading representative on the:

  (i) operation of the market participant's order entry system;

  (ii) operation of the trading platform; and

  (iii) relevant market integrity rules and market operating rules.

Trading systems and algorithms

RG 266.67 Trading participants should have adequate risk management systems that:

(a) identify the risks associated with their services and operations; and

(b) include measures to keep those risks to an acceptable minimum.

RG 266.68 Trading participants should establish and maintain controls to manage or mitigate those risks in a proportionate way.

RG 266.69 If a trading participant relies on policies or procedures to manage or mitigate risk, those procedures should not merely restate the law. They should provide representatives with clear, practical guidance on how the participant will comply with its obligations.

RG 266.70 In assessing what arrangements are appropriate, trading participants should consider the nature, scale and complexity of their business and trading activity. They should include in their consideration:

(a) the types of clients they service and the nature of their trading activity, including the provision of DEA (see RG 266.75);

(b) where the trading system does permit DEA, whether the trading participant intends to allow authorised persons to delegate their DEA;

(c) the types of financial products available to clients;

(d) the nature of any principal trading conducted by the participant;

(e) the complexity of the technology infrastructure, including its trading system;

(f) the complexity of the trading algorithms used by the participants, either as principal or by clients using a trading algorithm provided by the participant;

(g) whether the trading participant uses a third-party trading system and whether it is provided to it by a related party of the authorised person conducting business through the trading participant's trading system;

(h) whether there will be a high message or trade ratio that flows through the trading system, including whether the participant expects that its clients will be using trading algorithms;

(i) whether the trading system relies on latency-dependent connections and interfaces such as co-located business; and

(j) whether the trading system interacts with a crossing system operated by the trading participant.

RG 266.71 To comply with Part 2.2B, a trading participant should have written arrangements governing the operation, oversight and control of its trading system.

RG 266.72 These arrangements should form part of the broader control framework for meeting Rule 2.2A.2, including the trading participant's obligation to maintain necessary organisational and technical resources. The framework should cover risks arising from trading systems and trading activities, including DEA, algorithmic trading and system security.

RG 266.73 For example, written arrangements may describe who can approve changes to trading system filters, how filter changes are tested and recorded, and when an authorised person's access to the trading system should be suspended or limited. They may also set out how the participant monitors DEA order flow, reviews algorithmic trading activity and escalates potential system security issues.

Note 1: For more guidance on trading system controls and trading algorithms, see Section E. For guidance on certification, testing and review, see Section F.

Note 2: Market participants must also consider their capital requirements under the Capital Rules. Regulatory Guide 166: *AFS licensing: Financial requirements* (RG 166) sets out financial requirements for AFS licensees.

Trading on multiple markets and multi-product trading system routing

RG 266.74 Trading participants must manage the risks associated with automated trading on multiple markets and in multiple product types. This risk management must accommodate the differing platform specifications and financial products and order types. It must also consider the impact that a disruption caused by automated trading on one market may have on another market. Participants must ensure that the trading participant does not interfere with the conduct of an orderly market and does not assist or facilitate manipulative trading.

Market access arrangements

RG 266.75 A DEA arrangement is one where an authorised client deals directly on a market through a trading participant's trading system and pre-trade controls. If a trading participant permits DEA for its clients, the trading participant will need to manage the associated financial risks. A sponsored direct market access (SDMA) arrangement allows the authorised client to submit trading messages directly into the trading platform independent of the trading participant's trading system. Such trading messages remain subject to the exchange-provided pre-trade controls, which are set by the trading participant: RG 266.98–RG 266.100.

RG 266.76 Trading participants are responsible for all trading messages submitted into a trading platform under their unique trading identifier, including those trading messages submitted by an authorised client either under a direct or sponsored market arrangement.

RG 266.77 To comply with Rules 2.2B.2 and 2.2A.2 when providing SDMA, a trading participant must be satisfied that the authorised client's trading system and organisational and technical resources are sufficient to meet the trading participant's risk management obligations. In our view, for a trading participant to comply with Rules 2.2B.2 and 2.2A.2 the authorised client would need to be a principal trader. Principal traders are trading participants that are permitted to trade on their own behalf and are subject to Rules 2.2B.2 and 2.2A.2 in relation to their own trading system and controls.

RG 266.78 To comply with their risk management obligations, a trading participant providing SDMA should:

(a) conduct robust due diligence when onboarding the client and monitoring their trading; and

(b) ensure that the client applies and maintains appropriate limit settings at their trading system level.

RG 266.79 For both DEA and SDMA, trading participants should adopt and enforce written procedures with authorised clients. These should address pre-trade and post-execution controls to minimise financial risk, including:

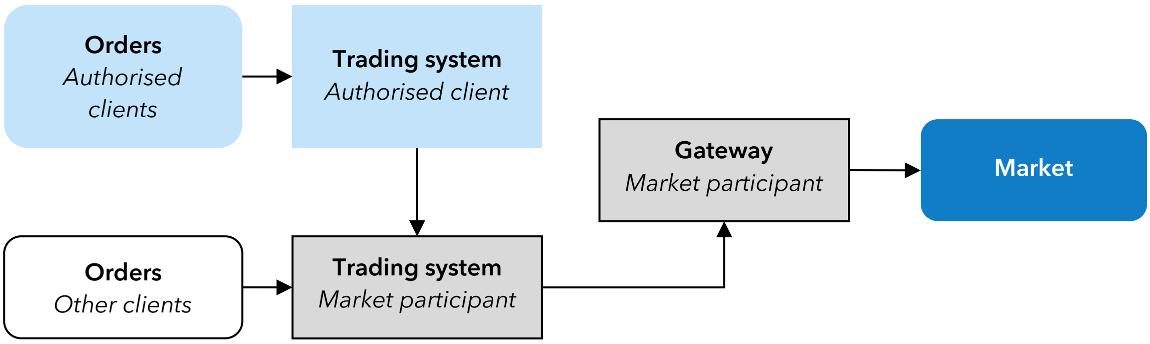
(a) considerations that should be taken into account before authorising the client to connect;

(b) the process for determining which controls to apply to a particular authorised client; and

(c) ongoing review of all controls imposed.

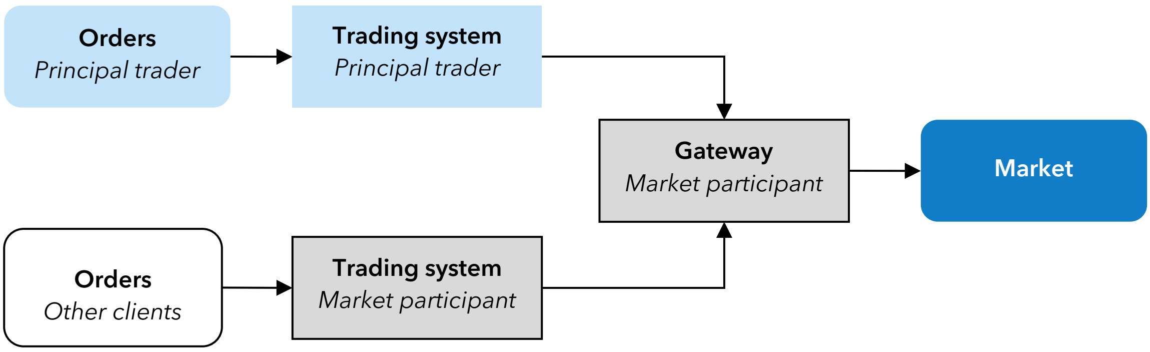
RG 266.80 In particular, the controls should ensure each authorised client has sufficient financial resources and will not create undue financial risk for the clearing participant or their trading. Trading participants should adopt and enforce written procedures that include ongoing review of the authorised person and controls imposed to ensure they have sufficient financial resources for their trading.

Figure 1: Direct electronic access: client or principal trader's orders are subject to market participant's order system



Note: See RG 266.75 for the processes set out in this flowchart (accessible version).

Figure 2: Sponsored direct market access: principal trader's orders bypass market participant's order system



Note: See RG 266.75 for the processes set out in this flowchart (accessible version).

E Arrangements for trading systems and algorithms

Key points

A trading participant has obligations to mitigate risks: see RG 266.81–RG 266.82. The participant must have appropriate:

- trading system design and documentation (see RG 266.83–RG 266.84);
- arrangements for a critical business service (see RG 266.85–RG 266.86);
- trading system controls (see RG 266.87–RG 266.106);
- security arrangements (see RG 266.107);
- trading algorithm development and documentation (see RG 266.111–RG 266.116);
- arrangements when making material changes to a trading algorithm (see RG 266.117–RG 266.119);
- monitoring and post-trade surveillance arrangements (see RG 266.120–RG 266.131);
- surveillance arrangements to identify false or misleading appearances (see RG 266.132–RG 266.138); and
- arrangements to immediately comply with any direction from ASIC to cease, suspend, limit or prohibit a trading system (see RG 266.140–RG 266.142).

Scope and application

RG 266.81 Automated trading systems and trading algorithms can improve the speed and efficiency with which a trading participant routes and executes orders. However, they also introduce specific risks that may affect the efficiency and integrity of a market or crossing system operated by a trading participant, or the proper functioning of a trading platform. These risks may be heightened by developments in AI, decision complexity and latency infrastructure. Part 2.2B imposes specific obligations on trading participants to help identify, manage and mitigate those risks.

RG 266.82 The obligations in Part 2.2B build on the general requirements in Part 2.2A, which require a trading participant to have the necessary organisational and technical resources and trading management arrangements. Together, these requirements ensure that trading messages submitted by the trading participant do not interfere with the efficiency and integrity of a market or the proper functioning of a trading platform.

Trading systems

Trading system design and documentation

RG 266.83 A trading participant's policies and procedures for compliance with Part 2.2B and system design documentation should be tailored to the trading participant's business and the type of activity envisaged for the trading system. These policies, procedures and system design documentation form the basis for initial certification, material change and annual reviews of the trading participant's trading system, which should be accurate, complete and up to date.

RG 266.84 A trading participant's trading system documentation should cover at least the following matters:

(a) system and subsystem architecture (hardware and software) including communication architecture, detailed design, processing logic, files and database designs, system security/integrity controls;

(b) the flow of trading messages including the origin of all orders and trading messages;

(c) targeted execution venues;

(d) controls, including filter arrangements;

(e) output descriptions and/or samples, including message types and formats, reports, logs, screen-based data fields, and other query results;

(f) input descriptions and/or samples and layouts including message types and formats, data entry screens, file structures, scanned or translated content, and other records; and

(g) external interfaces including data format requirements, specifications, and directional diagrammatic representation of connectivity between systems.

Critical business services

RG 266.85 We consider a trading system to be a critical business service for the purposes of Chapter 8B. Therefore, in addition to the trading system obligations in Part 2.2B, trading participants will need to consider their obligations under Chapter 8B. These obligations include ensuring:

(a) adequate arrangements to ensure the resilience reliability and integrity of the trading system (see RG 266.341);

(b) sufficient scalable capacity for ongoing and planned market operations and services (see RG 266.347); and

(c) effective business continuity plans for responding to a major event (see RG 266.410).

RG 266.86 If the requirements in Chapter 8B and Part 2.2B overlap, a trading participant may take that overlap into account to avoid duplication. For example, if a trading participant has appropriate security arrangements in place to comply with Chapter 8B it may take those arrangements into account when assessing its compliance for the purposes of the annual review in Rule 2.2B.9.

Trading system controls

RG 266.87 Trading participants must have in place appropriate controls to prevent the submission of trading messages that may interfere with the efficiency and integrity of a market or the proper functioning of any trading platform: Rule 2.2B.2(1)(a). Filters are critical pre-trade controls that should assess the market impact of a trading message before being submitted to a trading platform.

RG 266.88 When considering what is an 'appropriate' control, the trading participant will need to consider:

(a) the trading participant's system capabilities and the type of business of the trading participant conducted through the trading system;

(b) the particular risks that the trading participant has assessed as relevant to that business (including financial, reputational and regulatory risks);

(c) the nature and volume of the order flow expected through the trading system;

(d) the type of clients and the nature of the trading strategies used;

(e) the extent and nature of the trading algorithms;

(f) the type of product or contract being traded; and

(g) the interaction of the trading system with other systems and components.

RG 266.89 For example, a trading participant that has a high volume of orders should implement extensive automated controls. Where orders require manual involvement, such as exception reviews (e.g. for orderly market or large order categories) or a post-trade monitoring review function, the trading representative should be appropriately qualified and trained for the role and meet the criteria in Rule 2.2A.1(2).

RG 266.90 Trading system controls should also be appropriate for any crossing systems operated by the trading participant.

RG 266.91 A trading participant cannot rely on a market operator's controls to filter anomalous orders and manage extreme price movements. However, these market operator controls may complement the trading participant's controls.

Direct control of trading system controls

RG 266.92 A trading participant must at all times have direct control over its trading system controls: Rule 2.2B.2(2).

RG 266.93 Direct control includes the ability to activate or deactivate filters in the trading system, and to change filter parameters. A trading participant may allow limited user-level discretion to change a filter within a defined range.

RG 266.94 Filters may operate outside the participant's trading system. For example, a filter could sit between the market operator and trading participant, be provided by an independent third-party provider, or sit within another trading system used by the trading participant. In these circumstances, the trading participant should ensure that any activation or deactivation of the filter, or any change to filter parameters, is authorised only by a qualified person of the trading participant. An example of a qualified person is someone with relevant experience in broking operations, operational management or compliance.

RG 266.95 A trading participant will not have direct control if:

(a) there is no administrator-level control; or

(b) another person, including an authorised client, can set or amend those controls without the trading participant's approval, oversight or ability to intervene.

RG 266.96 In SDMA arrangements a principal trader client has operational access to set or amend their controls at the level of their own trading system. This does not, of itself, mean the trading participant lacks direct control for the purposes of Rule 2.2B.2(2). A trading participant will retain direct control if it has effective governance and oversight arrangements for those controls, including:

(a) appropriate due diligence before onboarding the client;

(b) documented parameters for the setting and amendment of controls;

(c) ongoing monitoring of the client's use of those controls;

(d) escalation arrangements; and

(e) the ability to require changes, suspend access or terminate the SDMA arrangement where necessary.

RG 266.97 In addition, the trading participant will have direct control over the exchange-provided controls that it sets for the client: see RG 266.75–RG 266.80.

Pre-trade controls for client and house accounts

RG 266.98 Trading participants may use exchange-provided pre-trade controls to support their compliance with the Futures Markets Rules. However, they must still ensure that their own trading controls meet the obligations under Rule 2.2B.2 of the Rules: see RG 266.87–RG 266.91.

RG 266.99 When setting their pre-trade controls trading participants must ensure that for each of their client and house accounts there are appropriate:

(a) predetermined order and position limits;

(b) price change limits; and

(c) order rejection capability of orders in excess of the limit set by the trading participant.

RG 266.100 These limits would be set at both the trading system and trading platform level (i.e. using both trading system and exchange-provided controls) and based on the trading participant's analysis of the financial resources or other relevant factors in relation to each of their house and client accounts: see Rule 2.2A.3.

Controls to immediately suspend, limit, prohibit or cancel

RG 266.101 A trading participant must have controls in its trading system to immediately suspend, limit or prohibit:

(a) trading by one or more authorised persons, clients, trading algorithms used by the trading participant, financial products, trading systems or markets (Rule 2.2B.2(1)(c)); and

(b) the entry of trading messages or orders, and cancel trading messages or orders that have already entered a market, where these form part of a series that has interfered, or is likely to interfere, with market efficiency or integrity (Rules 2.2B.2(1)(d)(i)–(iv)).

Note: 'Immediately' means promptly and without delay once a decision (either automatically or by an authorised representative of the trading participant) is made to use the controls to suspend, limit, prohibit or cancel the trading or entry of trading messages.

RG 266.102 A trading participant may identify a trading message, series of trading messages or orders from a particular source (e.g. a particular authorised person, account or algorithm) that is interfering, or is likely to interfere, with the efficiency or integrity of the market. If this occurs, the participant must use the controls required by Rule 2.2B.2(1)(c).

RG 266.103 These controls may include:

(a) termination of a trading system (referred to as a 'kill switch');

(b) forced logout of an authorised person; or

(c) a control implemented by amending the parameters of a particular filter to zero or a level that would prevent further trading.

RG 266.104 In addition, under Rule 2.2B.3, trading participants must have adequate monitoring systems. These systems should help the participant identify trading messages that are likely to interfere or have interfered with the efficiency or integrity of the market or the proper functioning of a trading platform. The monitoring systems should also enable participants to suspend (i.e. isolate for review), limit or prohibit further entry of the order or trading messages and cancel any that have already entered the market or crossing system. For further guidance, see RG 266.120–RG 266.131

Changes to trading system controls

RG 266.105 A trading participant must have processes to record changes to its controls, including automated filters and filter parameters: Rule 2.2B.2(1)(a). To comply with this requirement, a trading participant should consider having an ongoing audit and review function that captures and records any changes to the controls or filter parameters. This includes intra-day changes to the filter parameters and changes made by authorised persons.

RG 266.106 A trading participant should be able to:

(a) control, monitor and reconstruct (i.e. for information purposes) any changes to systems, filters or parameters within a trading system;

(b) identify which filters or controls are activated and which are not activated at any point in time;

(c) conduct ongoing audits and reviews of the controls of the principal trader client sponsored under a SDMA arrangement, including exchange-provided controls, to ensure they remain appropriate (see RG 266.75– RG 266.80); and

(d) limit changes to filters and filter parameters at the 'administrator' level, so they can be implemented only after they are authorised by a qualified person (e.g. a person with relevant experience in broking operations, operational management or compliance).

Security arrangements

RG 266.107 A trading participant must have security arrangements in place to monitor and prevent unauthorised access to a trading system: see Rule 2.2B.2(1)(b). These arrangements should include:

(a) authentication and authorisation of users, so that the operating system and application security limit internal access to authorised personnel;

(b) encryption of information;

(c) firewalling to prevent unauthorised external access;

(d) periodic testing of the trading participant's security management; and

(e) administration and ownership of system management.

Note: For details of additional requirements relating to information security controls, see Section L.

Trading algorithms

RG 266.108 The guidance in RG 266.108–RG 266.119 focuses on obligations that apply specifically to trading algorithms. These obligations supplement the broader requirements in Part 2.2B that apply to trading systems generally

RG 266.109 Trading algorithms include any computer algorithms that automatically determine one or more parameters of an order with limited or no human intervention. An algorithm that determines any order parameters is likely to be a trading algorithm under the rules. This includes but is not limited to algorithms that determine:

(a) whether to initiate an order;

(b) the timing of the order;

(c) the price or quantity of an order; or

(d) how to manage an order after its submission;

RG 266.110 An algorithm is not a trading algorithm if it is only used for:

(a) routing orders to one or more trading platforms (i.e. a smart order router);

(b) submitting orders that involve no determination of any order parameters;

(c) producing confirmations of orders; or

(d) post-trade processing of executed transactions.

Trading algorithm development and documentation

RG 266.111 Trading participants must have appropriate controls and governance arrangements for the development, testing, approval, deployment and monitoring of all trading algorithms used or made available by them: Rule 2.2B.4. What is ‘appropriate’ will depend on the nature and risk profile of the trading participant’s business and the type and complexity of the trading algorithm used.

RG 266.112 Trading participants should maintain comprehensive documentation for each trading algorithm. The documentation should be sufficiently clear to allow the trading participant’s risk function (i.e. compliance or internal audit) to understand how the algorithm operates and assess whether it is operating effectively.

RG 266.113 The trading participant must also take reasonable steps to test the trading algorithm before using it (or providing it to a client) for the first time or before making a material change to it: Rule 2.2B.4. This requirement does not apply to a trading algorithm that is deployed by a trading participant's client (i.e. not provided by the trading participant to the client). For further guidance on testing, see RG 266.185–RG 266.191.

RG 266.114 An authorised person, such as a client, might use their own trading algorithm. In these circumstances, a trading participant should consider testing the trading algorithmic flow against the trading participant's trading system filters. Testing should occur before first use (i.e. at the development stage) and to the extent possible before any material change is implemented. If the authorised person intends to use an AI or machine learning initiated trading algorithm, that should also inform the trading participant's assessment of the robustness of its own controls and monitoring systems.

RG 266.115 A trading participant might rely on a third-party service provider to provide, support or develop a trading algorithm. In these circumstances, the trading participant should have adequate due-diligence, governance and oversight arrangements of the third-party service provider to ensure compliance with Rule 2.2B.4: see RG 266.156.

RG 266.116 AI and machine learning may introduce additional risks in algorithmic trading. Unlike a traditional trading algorithm that follows pre-set instructions, AI-driven algorithms can be more opaque and adaptive, changing their strategies in real time in response to market conditions in ways that are less predictable. The complexity and risks of these different models should be factored into the trading participant's governance, testing and ongoing monitoring arrangements.

Material change to a trading algorithm

RG 266.117 If the trading participant makes a material change to a trading algorithm, it must take reasonable steps to test the algorithm before implementing the change: Rule 2.2B.4(2)(c). The purpose of the test is to ensure the algorithm will not interfere with the efficiency and integrity of a market or any crossing system, or the proper functioning of a trading platform.

RG 266.118 Whether a change to a trading algorithm is material, depends on the function, model, complexity usage and integration of the trading algorithm. A material change may include a change that when implemented:

(a) significantly affects the algorithm's outputs, risk profile or control environment; or

(b) has potential financial, operational, reputational or regulatory consequences for the trading participant

RG 266.119 Examples of material changes to an algorithm might include:

(a) modification of the core functionality of an algorithm (such as adding new order types);

(b) expansion of the algorithm's scope, (e.g. the addition of new products, legal entities, markets being traded); or

(c) modification of the algorithm's controls, (for example the modification of the design or behaviour of the control or a change impacting the transparency or monitoring of an algorithm).

Monitoring and surveillance

RG 266.120 A trading participant must have in place adequate monitoring systems and post-trade surveillance arrangements: Rule 2.2B.3(1) and (2).

RG 266.121 What is considered 'adequate' will depend on the scale, size and complexity of the trading participant's business and trading activity.

Note: A trading participant that operates a crossing system should refer to RG 266.313–RG 266.325.

Adequate monitoring systems

RG 266.122 Monitoring systems should be capable of immediately identifying a trading message or series of trading messages that are likely to interfere or have interfered with the efficiency or integrity of a market or the proper functioning of a trading platform. This applies to manual and automated monitoring systems, including alerts generated by pre-trade filters. In this context, monitoring systems should be able to identify relevant trading messages that require action or review promptly and without delay (i.e. in real-time or near real-time).

RG 266.123 If the trading participant identifies, from its monitoring, activity that has interfered with or is likely to interfere with the efficiency or integrity of the market, it should take steps to address the issue as quickly as possible. Where appropriate, this includes immediately suspending, limiting, or prohibiting trading for authorised persons, clients, trading algorithms used by the trading participant, or financial products, trading systems or markets: see RG 266.101–RG 266.103.

RG 266.124 A trading participant may consider monitoring the following:

(a) the nature and liquidity demands of the trading system to avoid unusual movements in market price or increased volatility;

(b) the level of use of the trading system to avoid generation of large numbers of the following types of orders, which may result in an adverse impact on a market:

(i) concurrent orders;

(ii) orders of small executable quantity, such as orders below an elected dollar or nominal value threshold; or

(iii) trading strategies that involve amending and/or cancelling a large number of orders that result in either a disproportionately low number of transfers or no transactions;

(c) whether the trading system appears to react to order book changes outside of the best market;

(d) the order-to-trade-ratio which quantifies the number of order submissions and amendments relative to actual trades. Excessively large order-to-trade ratios may indicate dysfunctional behaviour, market misconduct or poorly programmed strategies; and

(e) erroneous orders entering the market. An ‘erroneous order’ is an order that is submitted in error or that contains an error in one of its attributes (e.g. the price or volume of the order does not reflect the price or volume at which the trading participant or its client intend to trade).

RG 266.125 A filter might reject a trading message, or series of trading messages, and pass them to an authorised representative for review. In these circumstances, the trading representative should decide whether the trading message should be amended, cancelled or submitted to the market.

RG 266.126 A trading representative might submit a rejected trading message into the market but place the trading message on an exception report for ongoing monitoring. When this happens, a compliance officer or other qualified person should be available to consult. Trading participants should ensure exception reports are monitored on a regular basis (and at least daily).

RG 266.127 We recognise that it may be difficult to assess the market impact of some trading messages and orders (or a series of trading messages and orders) before they are submitted. For example, a trading message may not affect the last traded price of a product but may still affect the depth of the order book in that product and give rise to a false or misleading appearance of active trading in that product: see RG 266.129–RG 266.131.

RG 266.128 Trading participants should also consider the effectiveness of the information barriers required to manage the involvement of those staff operating in a compliance or information technology (IT) oversight role who have access to information on the nature of the trading system and to client order flow.

Adequate post trade surveillance

RG 266.129 A trading participant must have adequate post-trade surveillance arrangements. To be adequate, the arrangements must enable the participant to identify, as soon as possible, a trading message or series of trading messages that may have created, or may have been intended to create, a false or misleading appearance of active trading in any contract or with respect to the market for, or the price of, any contract: Rules 3.1.2 and 3.1.2A.

RG 266.130 These arrangements should complement the trading participant's monitoring systems. They should also include surveillance systems and appropriately qualified and capable representative(s) who regularly analyse historical orders, trading patterns and system alerts.

RG 266.131 In addition, as part of their post-trade surveillance, trading participants should be able to identify whether their controls, including filter parameters, are operating as intended or need adjustment.

False or misleading appearances

RG 266.132 As gatekeepers, market participants must not give effect to an order that may create a false or misleading appearance of active trading:

(a) in a contract; or

(b) with respect to the market for, or the price of, a contract (see Rules 3.1.2 and 3.1.2A).

Client of clients

RG 266.133 In relation to client orders, the scope of Rule 3.1.2(2) extends beyond a market participant's direct clients and includes orders made on behalf of any other person. We do not expect a market participant to understand everything about an underlying client of a direct client where that information is not reasonably available to the market participant. For example, we do not expect a market participant to know the details of an underlying client whose orders are submitted by a direct client operating an omnibus arrangement. However, if the participant becomes aware, or there are circumstances in those orders where the participant ought reasonably suspect, that the order may create a false or misleading appearance of active trading, the participant must not give effect to that order. Trading participants must actively monitor those orders: Rule 2.2B.3(1) and (2).

Circumstances of order

RG 266.134 The matters listed in Rule 3.1.2A apply to both the intention limb (Rule 3.1.2(2)(c)(i)) and the effect limb (Rule 3.1.2(2)(c)(ii)). Accordingly, a market participant's monitoring arrangements, and its pre-trade and post-trade controls to comply with Rule 3.1.2, should be the same for both the 'effect' and 'intention' limbs of the rule, although the relevance of those matters may differ depending on the circumstances and which limb applies.

RG 266.135 After taking into account the matters specified in Rule 3.1.2A, if a market participant ought reasonably suspect that either its direct client, or a client of its direct client, has placed an order with the intention of creating a false or misleading appearance of active trading, Rule 3.1.2(2)(c)(i) applies. The market participant must not offer to purchase, sell or deal in any contract for that person if doing so would give effect to the order. In assessing whether the market participant ought reasonably suspect that intention, it must consider any other relevant information available to it. This may include the order information, the client's history of trading, concerns raised by ASIC or information received from a third party.

RG 266.136 Separately, after taking into account the matters specified in Rule 3.1.2A, if a market participant ought reasonably suspect that an order or series of orders will have the *effect* of creating a false or misleading appearance of active trading, Rule 3.1.2(2)(c)(ii) applies. The market participant must not offer to purchase, sell or deal in any contract if doing so would give effect to the order. This may include situations where the circumstances of that order are such that the participant *ought reasonably suspect* it will have that effect, whether or not a person intended that effect. For example, where the order has been generated by an agentic AI system which has initiated, adapted or optimised trading activity outside of the person's initial specifications.

RG 266.137 Where a market participant ought reasonably suspect a false or misleading appearance of active trading, the participant should take appropriate steps to understand the purpose of the order and the circumstances of the underlying client, to the extent that information is available to it. Those steps may include escalating the matter internally, considering whether a suspicious activity report is required, and using available controls to prevent further manipulative trading.

RG 266.138 In addition to the matters specified in Rule 3.1.2A, Table 8 sets out some indicators that may alone or in combination, give rise to circumstances in which a market participant ought reasonably suspect that an order is intended to create or will have the effect of creating a false or misleading appearance of active trading in any contract, or with respect to the market for, or the price of, any contract. These indicators are not intended to be an exhaustive list and, although specific to Rule 3.6.1(1)(a) and (b), may still serve as a useful guide. A participant should also consider any other relevant matter relating to that bid or offer that may indicate suspicious trading: see Rule 3.1.2A(l).

RG 266.139 Market participants must also have adequate post-trade surveillance arrangements to identify a trading message or series of trading messages that may have created, or may have been intended to create, a false or misleading appearance of active trading: see Rule 2.2B.3.

ASIC direction to limit trading

RG 266.140 Under Rule 2.2B.10, we may give a direction to a trading participant that is not complying with the trading system requirements, or where we otherwise consider it appropriate, to:

(a) cease submitting trading messages to one or more markets until we are satisfied that the trading participant complies with the trading system requirements for the relevant market; or

(b) immediately suspend, limit or prohibit the submission of trading messages for one or more authorised persons or clients, financial products, markets or trading algorithms used by the trading participant.

Note: 'Immediately' means promptly and without delay.

RG 266.141 We will provide directions under Rule 2.2B.10 in writing. However, there may be circumstances where we need to provide a direction quickly. In these circumstances, we may advise the trading participant verbally (either by telephone or in person) that we intend to give a written direction and follow up with the written direction.

RG 266.142 A trading participant should consider taking immediate action to cease, suspend, limit or prohibit relevant submission of trading messages before receiving the written direction.

F Initial certification, material change and annual reviews

Key points

A trading participant must review and certify its trading system and related controls: see RG 266.143–RG 266.150. This includes:

- an initial review and certification to ASIC before the first use of a trading system for a market (see RG 266.151–RG 266.161);
- a review of any material changes to a trading system and or to related controls before the changes are implemented (see RG 266.162–RG 266.170);
- an annual review of its trading system (where it has not carried out a material change review in the previous 12 months) (see RG 266.171–RG 266.176);
- any further certification we direct a trading participant to provide (see RG 266.177–RG 266.178); and
- testing the controls, arrangements and resources of a trading system, before first use or before implementing a material change or annually, as necessary (see RG 266.182–RG 266.191).

A suitably qualified and experienced person must conduct the initial certification review, material change review and annual review. A responsible officer must provide the relevant written statement confirming that the trading participant complies with its obligations: see RG 266.179–RG 266.181.

Scope and application

RG 266.143 Under Part 2.2B, a trading participant must undertake:

(a) an initial review and certification of its trading system,

(b) a review before implementing a material change, and

(c) an annual review (unless a material change review has been performed during the previous 12 months).

RG 266.144 A trading participant must also test the controls, arrangements and resources of its trading system to assess whether they enable the trading participant to comply with Rule 2.2A.2 and Part 2.2B for the relevant market.

RG 266.145 A market operator may also impose additional or different qualification or certification requirements under its operating rules, operating procedures or as part of an access agreement before permitting a trading participant to connect to a trading platform. Satisfying a market operator's requirements does not mean the trading participant has satisfied the requirements of the Futures Markets Rules.

Design and scope of review

RG 266.146 The trading participant must design each review to appropriately assess whether the controls, arrangements and resources of the trading system enable the trading participant to comply with Rule 2.2A.2 and Part 2.2B. The nature and scope of the particular review will depend largely on:

(a) the type of review (initial, material change or annual);

(b) the nature, scale and complexity of the business of the trading participant conducted through the trading system;

(c) the nature and volume of the order flow expected through the trading system;

(d) how the trading system interacts with other interconnected systems or necessary controls and whether an assessment of the interconnected systems and controls that are not part of the trading system is required;

(e) the type of clients and the nature of the trading strategies used;

(f) the impact and nature of any changes reviewed;

(g) whether a third-party vendor provides the trading system;

(h) any other identified risk and financial management factors.

RG 266.147 All reviews should be supported by documentation demonstrating that the trading participant has:

(a) effective processes for approving all material changes to the trading system and its related controls; and

(b) adequate internal controls to prevent unauthorised changes.

RG 266.148 If a trading participant is operating multiple trading systems, it may conduct a combined review. The participant may only conduct a combined review if the review adequately covers each relevant trading system and market, and the resources required for each system.

RG 266.149 By testing and assessing their controls, arrangements and resources, trading participants are considering whether their overall operational effectiveness, security and resilience in relation to the trading system enable them to comply with Part 2.2B and Rule 2.2A.2. Trading participants should take a pragmatic approach to what is appropriate for their business.

RG 266.150 Table 5 provides an overview of the review requirements.

Table 5: Overview

Review requirement	Initial review	Material change review	Annual review
Assess the relevant controls, arrangements and resources Note: See RG 266.87–RG 266.107 for further details.	Rule 2.2B.5(2)(a)	Rule 2.2B.8(2)(a)	Rule 2.2B.9(2)
Test the relevant controls, arrangements and resources Note: See RG 266.182 for further details.	Rule 2.2B.5(2)(d)	Rule 2.2B.8(2)(d)	Rule 2.2B.9(2)(c) Note: These steps apply as necessary to assess whether the trading participant's controls, arrangements and resources enable compliance with Rule 5.5.2 and Part 5.6.
Review relevant documentation for the trading system Note: See RG 266.83–RG 266.84 for further details	Rule 2.2B.5(2)(b)	Rule 2.2B.8(2)(b)	Rule 2.2B.9(2)(a) Note: These steps apply as necessary to assess whether the trading participant's controls, arrangements and resources enable compliance with Rule 5.5.2 and Part 5.6.
Review relevant implementation documentation for the trading system	Rule 2.2B.5(2)(c)	Rule 2.2B.8(2)(c)	Rule 2.2B.9(2)(b) Note: These steps apply as necessary to assess whether the trading participant's controls, arrangements and resources enable compliance with Rule 5.5.2 and Part 5.6.
A suitably qualified and experienced person must conduct the review. Note: See RG 266.179–RG 266.181 for further details.	Rule 2.2B.5(3)	Rule 2.2B.8(3)	Rule 2.2B.9(3)
Responsible officer to provide written statement confirming compliance with the obligations Note: See RG 266.179–RG 266.181 for further details.	Rule 2.2B.6(2)(g)	Rule 2.2B.8(1)(b)	Rule 2.2B.9(4) – Note: To be provided no later than 20 days on completion of the annual review

Initial certification review

RG 266.151 Before using a trading system in relation to a market for the first time, a trading participant must:

(a) conduct an initial certification review by a suitably qualified and experienced person (see Rule 2.2B.5(3));

(b) submit the relevant form on the ASIC Regulatory Portal with representations from a responsible officer about the accuracy of the review; and

(c) receive written confirmation from ASIC that the certification complies with Rule 2.2B.6(2) (see Rule 2.2B.6(1)(b)).

RG 266.152 A trading participant that wishes to use a trading system in relation to another market for which it is not certified, must provide ASIC with an initial certification for use of that system on that market under Rule 2.2B.6.

RG 266.153 An initial review is not required for trading systems that were in use before the commencement of *ASIC Market Integrity Rules (Futures Market) Amendment Instrument 2026/575*.

RG 266.154 We will not accept a qualified certification. For example, we will not accept certification that is premised on caveats that may undermine the integrity of the certification.

RG 266.155 The fact that a trading system has been certified does not absolve the trading participant of any of its underlying obligations under the Futures Markets Rules.

Use of third-party service providers

RG 266.156 A trading participant must provide an initial certification for any third-party system it uses, unless orders coming through that system are subsequently processed by one of the trading participant's certified trading systems.

RG 266.157 The fact that one trading participant has certified a third-party provider's system does not imply that another trading participant using that system is not also required to certify that system. For a trading system developed by a third party, we will accept parts of the technical certification documentation supplied by that third party as supporting documentation for the initial certification. However, this is dependent on the trading participant:

(a) demonstrating that it has reviewed the trading system as required by Rule 2.2B.5; and

(b) being able to make the representations required by Rule 2.2B.6(2)(g)—including by providing evidence of completed user acceptance testing of system integration with internal systems.

RG 266.158 A trading participant might rely on a third party to provide, support or develop any aspect of a trading system or trading algorithm. If this is the case, the trading participant should maintain adequate governance and oversight arrangements sufficient to ensure that services provided support the participant's compliance with their obligations under Rule 2.2A.2 and Part 2.2B.

RG 266.159 At a minimum, participants should:

(a) conduct due diligence inquiries to ensure that the service provider is able to support the participant in meeting its obligations under Part 2.2B (see RG 266.370);

(b) ensure that, when a service provider is providing controls relating to a trading system, that the trading participant has direct control of those controls (Rule 2.2B.2(2)) (see RG 266.92–RG 266.97);

(c) ensure that suitably qualified and experienced staff review any evidence supplied by the service provider when conducting an initial, material or annual review of a trading system (see RG 266.179).

RG 266.160 When relying on a third-party service provider for a trading system, the trading participant remains responsible for complying with the trading system review obligations in Rules 2.2B.5 to Rule 2.2B.9. This includes ensuring that any review is properly scoped and supported by access to the information needed to assess the system.

RG 266.161 Where a trading system or trading algorithm is subject to an outsourcing arrangement within the meaning of Rule 8B.1.2, additional obligations will apply to that arrangement under Rule 8A.3.3: see RG 266.366–RG 266.389.

Material change review

RG 266.162 Before making a material change to a trading system or to the controls, arrangements and resources of that trading system, a trading participant must undergo a material change review. A suitably qualified and experienced person must conduct the review: Rule 2.2B.8.

RG 266.163 The material change review should be designed to assess and test the controls, arrangements and resources of the trading system that are related to or impacted by the material change. This must also include a review of the trading participant's policies, procedures, system design documentation and other relevant implementation documentation to the extent that they relate to, or are impacted by the material change. The trading participant should also assess any impacts on related systems and other interdependencies.

RG 266.164 If a trading participant is operating multiple trading systems, we consider that documentation, policies and procedures that apply across trading systems could be considered in totality when reviewing material changes across those systems.

RG 266.165 Trading participants should have adequate arrangements to ensure they have timely access to skilled and knowledgeable internal and vendor technical support for their specific trading system configurations, particularly while implementing changes to a trading system.

What is a material change under Rule 2.2B.8?

RG 266.166 The term 'material' is a broad concept and should be considered in the context of the nature, scale and complexity of the business being conducted by the trading participant through a trading system.

RG 266.167 We would consider the following changes to be material:

(a) a change to the trading system—or to the controls, arrangements or resources relating to that trading system—that may increase the potential for the trading participant to fail to comply with its obligations under the Futures Markets Rules;

(b) a series of such changes that, when considered together, may have the same material effect; or

(c) a change, or series of changes, to a trading system that may result in the trading system—or the related controls, arrangements or resources—no longer enabling compliance with Rule 2.2A.2 or Part 2.2B.

RG 266.168 A trading participant will need to take a practical approach when determining whether a particular change or series of changes to the trading system or its controls, arrangements and resources constitute a 'material' change. This is regardless of whether that change was made by the trading participant or the system provider.

RG 266.169 A trading participant should consider, at a minimum, the following factors when assessing whether a change is material:

(a) the ability of the trading participant to meet the requirements of Rule 2.2.A.2 and Part 2.2B, particularly Rule 2.2B.2, after the change is made;

(b) the potential for a change to result in trading activity that may interfere with the efficiency and integrity of the market provided by an operator;

(c) the potential for a change to result in a breach of Rule 3.1.2, taking into account Rule 3.1.2A (false or misleading appearance); and

(d) the potential for a change to result in trading activity that may interfere with the proper functioning of a relevant market.

RG 266.170 We have provided examples of what may or may not be considered a material change in Table 6.

Table 6: Examples of material changes under Rule 2.2B.8

Type of change	Examples
Material change	1 Upgrades in system complexity—for example, single market to multi-market system, or from an automated principal-only order processing system to a system that accommodates both principal and agency order flow (i.e. providing DEA services to a client). 2 Enhancements to client functionality affecting order types. 3 Changes to allow client access to additional order books or execution venues, which may affect the types of orders and messages passed into the market. 4 Provision of DEA or the addition of new client order flow which may affect filter and filter parameter capability. 5 Cumulative incremental changes to a system over a period of time that, when considered together, may constitute a material change when compared with the system at the time of its initial certification or previous annual review. 6 Changes to the type, size and growth of client order flow that may require significant changes to system capacity. 7 Changes that increase the risk of creating, or appearing to create a disorderly market or manipulative trading. 8 Changes that increase the risk of a high order-to-trade ratio relative to the financial product, underlying market liquidity or current market volatility. 9 Implementation of a new algorithmic trading strategy, or a substantive change to the decision logic, execution logic, order routing, throttling, pricing, or risk controls of an existing algorithm, where the change may alter the nature, speed, volume, or pattern of orders sent to the market. 10 Introduction of, or a substantive change to an AI or machine learning model used in trading, order generation, execution, routing, surveillance, or pre-trade risk management. This includes where the model is adaptive or the change may affect system behaviour, the performance of filters or controls, or the risk of disorderly or manipulative trading.
Not material (generally)	1 Staff changes not affecting compliance capability (e.g. the absence of a designated compliance person may not be material, but may require a review of supervisory staff or trading representatives). 2 User interface or screen display changes for access to relevant execution venue. 3 Physical relocation from one co-location facility to another of the same provider, without other substantive changes.
Treated as new system	1 Migration to a new third-party system provider, where the migration results in a new trading system (requires initial certification under Rule 2.2B.6, rather than a material change assessment).

Annual review

RG 266.171 Under Rule 2.2B.9, a trading participant must have an appropriately qualified person undertake an annual review of the trading system. An annual review is not required if the trading participant has performed a material change review (in accordance with Rule 2.2B.8) within the last 12 months.

RG 266.172 A material change review is generally limited to the particular controls, arrangements or resources affected by the material change. It may nonetheless be prudent for the trading participant to consider whether they should also conduct an annual review of the remaining aspects of the trading system, to ensure compliance with Rule 2.2A.2 and Part 2.2B.

RG 266.173 The annual review must include an assessment of whether the trading participant's controls, arrangements and resources in relation to the trading system enable the trading participant to comply with Rule 2.2A.2 and Part 2.2B. It must also include, as necessary:

(a) reviewing the trading participant's policies, procedures, system design documentation and other relevant documents in relation to the trading system and implementation of changes to the trading system; and

(b) testing of the trading participant's controls, arrangements and resources in relation to the trading system.

RG 266.174 The type, form and scale of testing undertaken as part of the annual review will depend on what is necessary for the trading participant to satisfy itself that it complies with Rule 2.2A.2 and Part 2.2B. In undertaking an annual review, a trading participant should consider whether the nature of existing order flows, or changes to those flows, are affecting system efficiency or performance relative to the original certification. The review should take into account any periodic testing of the trading system or related controls and any relevant incidents that occurred during the previous 12 months.

RG 266.175 To avoid duplication, a trading participant may take into account testing carried out during the previous 12-months when assessing what further testing would be necessary to ensure compliance with Rule 2.2A.2 and Part 2.2B as part of its annual review. This includes testing undertaken for the purposes of Chapter 8B of the Futures Market Rules.

RG 266.176 When relying on a third-party provider trading system, participants still need to satisfy themselves that their controls, arrangements and resources for the trading system enable compliance with Part 2.2B and Rule 2.2A.2: see RG 266.156.

Further certification

RG 266.177 We may direct a trading participant to provide further certification for a market, from an appropriately qualified person acceptable to ASIC: see Rule 2.2B.7. The trading participant must comply with ASIC's direction within the time specified in the direction.

RG 266.178 Examples of when we may require a further certification include where:

(a) we are not satisfied with the quality of a review undertaken for an initial, material change or an annual review;

(b) we consider that a trading system no longer operates in the manner for which it was initially certified; and

(c) we consider that a trading system no longer enables the trading participant to comply with the trading system requirements in Part 2.2B.

Suitably qualified and experienced person and responsible officer

RG 266.179 The initial, material and annual reviews must be conducted by a person who is suitably qualified and experienced to review the trading participant's trading system. The relevant responsible officer must make the written statement required for the review or certification: see Table 7. 'Officer' has the same meaning as under s9AD of the Corporations Act.

RG 266.180 The responsible officer should have responsibility for a function of the trading participant's business that uses the trading system. Before confirming the accuracy of the information provided in the review, the responsible officer should have reviewed evidence supporting the initial certification, material change or annual review. This evidence includes:

(a) the methodology of the review;

(b) the results of testing; and

(c) details of the qualified person who conducted the review. The officer should be satisfied that the qualified person has the appropriate technical qualifications and experience for the complexity and interconnected nature of the trading systems being reviewed and the underpinning regulatory requirements.

RG 266.181 The trading participant must document and retain records for a period of at least seven years. The records must cover the methodology, scope and results of the review, and any recommended changes applied to the control arrangements and resources of the trading system as a result of the review.

Table 7: Written statement by a responsible officer

Review type	Content of written statement	Completion timeframe	Submission to ASIC
Initial certification review	State that the information provided in the Initial Certification in relation to Rule 2.2B.6(2)(a)–(f) is accurate, including the statement about whether the trading participant has controls, arrangements and resources that meet Rules 2.2A.2 and 2.2B.2.	Before submission	Required
Material change review	Confirm compliance with Rule 2.2A.2 and Part 2.2B.	On completion of review	Not applicable
Annual review	Confirm compliance with Rule 2.2A.2 and Part 2.2B.	No later than 20 business days after completion of the review	Not applicable

Testing controls, arrangements and resources of a trading system

RG 266.182 Trading participants must have appropriate arrangements to conduct testing of their controls, arrangements and resources in relation to a trading system to ensure that they are complying with Rule 2.2A.2 and Part 2.2B. This testing should, at a minimum occur:

(a) before using a trading system for the first time (for the purposes of initial certification as outlined in RG 266.151);

(b) before implementing a material change; and

(c) annually, as necessary. For example, testing may be targeted to key risks to ensure compliance with Part 2.2B and Rule 2.2A.2 and take into account periodic testing undertaken throughout the 12-month period.

RG 266.183 In addition, trading participants must test their trading algorithms before:

(a) first using the algorithm or first making it available to a client; and

(b) implementing a material change to the algorithm (see RG 266.117–RG 266.119).

RG 266.184 If a trading system incorporates trading algorithm functionality (e.g. embedded execution algorithms), participants may adopt a unified approach to testing the trading system controls and integrated algorithms.

Types of testing and testing methodologies

RG 266.185 The nature and extent of the testing arrangements a trading participant puts in place will depend on the type of business the trading participant intends to conduct through its trading system or algorithm.

RG 266.186 Trading participants should implement a testing program that is proportionate to the risks associated with their trading systems, controls and trading algorithms. The scope, frequency and intensity of testing vary depending on the nature, scale and complexity of the participant's business and any emerging risks. A participant may develop a testing program where testing occurs across a multi-year cycle. If a trading system or trading algorithm is a critical business service, the tests may also be used for the purposes of compliance with Chapter 8B.

RG 266.187 The testing methodologies should be designed to ensure that:

(a) controls, including filters and filter parameters, work as intended;

(b) the trading system or algorithm can continue to work effectively in stressed market conditions; and

(c) testing results are quantifiable and produce clear qualitative outcomes.

RG 266.188 When testing the controls, arrangements and resources of the trading system, a trading participant should maintain a documented test strategy. The strategy should set out the intended scope of testing, test plans, test cases, test results, defect resolution and final outcomes. We may request this information to confirm the scope of testing. The testing methodology should also support an ongoing process for managing changes to the controls, arrangements and resources of the trading system over time, including material changes.

RG 266.189 Testing may include, but not be limited to:

(a) *Unit testing*—This involves testing code fragments or modules in isolation.

(b) *Conformance testing*—This involves testing system conformance with the targeted operator, execution venue and order book.

(c) *Functional testing*—This involves confirming that the trading system and filters function as intended for the proposed business.

(d) *Regression testing*—This involves running previous tests to confirm that further changes have not introduced new bugs.

(e) *Stress testing*—This involves testing both trading system logic and filters under extreme circumstances and market conditions and consideration of the system's scalability, capacity, stability and performance. This could include scenarios based on overseas case studies of volatile or stressed circumstances.

(f) *System testing*—This involves testing both trading system logic and filters when used in conjunction with other systems.

(g) *Acceptance testing*—This involves validation by end users before use within the production environment.

(h) *Capacity testing*—This involves testing that arrangements have sufficient capacity to accommodate reasonably foreseeable volumes of trading activity through the trading system and to prevent capacity limits on messaging from being breached (see RG 266.347–RG 266.350).

Testing in non-production environments

RG 266.190 A trading participant should use a non-production environment to stress test whether the trading system and trading algorithm operate as intended. This testing should assess trading system controls and algorithms against both expected order flow and severe but plausible scenarios of high-volume order flows. In particular, controls should be stress tested under conditions that simulate production use, such as a low-latency, high-message-volume and volatile environment.

RG 266.191 We recognise some trading system control scenarios may be difficult to reproduce within a development or sandbox environment. However, before going live, a trading participant is expected to take steps that reflect the size, scope and nature of the trading participant's business to test for these situations. The degree of testing should be commensurate with the degree of risk to market integrity and efficiency

G 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 266.192 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 266.193 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 266.194 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 266.195 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 266.27–RG 266.28.

RG 266.196 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 266.197 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: see Rule 2.3.3. The monthly reconciliation should be lodged through the ASIC Regulatory Portal.

H 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 266.198 This section provides guidance on the Capital Rules.

RG 266.199 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.

Lodging forms and returns

RG 266.200 A market participant should lodge capital returns using the ASIC Regulatory Portal: see Rule 9.4.2 of the Capital Rules.

RG 266.201 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 266.202 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 266.203 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 266.204 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.

I 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 imposes minimum presence requirements on those foreign market participants.

RG 266.205 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 266.206 Part 2.4 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 266.207 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 266.208 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 266.209 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 266.210 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.

J 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 266.212–RG 266.219.

We do not expect a market participant to actively seek to detect reportable matters: see RG 266.220–RG 266.231. However, we have outlined what we consider constitutes reasonable grounds to suspect that suspicious activity has occurred: see RG 266.232.

A market participant should have a clear, well-understood and documented process for complying with its obligations under Rule 3.6.1: see RG 266.246–RG 266.250.

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 266.251–RG 266.260.

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 266.257.

Market participants should notify ASIC as soon as practicable and using the ASIC Regulatory Portal: see RG 266.261–RG 266.262.

RG 266.211 This section provides guidance on a market participant's obligations under Part 3.6. 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 266.212 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 266.326, the guidance in this section applies to crossing system operators' obligations to report suspicious activity on a crossing system.

RG 266.213 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 266.214 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 266.232–RG 266.239 for guidance on the meaning of 'reasonable grounds to suspect' and RG 266.263–RG 266.265 for guidance on the content of notifications under Rule 3.6.1.

RG 266.215 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 266.216 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 266.256–RG 266.260 for further information about the interaction between Rule 3.6.1 and the AML reporting legislation.

RG 266.217 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 266.266 for further information about Rule 3.6.2, including exceptions to the rule.

RG 266.218 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 266.219 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 8 and Table 9 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 266.220 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 266.221 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 266.222 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 3.1.2A 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);

DRAFT

(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 266.223 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 8 and Table 9).

RG 266.224 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 8 and Table 9 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 266.225 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 266.226 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 266.244.

Retrospective review

RG 266.227 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 266.228 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 266.229 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 266.230 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 266.231 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 8 and Table 9), 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 266.232 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 266.233 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 266.234 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 266.235 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 266.224. Nor do we expect a market participant to

DRAFT

undertake extensive legal analysis to determine whether a contravention of the Corporations Act or market integrity rules has occurred: see RG 266.237.

RG 266.236 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 266.237 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 266.238 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 266.239 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 266.240 In RG 266.241, 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 8 and Table 9 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 266.224), 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 266.241 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 266.242 Table 8 and Table 9 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 8 and Table 9 refer to trading in shares, the indicators are equally relevant for trading in all financial products.

RG 266.243 The presence of one or more of the indicators described in Table 8 and Table 9 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 266.244 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 266.245 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 266.266.

Table 8: 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	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 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 Other indicators may include: • the type of financial product that is the subject of the order or transaction; • the amount invested (including whether this is out of proportion with the client's monetary means or earning capacity); • the risk profile of the client; • the size of the order; • the length of time the security is held; • a significant increase in profit in the client's or trader's account; and • a significant increase in the particular market participant's representative's commission 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

Primary indicator	Other indicators
An order or transaction occurs immediately before a price-sensitive announcement	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 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 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) 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
An order is placed or a transaction entered into immediately after a client opens a new account	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 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 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
A client or trader opens simultaneous positions in related derivatives (e.g. contracts for difference (CFDs) or options)	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 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 Other indicators may include: • the trading in the derivatives is inconsistent with the client’s or trader’s prior trading history or risk profile; and • the trading takes place just before a price-sensitive announcement
A trading account receives a large transfer of money before an order is placed or a transaction entered into	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 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 Another indicator may be that the authorisation on the account has recently changed

Primary indicator	Other indicators
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	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) 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 Other indicators may include: • the employee has not received internal consent for the trade; • 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 • the trading is accompanied by the trader taking simultaneous positions in related derivatives
Trading takes place before the release of a research report that has been prepared by the market participant	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) 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 Other indicators may include: • the employee has not received internal consent for the trade; and • no effective information barriers are in place between the market participant's business units 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)

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 9: 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
An order is placed: • near the close of the trading day; or • on the last day of the month, quarter, half year or financial year	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') Other indicators include: • the client or trader chooses not to buy or sell at other times of the trading day when better prices are available; 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

Primary indicator	Other indicators
An order is placed near the expiry date of related derivatives (e.g. options)	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 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
A client or trader places matched orders—prearranged trades	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' 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
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	These orders may be intended to create a false or misleading appearance of buying or selling demand ('layering the order book') 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

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 266.246 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:

(a) identifying indicators of reportable matters;

(b) ensuring that employees escalate potentially reportable matters to compliance staff, who are made aware of the indicators identified;

(c) determining whether indicators of reportable matters give rise to an obligation to report; and

(d) notifying ASIC in writing of reportable matters.

RG 266.247 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 266.246(c)) will help market participants demonstrate to ASIC compliance with the obligation under Rule 3.6.1.

RG 266.248 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 266.249 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 266.250 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 266.251 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 266.252 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 266.253 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 266.254 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 266.255 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 266.256 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 266.257 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 266.258 It is important to note that market participants cannot discharge their obligation to report under AML reporting legislation by reporting to ASIC.

RG 266.259 Market participants should refer to the Obligations and guidance page on the AUSTRAC website for information about how to comply and report, and designated services and reporting entities.

RG 266.260 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 266.261 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 266.262 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 266.263 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 266.264 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 266.265 As stated in RG 266.257, 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 266.266 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 266.267 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 266.268 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 266.269 This protection extends to the officers, employees and representatives of a market participant: s1100D.

K 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: see RG 266.274–RG 266.299;
- provide fair treatment to all users of a crossing system: see RG 266.305–RG 266.312;
- monitor activity on the crossing system, report significant breaches of its user obligations and operating procedures to ASIC, and report suspicious activity to ASIC: see RG 266.313–RG 266.324; and
- have controls to ensure the efficiency and integrity of the crossing system: see RG 266.326–RG 266.330.

Scope and application

RG 266.270 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 266.271 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 266.272 A full list of crossing systems that are registered with ASIC is available on our website.

RG 266.273 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 266.274 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 10 sets out the details required to be included in a crossing system initial report.

Table 10: 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 266.275 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 266.279–RG 266.299 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 266.276 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 266.277 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 266.278 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 266.279 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 11. More detailed guidance about what we expect a crossing system operator to disclose is provided in column 3.

Table 11: 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: (a) the minimum requirements (e.g. technical capabilities) and the process for gaining access to the system; and (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)

Making the information publicly available

RG 266.280 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 266.281 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 266.282 When a crossing system operator implements a change to the operation of the crossing system described in Table 11, 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 266.283 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 266.284 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 266.285 Publicly available crossing system information is also accessible via links on our website.

Disclosure to crossing system clients

RG 266.286 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 11, 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 12 (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 12.

RG 266.287 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 266.288 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 266.289 A crossing system operator only needs to provide the information outlined in Table 12 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 12: 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	Crossing system operators should consider including: (a) how users are expected to access the crossing system and enter orders into the crossing system; (b) technical specifications users must comply with; (c) controls for maintaining the efficiency and integrity of the crossing system; and Note: A crossing system operator has obligations under Rule 2.2A.2 in relation to the efficiency and integrity of its crossing system. (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
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	Crossing system operators should consider including: (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; (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 (c) whether the order type interacts with an exchange market or another crossing system (e.g. a shadowing arrangement)
Operations	A description of the operation of the crossing system—including, but not limited to: (a) how orders are managed, including how prices are determined and cancellations are managed; (b) details of any different treatment or arrangements for certain users or order types; (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);	Crossing system operators should consider including: (a) the hours of operation of the crossing system; (b) how orders are prioritised and matched on the crossing system (e.g. price–time priority or some other basis); (c) how order and trade cancellations are managed; (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 266.300–RG 266.304); (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); (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;

Type of information	Non-public crossing system information	Guidance
Operations (cont.)	(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 (e) how any other conflicts of interest that may arise are managed	(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); (h) the arrangements for managing conflicts of interest that may arise in relation to the crossing system; (i) the licensed market(s) to which transactions are reported (i.e. ASX 24); (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 (k) how system failures are managed, including when users will be informed and how users' orders will be managed during system failures
Fees	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	Crossing system operators should consider including: (a) disclosure of fees charged by a crossing system operator to allow another crossing system to gain access to the crossing system; (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 (c) where there are no additional fees beyond standard commission, this should be disclosed 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

RG 266.290 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 266.291 We expect that, where retail clients use a crossing system, the disclosure to them about the matters in Table 12 is clear, concise and effective.

Providing the information to clients

RG 266.292 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 266.293 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 266.294 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 266.295 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 11 and Table 12. 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 266.282.

RG 266.296 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 266.297 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 266.298 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 266.299 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 266.300 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 266.301 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 12.

RG 266.302 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 266.303 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 266.304 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 266.305 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 266.306 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 266.307 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 266.308 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 11 and Table 12.

Fairness and priority in dealing

RG 266.309 Rules 5.3.2 and 5.3.3 relate to fairness and priority when dealing with client orders in a crossing system.

RG 266.310 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 266.311 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 266.312 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 266.313 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 12; and

(b) the operating procedures of the crossing system as described in Table 12.

RG 266.314 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 266.315 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 266.326–RG 266.330.

RG 266.316 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 266.317 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 12);

(d) activity that has interfered with, or is likely to interfere with, the efficiency and integrity of the crossing system (see RG 266.326–RG 266.330);

(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 266.318 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 266.326–RG 266.330.

Managing breaches identified through monitoring activity

RG 266.319 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 266.320 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 266.321 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 266.322 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 266.323 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 266.324 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 266.325 The guidance in Section J 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 266.326 Rule 2.2A.1 requires a crossing system operator to have:

(a) appropriate automated filters designed to ensure the efficiency and integrity of its crossing system (Rule 2.2A.1(1)); and

(b) controls that enable the immediate suspension or cancellation of orders in a series of related orders (Rule 2.2A.1(2)).

RG 266.327 In relation to the obligation in Rule 2.2A.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 266.328 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 266.329 The requirement in Rule 2.2A.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 266.330 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.

L 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: see RG 266.336–RG 266.366.

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: see RG 266.366–RG 266.389.

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: see RG 266.390–RG 266.409.

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: see RG 266.410–RG 266.436.

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: see RG 266.437–RG 266.441.

Scope and application

RG 266.331 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 266.332 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 266.333 AFS licensees should also consider RG 104, which provides further guidance on complying with their obligations to have adequate resources to provide financial services and conduct supervisory arrangements: see RG 104.89–RG 104.100.

RG 266.334 ASIC has provided relief from some of the outsourcing arrangement obligations in Chapters 8A and 8B of the Rules where supply of energy or communications services may have been identified critical business services, in Chapters 8A and 8B of the Rules: see *ASIC Market Integrity Rules (Futures Markets) Class Waiver 2025/513*.

Critical business services

RG 266.335 Part 8B.2 requires market participants to implement an appropriate framework for ensuring the resilience, reliability, integrity and security of their critical business services.

Identifying critical business services

RG 266.336 Market participants must identify the critical business services relevant to their business: Rule 8B.2.1(2)(a). 'Critical business services' means functions, infrastructure, processes or systems 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 266.337 In defining critical business services, we have provided a non-exhaustive list of 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, routing and entry;

(b) clearing and settlement of transactions;

(c) payments and deliveries of securities and funds;

(d) accounting for and reconciling client money, trust accounts, securities and funds;

(e) provision of trade confirmations; and

(f) regulatory data reporting to market operators.

RG 266.338 However, identification of critical business services may vary between market participants, with differences in the nature, scale and complexity of their operations and consideration of a broad range of factors such as:

(a) the criticality of a service to users or the market participant;

(b) the potential impact on the market participant, users of the service or on market integrity in the event of disruption or prolonged disruption;

(c) any dependencies that third-party businesses may have on a service; and

(d) operational risk appetite, internal frameworks, defined indicators and limits.

Note: When considering 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*.

RG 266.339 Market participants should take care not to exclude a function, infrastructure, processes or systems from their identified critical business services solely because:

(a) it is not considered core to the business or to continuing operations, without giving due regard to other relevant considerations;

(b) contingency arrangements or workarounds are in place; or

(c) it is used by only a small number of clients.

RG 266.340 Market participants may use different terminology to describe or categorise services identified as critical business services. For example, a critical business service may be described using a label used in another regulatory regime or firm-wide framework. Market participants should be able to clearly demonstrate how such a framework satisfies their obligations under Chapter 8B. Importantly, these obligations extend beyond business continuity planning.

Adequate arrangements for critical business services

RG 266.341 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 266.342 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 (RG 266.343–RG 266.346);

(c) ensuring critical business services have sufficient and scalable capacity for the market participant's ongoing and planned operations and services (RG 266.347–RG 266.351);

(d) preventing unauthorised access to or use of critical business services (RG 266.393);

(e) managing the implementation of new critical business services and of changes to existing critical business services (RG 266.352–RG 266.365);

(f) dealing with a major event (RG 266.410–RG 266.436); and

(g) managing outsourcing arrangements for critical business services (RG 266.366–RG 266.389).

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

RG 266.343 Market participants must have adequate risk management systems and effective compliance measures to manage or mitigate risks relating to their critical business services: see section 912A(1)(d), RG 104.23–RG 104.32, RG 104.59–RG 104.66 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 266.344 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 266.345 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 comply with Rule 8B.2.1(2)(b).

RG 266.346 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 266.347 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).

System capacity management and stress testing

RG 266.348 Market participants should have sufficient system capacity to accommodate reasonably foreseeable volumes of trading activity.

RG 266.349 Systems should be adaptable and scalable to allow for changes in trading patterns and 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.

RG 266.350 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. 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.

Monitoring and review

RG 266.351 To ensure that critical business services have sufficient and scalable capacity for the participant's ongoing and planned operations and services, market participants should monitor and periodically 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.

RG 266.352 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 266.353 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*—Ensures that a system works as intended by verifying its features against its functional requirements.

(b) *Connectivity 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*—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 market integrity rules.

(d) *Regression 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.

Review and change of critical business services arrangements

RG 266.354 Periodic review of a market participant's critical business services arrangements is fundamental to ensuring the continued resilience, reliability, integrity and security of critical business services. It is also important to review that the arrangements remain within the risk appetite and risk tolerance levels of the market participant. 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 266.355 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 and apply necessary changes: Rule 8B.2.1(3).

RG 266.356 The board or senior management of the market participant should have oversight of the review.

Documentation of arrangements

RG 266.357 Market participants must document their critical business services arrangements, the scope and results of each review, and changes made to the arrangements.

Change management of critical business services

RG 266.358 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 266.359 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 266.360 Where appropriate, adequate arrangements may also include implementation of a recovery point mechanism. 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 266.361 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 is a reasonable time will depend on the nature, complexity and impact of the change, including on clients and other third parties.

RG 266.362 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). Market participants should 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 266.363 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 266.364 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 266.365 Adequate change management arrangements mitigate the risk of market disruptions and adverse impacts caused by failures of critical business services.

Outsourcing of critical business services

RG 266.366 Market participants may enter into an outsourcing arrangement with a service provider under which the service provider will provide, operate or support their critical business services. The range of outsourcing arrangements covered by Rule 8B.2.3 is intentionally broad. 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 266.367 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 266.368 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.

Note: Market participants considering outsourcing arrangements for critical business services may also refer to IOSCO Principles on outsourcing (PDF 639 KB), final report, October

2021. APRA-regulated entities should refer to Prudential Standard CPS 230 *Operational risk management*, which sets out standards for managing material service provider arrangements.

RG 266.369 ASIC has provided relief from some of the outsourcing arrangement obligations, where supply of energy or communications services may have been identified as critical business services (*ASIC Market Integrity Rules (Futures Markets) Class Waiver 2025/513*). Technology systems and associated technology infrastructure (e.g. physical and virtual data centres) provided by specialist third parties are not covered by the waiver. Reliance on the waiver should be documented for relevant areas of the obligations. It is good practice to continue to meet the requirements to the extent possible.

Due diligence inquiries

RG 266.370 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, reliably, continuously and to a high standard.

RG 266.371 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.

RG 266.372 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 a third-party service provider. Where the outsourced arrangement is with a wholly owned group entity based outside Australia there may be more focus on added risk that the market participant may not be able to exercise the same level of oversight—for example, due to time zone differences, language barriers and whether the overseas-based wholly owned group entity is familiar with Australian legislative requirements.

RG 266.373 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 266.374 When outsourcing arrangements are undertaken on a cross-border basis, market participants should consider 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 266.375 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 266.376 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 physical and cyber 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 266.377 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). Market participants should have written supervisory procedures that set out how they will monitor and oversee the outsourced tasks provided by service providers.

RG 266.378 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 266.379 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 266.380 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.

RG 266.381 Market participants should 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.

Conflicts of interest

RG 266.382 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 266.383 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 266.384 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 266.385 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.

Attestation requirement

RG 266.386 Market participants must ensure, for each outsourcing arrangement entered into after 10 March 2023 (including when an existing outsourcing arrangement is renewed or materially changed after 10 March 2023), 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).

RG 266.387 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 266.388 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.

Outsourcing involving cloud computing services

RG 266.389 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.

Information security

RG 266.390 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 266.391 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 266.392 Information assets include information and information technology, including software, hardware and data (both soft and hard copy).

RG 266.393 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 266.394 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 266.395 Market participants are not required to retain all of their 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 266.396 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 266.397 A market participant's information security arrangements should set out the responsibilities of all parties who have an obligation to maintain information security.

RG 266.398 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 266.399 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 266.400 Those responsible for information security should ensure that the market participant maintains the information security capability in this manner.

RG 266.401 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 266.402 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 266.403 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 266.404 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 266.405 A market participant should test the effectiveness of its information security controls through a systematic testing program.

Availability of access to data

RG 266.406 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 266.407 Market participants should 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 266.408 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 and carry out supervisory arrangements: 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 266.409 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 266.410 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 266.411 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.

RG 266.412 For a critical business service that is the subject of an outsourcing arrangement, a market participant must have in place adequate arrangements to ensure it can carry out its business continuity plan for that critical business service. A market participant may, subject to appropriate due diligence, rely on the service provider's business continuity plan (including any back-up or redundancy arrangements). In such situations, the service provider's plans should be referred to in the market participant's plan. Where a market participant relied on a service provider's business continuity plan for a critical business service, the participant remains responsible for ensuring that the plan satisfies its obligations under the Futures Markets Rules.

Identifying possible major events

RG 266.413 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 266.414 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 266.415 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 266.416 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 266.417 Undertaking a business impact analysis will assist market participants to identify the potential likelihood of a major event occurring and the impact a major event may have on the market participant.

RG 266.418 Market participants may apply thresholds to levels of disruption and impact as part of their business impact analysis and in identifying possible major events. Market participants should also consider potential impacts on clients, other participants and market integrity. Plans for timely and orderly restoration of usual operations following a major event should be reflected in the critical business services arrangements.

RG 266.419 Mapping assets and dependencies (including third parties and financial market infrastructures) will also help market participants to identify potential impacts when a dependency is unavailable, so they can develop appropriate workaround actions.

Appropriate to the nature, scale and complexity of their business

RG 266.420 Market participants must 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 should ensure business continuity plans 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 266.421 Market participants should consider their business risk appetite when deciding what, if any, redundancy arrangements are needed for critical business services.

RG 266.422 Market participants may consider establishing 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 266.423 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 266.424 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 266.425 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 266.426 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 266.427 Market participants must notify ASIC immediately on becoming aware of a major event: Rule 8B.4.1(6). 'Immediately' means promptly and without delay. We would consider a market participant is acting promptly and without delay if it notifies ASIC as quickly as possible in the circumstances and does not defer or postpone the notification. We also request that the participant notify ASIC when operations return to normal.

RG 266.428 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 266.429 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 266.430 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 266.431 Plan testing should identify weaknesses, develop experience in managing major events and strengthen the business continuity plan.

RG 266.432 Scenario testing 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 266.433 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 266.434 Whenever practical and useful, we recommend that market participants should participate in industry-wide or cross-border testing with other intermediaries and stakeholders and 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 266.435 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.

Documentation of plans and testing

RG 266.436 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 CPS 230, which includes information on business continuity.

Governance

RG 266.437 Market participants must have appropriate governance arrangements and adequate financial, technological and human resources to comply with their obligation under Chapter 8B: Rule 8B.5.1(1).

RG 266.438 Oversight and accountability for critical business services and business continuity should 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 266.439 Persons with responsibility for oversight are generally those 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 266.440 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 266.441 The board or senior management should 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.

Appendix 1: Procedures, determinations and practice notes

RG 266.442 Table 13 lists the old SFE procedures, determinations and practice notes relevant to the ASIC market integrity rules.

Table 13: 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 266.443 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* (RG 172) 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	*Australian Securities and Investments Commission Act 2001*
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	*ASIC Market Integrity Rules (Capital) 2021*—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	*Corporations Act 2001*, 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	*ASIC Market Integrity Rules (Futures Markets) 2017*—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 2.2.7 (for example)	A rule of the *ASIC Market Integrity Rules (Futures Markets) 2017* (in this example numbered 2.2.7) 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
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

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*

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*

CP 386: *Proposed amendments to the ASIC market integrity rules: Trading systems and automated trading.*

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 2.2A.1–2.2A.2.

Waivers

ASIC Market Integrity Rules (Futures Markets) Class Waiver 2025/513

Other publications

ACSC, *Information security manual*

APRA, CPS 220 *Risk management*

APRA, CPS 230 *Operational risk management*

APRA, CPS 234 *Information security*

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*