Australian Securities and Investments Commission

Office address (inc courier deliveries):
Level 5, 100 Market Street,
Sydney NSW 2000

Mail address for Sydney office:
GPO Box 9827,
Melbourne VIC 3001

Tel: +61 1300 935 075

www.asic.gov.au/

17 September 2024

To: All Market Participants

Identifying critical business services and notifying ASIC of major events

ASIC is committed to advancing digital and data resilience and safety as one of its strategic priorities for 2024–25. Resilient market operators and market participants are essential to the integrity of our securities and futures markets and to the efficient functioning of the economy, while cyber-attacks and other outages continue to have the potential to cause widespread disruption and harm. The market integrity rules set minimum expectations and controls to mitigate these risks and help to safeguard the integrity and resilience of Australia's markets.

This letter outlines ASIC's observations and guidance from its thematic review of market participants' arrangements for identifying their critical business services and notifying ASIC of major events in accordance with Chapter 8B of the *ASIC Market Integrity Rules (Securities Markets) 2017* and Chapter 8B of the *ASIC Market Integrity Rules (Futures Markets) 2017* (Resilience Rules).

We expect market participants to maintain a strong and continued focus on their technological and operational resilience. Market participants are required to proactively manage and test for risks to the resilience, reliability, integrity and security of critical business services and to undertake a review of their critical business services arrangements at least annually, and following each material change (Rule 8B.2.1(2)(b) and (3)).

This is not a 'set-and-forget' process. We expect that oversight and accountability for critical business services and business continuity will come from the highest levels within market participants.

When reviewing critical business services arrangements, market participants should consider the guidance outlined in this letter and in Regulatory Guides 265 and 266, and adjust their settings where required.

ASIC's observations and expectations

1 Approach to identifying critical business services

A market participant must have adequate arrangements in place to identify critical business services as part of their critical business services arrangements (Rule 8B.2.1(2)(a)).

We expect market participants to determine which services are critical in the context of their own business and consider the nature, scale and complexity of their operations. Market participants may determine the criticality of their business services based on their operational risk appetite, with defined indicators and limits (RG 265.568 and RG 266.237). In doing so, we expect market participants will carefully consider each business service, including potential impacts of disruption on clients, the market participant, third-party businesses who depend on the services and the market.

Market participants should be prepared to demonstrate their rationale for excluding any specific participant operations or services.

We observed significant differences in the ways market participants approached the identification of their critical business services. Some market participants' approaches to the identification were robust and thorough, while others lacked breadth and detail and required improvement.

We observed that some market participants relied solely on the examples provided in the Resilience Rules, RG 265.569 and RG 266.238 to identify critical business services. These examples are not exhaustive lists and should not be used verbatim in a 'tick box' manner.

We suggest a better practice approach to identifying critical business services is to start by identifying all:

- operations, activities and conduct of the participant in connection with the market of which it is a participant (participant operations); and
- services provided by the participant in connection with the market of which it is a participant (participant services).

Market participants can then identify the supporting functions, infrastructure, processes and systems that underpin those participant operations and participant services. They should then consider which of these, in the event of failure, would likely cause significant disruption to their operations or services.

Market participants should make an assessment as to which disruptions are likely to be significant or material, after considering potential impacts on the business, clients, other participants and market integrity. Market participants may use internal frameworks to implement thresholds reflecting tolerance levels.

2 Improper exclusion of critical business services

Comprehensive identification of critical business services is an essential first step to ensure market participants have adequate critical business services arrangements that comply with Rule 8B.2.1 of the Resilience Rules. It is also integral to ensuring market participants are operationally and technologically resilient.

We observed that some market participants excluded potential critical business services solely on the basis that:

(a) they were not considered core to the business or to continuing operations; or
(b) contingency arrangements or workarounds were in place; or
(c) they were used by only a small number of clients.

We encourage market participants to take a holistic approach to identifying their critical business services and consider a range of relevant factors when assessing the potential for disruption or impact.

(a) A participant operation or service should not be excluded solely on the basis that it is not considered core to the business or to continuing operations

Some market participants excluded certain participant operations or services from their critical business services simply because they were not considered core to the business or essential to continuing operations, without due regard to other relevant considerations. For example, some participants did not consider that operational failures of real-time trade surveillance capabilities and compliance operations would likely cause significant disruption to participant operations. Where a market participant conducts high-volume trading or its surveillance system produces a high level of potential misconduct alerts, we would expect that system to be considered for inclusion.

Failure of a trade surveillance system or compliance function to operate effectively may result in a failure to detect, prevent or disrupt prohibited conduct such as market manipulation. This may be likely to cause significant disruption to participant operations or materially impact participant services. Instances of market manipulation may also have a significant and detrimental impact on markets and investors if undetected. In times of operational disruption, there may also be increased instances of bad actors targeting markets with prohibited behaviours.

Failure of participant operations or services may also lead to a breach of regulatory obligations. We remind market participants of their trading and pre- and post-trade transparency obligations under the market integrity rules (Chapters 5 and 6 of the *ASIC Market Integrity Rules (Securities Markets) 2017* and Chapter 3 of the *ASIC Market Integrity Rules (Futures Markets) 2017*).

Market participants should consider a range of factors when assessing whether a failure of a function, infrastructure, process or system to operate effectively would likely cause significant disruption to participant operations, including the nature, scale and complexity of their operations. Market participants should also consider the potential impacts beyond their own commercial interests including, where relevant, harm to consumers, other participants and market integrity.

The Resilience Rules are principles-based, not prescriptive, and the examples discussed in this letter indicate some aspects of your business that should be considered in the identification of critical business services.

(b) A critical business service should not be excluded solely on the basis that contingency arrangements or workarounds are in place

We observed that some market participants determined that a function, infrastructure, process or system was not a critical business service solely because they had a contingency plan or work-around solution for a participant operation or participant service (or a function, infrastructure, process or system that delivers or supports it).

Rule 8B.2.1(2)(b) of the Resilience Rules requires participants to have adequate arrangements for managing any risks to the resilience, reliability, integrity and security of critical business services. This may include implementing contingency plans or workarounds.

However, having contingency arrangements in place does not mean that a function, infrastructure, process or system is not a critical business service. The existence of contingency arrangements may in some instances reflect the criticality of a function, infrastructure, process or system and its potential to cause significant disruption or have a material impact in the event of failure. We note that contingency arrangements are also at risk of failure.

We also observed that some market participants were unsure of the extent to which critical business services required backup arrangements. Rule 8B.4.1(1) of the Resilience Rules requires participants to establish, implement and maintain plans (Business Continuity Plans or BCPs) for effectively responding to an event that would or would be likely to cause significant disruption to participant operations or materially impact the participant services (Major Event). However, we do not expect market participants to have full redundancy arrangements for every critical business service or to duplicate all systems and vendors. Market participants need to consider the nature, scale and complexity of their critical business services, participant operations and participant services, as well as their structure and location when assessing the appropriateness of their business continuity plans (Rule 8B.4.1(3) of the Resilience Rules). Also, when assessing adequacy of critical business services arrangements, market participants should ensure they are commensurate with the nature, scale and complexity of the services offered.

(c) A participant operation or service should not immediately be excluded because it is used by only a small number of clients

Some market participants determined that certain participant operations or services (such as an algorithmic trading service offering) were not a critical business service on the basis that they are only used by a small group of clients or carry low trade volumes.

A market participant should consider the characteristics of the service and clients using the service in determining whether a failure of a function, infrastructure, process or system might have a material impact on participant services and therefore be a critical business service. Even where few clients rely on a participant service, the market participant should consider the potential extent to which clients would be affected if it cannot provide the service (e.g. substitutes available to clients, frequency of use, how reliant clients are on the service on a day-to-day basis). Market participants should also consider the potential for disruption to a function, infrastructure, process or system to affect their financial position and reputation.

We will continue to monitor the identification of critical business services to ensure none are inappropriately excluded.

3 Documenting critical business services

Rule 8B.2.1(4) of the Resilience Rules requires a market participant to document its critical business services arrangements and details of reviews and changes to those arrangements. We observed that some market participants had difficulty demonstrating their approach to identifying their critical business services or had poor processes for maintaining records of their critical business services.

A market participant should be able to clearly demonstrate its rationale in assessing and identifying critical business services, including its consideration of functions, infrastructure, processes and systems it determined were not critical business services. Market participants should consider maintaining these documents in a centralised location.

Some market participants used different terminology to describe their critical business services, either to categorise different critical business services, to align with other regulatory regimes or with existing firm-wide terminology. Examples included labelling certain critical business services as ‘dependencies’ or ‘subservices’. These dependencies are functions, infrastructure, processes and systems identified as likely to impact participant operations or services. In some cases, the ‘dependencies’ were maintained in separate documents. In other cases, they were mapped to the critical business services. Where such terminology is used, an example of better practice is to carry out this mapping of arrangements to demonstrate compliance with the Resilience Rules.

All functions, infrastructure, processes and systems that, in the event of failure to operate effectively, would likely cause significant disruption to participant operations, activities or conduct, or materially impact participant services should be classified as critical business services. Irrespective of any other labels a market participant may use to describe or categorise these, they should still be identified as critical business services and treated as such under the Resilience Rules.

4 Reliance on existing frameworks

We observed that some market participants relied partly or entirely on existing frameworks relating to technological and operational resilience when implementing their critical business services arrangements.

Examples include critical business services identified by reference to a market participant's BCP, global risk framework, international regulatory obligations or ASX Guidance Note 10, which provide definitions of 'criticality' and an existing scope of key systems and processes.

A market participant that assumes that existing frameworks satisfy the Resilience Rules risks failing to identify critical business services and contravening their obligations to have in place adequate arrangements to ensure their resilience, reliability, integrity and security. For example, the scope of many BCPs is narrower than the critical business services definition in the Resilience Rules. The Resilience Rules focus on technological and operational resilience for the day-to-day running of participant operations and services and are not limited to business continuity events. Further, a participant should not consider that a function, infrastructure, process or system is not a critical business service solely because a failure of the operation or service would not trigger a business continuity event.

We expect market participants to be able to clearly demonstrate how existing frameworks or elements of them comply with Chapter 8B of the Resilience Rules. We recommend market participants undertake and document a comprehensive gap analysis to ensure compliance with the obligations in the Resilience Rules.

5 Outsourcing critical business services

Rule 8B.2.3 of the Resilience Rules provides a framework for managing the risks associated with outsourcing arrangements. An outsourcing arrangement is an arrangement between the market participant and a third-party service provider (including a related body corporate) to provide, operate or support one or more of the market participant's critical business services. The Resilience Rules are designed to mitigate risks associated with third parties providing services or performing tasks that are critical to the market participant's business and on which the business is dependent.

We observed that some market participants did not identify which of their critical business services were outsourced. Market participants should have an end-to-end view of outsourced critical business services to adequately identify and manage outsourcing risks. Market participants' critical business services arrangements must include arrangements for managing outsourcing arrangements in relation to critical business services (Rule 8B.2.1(2)(g) of the Resilience Rules).

Where it has an outsourcing arrangement in respect of a critical business service, a market participant may rely on the third-party service provider's BCP (including any back up/redundancy arrangements) for that outsourced service. As detailed in Rules 8B.4.1(2)(a) and (b) of the Resilience Rules, a market participant's BCPs must be designed to enable continuity of usual operation of critical business services, participant operations and participant services during a Major Event. To the extent this is not possible, timely and orderly restoration of those usual operations should be the focus.

A market participant must have in place adequate arrangements to ensure it can carry out its BCPs with respect to any critical business services the subject of an outsourcing arrangement (Rule 8B.4.1(5) of the Resilience Rules). We expect that where a service provider's BCP is relied on, the participant's due diligence should ensure all Resilience Rules obligations are met. In such a case, the service provider's plans should be incorporated by reference into the market participant's own BCP as the two will be interrelated and contain some overlap.

A market participant entering an outsourcing arrangement must comply with the requirements outlined in Rule 8B.2.3(1) of the Resilience Rules (covering, among other things, due diligence, legally binding agreements and performance management) in a manner that is appropriate to the nature, complexity and risks of the arrangement and materiality of the arrangement to the participants' operations and services (Rule 8B.2.3(2) of the Resilience Rules). For each outsourcing arrangement, the board or a director or senior manager must confirm and attest that the market participant's obligations under the Resilience Rules have been met (Rule 8B.2.3(1)(h)).

6 Major Event notification

A market participant's critical business services arrangements must include arrangements for dealing with a Major Event (Rule 8B.2.1(2)(f) of the Resilience Rules).

As part of their business impact analysis, in determining the types of Major Events that may affect the participant's critical business services, participant operations and participant services (Rule 8B.4.1(4)(a) of the Resilience Rules), market participants may choose to apply thresholds to levels of expected disruption and potential impacts to participant operations and services. 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 (Rule 8B.4.1(2) of the Resilience Rules).

Rule 8B.4.1(6) of the Resilience Rules and RG 265.664 and RG266.333 state that a market participant must notify ASIC immediately upon becoming aware of a Major Event. We have elaborated on our guidance to clarify that 'immediately' means promptly and without delay rather than instantaneously. 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.

The importance of market participants maintaining a strong and continued focus on their technological and operational resilience continues to be a strategic and enforcement priority for ASIC.

We will continue to engage with market participants on this topic and test compliance with Chapter 8B of the Resilience Rules. We will also consider taking enforcement action where we identify significant breaches of the Resilience Rules.

Our thematic review observations indicated opportunities for market participants to improve their implementation of appropriate frameworks to ensure the resilience, reliability, integrity and security of their critical business services. When reviewing critical business services arrangements, market participants should consider the guidance outlined in this letter and in Regulatory Guides 265 and 266, and improve their settings where required.

Market Conduct
Australian Securities and Investments Commission