ASIC Market Integrity Rules (Securities Markets and Futures Markets) Amendment Instrument 2022/74

I, Calissa Aldridge, delegate of the Australian Securities and Investments Commission, make the following legislative instrument.

Date 9 March 2022

Calissa Aldridge

Contents

Part 1—Preliminary

1 Name of legislative instrument

This is the *ASIC Market Integrity Rules (Securities Markets and Futures Markets) Amendment Instrument 2022/74*.

2 Commencement

This instrument commences on the day that is 12 months after the day it is registered on the Federal Register of Legislation.

Note: The register may be accessed at www.legislation.gov.au.

3 Authority

This instrument is made under subsection 798G(1) of the *Corporations Act 2001*.

4 Schedules

Each instrument that is specified in a Schedule to this instrument is amended or repealed as set out in the applicable items in the Schedule concerned, and any other item in a Schedule to this instrument has effect according to its terms.

5 Repeal of amending and repealing instruments

(1) The repeal of an instrument by section 4 does not affect any amendment to or repeal of another instrument (however described) made by the instrument.

(2) Subsection (1) does not limit the effect of section 7 of the *Acts Interpretation Act 1901* as it applies to the repeal of an instrument by section 4 of this instrument.

Schedule 1—Amendments to the ASIC Market Integrity Rules (Securities Markets) 2017

1 Rule 9.1.3

Repeal the rule.

2 After Chapter 8

Insert:

Chapter 8A: Market operators—Critical Business Services, Information Security and Business Continuity Plans

Part 8A.1 Application and Definitions

8A.1.1 Application of Chapter

This Chapter applies to:

(a) the operator of a Market on or through which offers to acquire or dispose of Equity Market Products are made or accepted; and

(b) the operator of a CGS Market.

8A.1.2 Definitions

In this Chapter:

Business Continuity Plans has the meaning given by Rule 8A.5.1.

Critical Business Services, in relation to an Operator, means functions, infrastructure, processes or systems which in the event of failure to operate effectively, would or would be likely to cause significant disruption to the Operator's Market Operations or materially impact the Operator's Market Services.

> Note: Critical Business Services referred to in this definition would generally include but are not limited to, functions, infrastructure, processes and systems that deliver or support order entry, routing and matching, trade execution, dissemination of market data, trading risk management, market surveillance, reporting of executed trades to a clearing and settlement facility and regulatory data reporting.

Critical Business Services Arrangements has the meaning given by Rule 8A.3.1.

Incident has the meaning given by subparagraph 8A.5.1(6)(a)(i).

Information Asset means information and information technology, including software, hardware and data (both soft and hard copy).

Major Event has the meaning given by Rule 8A.5.1.

Market Operations, in relation to an Operator, means the operations, activities and conduct of the Operator's Market or CGS Market (as the case may be) or of the Operator in connection with that Market or CGS Market.

Market Services, in relation to an Operator, means the services, data and associated products provided by the Operator in connection with the Operator's Market or CGS Market (as the case may be).

Operator means an operator referred to in paragraph 8A.1.1(a) or (b).

Outsourcing Arrangement means an arrangement between an Operator and another person (***Service Provider***) under which the Service Provider will provide, operate or support one or more of the Operator's Critical Business Services.

Participant means a Participant of a Market referred to in paragraph 8A.1.1(a) or of a CGS Market.

Service Provider: has the meaning given in the definition of ***Outsourcing Arrangement***.

Part 8A.2 Trading controls

8A.2.1 Operator to have trading controls

An Operator must have controls, including automated controls, that enable immediate suspension, limitation or prohibition of the entry by a Participant of Trading Messages where required for the purposes of ensuring the Market or CGS Market (as the case may be) is fair, orderly and transparent.

Part 8A.3 Critical Business Services

8A.3.1 Resilience, reliability, integrity and security

Adequate arrangements

(1) An Operator must have adequate arrangements (***Critical Business Services Arrangements***) to ensure the resilience, reliability, integrity and security of its Critical Business Services.

Note: Arrangements referred to in subrule (1) would generally include, but are not limited to, policies, procedures and organisational resources including financial, human and technological resources.

(2) Without limiting subrule (1), an Operator's Critical Business Services Arrangements must include arrangements for:

(a) identifying Critical Business Services; and

(b) identifying, assessing, managing and monitoring for any risks to the resilience, reliability, integrity and security of Critical Business Services; and

(c) ensuring Critical Business Services have sufficient and scalable capacity for ongoing and planned Market Operations and Market Services; and

(d) preventing unauthorised access to or use of Critical Business Services; and

(e) managing the implementation of new Critical Business Services and of changes to existing Critical Business Services in accordance with Rule 8A.3.2; and

(f) dealing with a Major Event in accordance with Part 8A.5 of these Rules; and

(g) managing Outsourcing Arrangements in relation to Critical Business Services in accordance with Rule 8A.3.3.

Review and change of arrangements

(3) An Operator must undertake a review of its Critical Business Services Arrangements:

(a) following each material change to its Critical Business Services; and

(b) at least once every 12 months,

and apply recommended changes to the Critical Business Services Arrangements arising from the review to ensure they comply with subrules (1) and (2).

Documentation of arrangements

(4) An Operator must document:

(a) its Critical Business Services Arrangements; and

(b) the scope and results of each review performed in accordance with subrule (3); and

(c) any changes applied to the Critical Business Services Arrangements as a result of the review or otherwise,

and must maintain that documentation for a period of at least seven years from the later of the date it is created or the date it is last amended.

8A.3.2 Change management for Critical Business Services

(1) An Operator must have adequate arrangements to ensure that its Critical Business Services Arrangements continue to comply with subrule 8A.3.1(1) following the implementation of a new Critical Business Service or of a change to an existing Critical Business Service.

(2) Without limiting subrule (1), the arrangements referred to in that subrule must include arrangements for:

(a) testing new Critical Business Services or material changes to existing Critical Business Services before implementation; and

(b) communicating with persons that may be materially impacted by the implementation for the purposes of ensuring those persons are adequately informed about the nature, timing and impact of the implementation a reasonable time before it occurs; and

(c) ensuring, to the extent reasonably practicable, that persons that may be materially impacted by the implementation are adequately prepared for the implementation before it occurs.

> Note: Persons that may be materially impacted by the implementation may include ASIC, Participants, other Operators and the operators of licensed clearing and settlement facilities.

(3) Without limiting paragraph (2)(b), an Operator must give written notice of the proposed implementation to ASIC a reasonable time before the implementation.

8A.3.3 Outsourcing of Critical Business Services

(1) An Operator that enters into an Outsourcing Arrangement must:

(a) before entering into the Outsourcing Arrangement, conduct due diligence enquiries for the purposes of ensuring the Service Provider has the ability and capacity to provide the services covered by the Outsourcing Arrangement effectively; and

(b) ensure that the Outsourcing Arrangement is contained in a documented legally binding agreement between the Operator and the Service Provider that:

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

  (ii) requires the Service Provider to give written notice to the Operator before the Service Provider:

    (A) enters into any arrangement with another person (***Sub-Contractor***) under which the Sub-Contractor will provide services material to the provision by the Service Provider of the services covered by the Outsourcing Arrangement; and

(B) makes any other material change to the manner in which the services covered by the Outsourcing Arrangement are provided; and

(iii) deals with the circumstances and manner in which the Outsourcing Arrangement may be terminated; and

(iv) provides for the orderly transfer of services provided under the Outsourcing Arrangement to the Operator or another Service Provider in the event of termination of the Outsourcing Arrangement; and

(c) while the Outsourcing Arrangement is in place, monitor the performance of the Service Provider for the purposes of ensuring the Service Provider is providing the services covered by the Outsourcing Arrangement effectively and has the ability and capacity to continue to provide those services effectively; and

(d) have in place adequate arrangements to:

(i) identify any conflicts of interest between the Operator and the Service Provider, including conflicts involving Sub-Contractors and related entities of the Operator, Service Provider and any Sub-Contractor; and

(ii) manage any conflicts of interest which have been identified or could arise; and

(e) have in place adequate arrangements to ensure the Operator is able to comply with its obligations under the Act and these Rules in relation to the Critical Business Services the subject of an Outsourcing Arrangement including, without limitation, arrangements with the Service Provider to:

(i) ensure the resilience, reliability, integrity and security of those Critical Business Services in accordance with Rule 8A.3.1; and

(ii) ensure the confidentiality, integrity and availability of information obtained, held or used by the Operator in relation to those Critical Business Services in accordance with Part 8A.4 of these Rules; and

(iii) deal with a Major Event in accordance with Part 8A.5 of these Rules; and

Note: Such arrangements may include, without limitation, requirements on the Service Provider to:

(a) protect technology from security breaches and cyber-incidents; and
(b) protect proprietary and client-related information and software; and
(c) protect confidential, market-sensitive and personal information from intentional or inadvertent disclosure to unauthorised individuals; and
(d) establish, implement and maintain emergency procedures and a plan for disaster recovery with periodic testing of backup facilities.

(f) ensure that the Operator and its auditors are able to promptly, upon request, access books, records and other information of the Service Provider relating to the Critical Business Services; and

(g) ensure that ASIC has the same access to all books, records and other information relating to the Critical Business Services and maintained by the Service Provider, that ASIC would have if not for the Outsourcing Arrangement; and

(h) ensure that for each Outsourcing Arrangement, the Operator's Board or a director or senior manager have confirmed that they have complied with the Operator's obligations in this subrule and made a written attestation to that effect.

(2) The Operator must comply with subrule (1) in a manner that is appropriate to:

(a) the nature, complexity and risks of the Outsourcing Arrangement; and

(b) the materiality of the Outsourcing Arrangement to the Operator's Market Operations and Market Services.

(3) In determining for the purposes of subrule (1) whether the Service Provider has the ability and capacity to provide the services covered by the Outsourcing Arrangement effectively, the Operator must take into account the extent to which the Service Provider is providing the same or similar services to other Operators and Participants.

(4) An Operator must give written notice to ASIC as soon as practicable after the Operator enters into an Outsourcing Arrangement, and in any event no later than 20 business days after entering into the Outsourcing Arrangement.

Part 8A.4 Information security

8A.4.1 Information security

(1) An Operator must have adequate arrangements to ensure the confidentiality, integrity and availability of information obtained, held or used by the Operator in relation to its Market Operations and Market Services.

(2) Without limiting subrule (1), the arrangements referred to in that subrule must include:

(a) arrangements to identify and document Information Assets that are integral to the provision of the Operator's Market Operations and Market Services; and

(b) controls, including automated controls, designed to prevent unauthorised access to Information Assets; and

(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.

(3) An Operator must have adequate arrangements to ensure the availability of access to data obtained, held or used by the Operator in its Market Operations and Market Services.

(4) Without limiting subrule (3), the arrangements referred to in that subrule must include arrangements designed to provide for the backup of the data and the timely recovery of the data in the event of any theft, corruption or loss of the data.

(5) An Operator must notify ASIC in writing, as soon as possible and, in any case, no later than 72 hours, after becoming aware 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.

Part 8A.5 Business Continuity Plans

8A.5.1 Business continuity

Business Continuity Plans

(1) An Operator must establish, implement and maintain plans (***Business Continuity Plans***) for effectively responding to an event (***Major Event***) that would or would be likely to cause significant disruption to the Operator's Market Operations or materially impact the Operator's Market Services.

> Note: A Major Event may include the failure of or disruption to a Critical Business Service, including one operated by a Service Provider, or an event such as a pandemic or influenza event, natural disaster, cyber-attack or power failure.

(2) An Operator's Business Continuity Plans must be designed to enable:

(a) continuity of the usual operation of the Operator's Critical Business Services, Market Operations and Market Services during a Major Event; and

(b) to the extent continuation of the usual operation of the Operator's Critical Business Services, Market Operations and Market Services during a Major Event is not possible, timely and orderly restoration of those usual operations following the Major Event.

(3) An Operator's Business Continuity Plans must be appropriate to the nature, scale and complexity of the Operator's Critical Business Services, Market Operations and Market Services and to the Operator's structure and location.

(4) Without limiting subrules (1) to (3), the Operator's Business Continuity Plans must identify and address:

(a) the types of Major Events that may impact the Operator's Critical Business Services, Market Operations and Market Services; and

(b) activation procedures including trigger conditions for enacting the Operator's Business Continuity Plans; and

(c) the potential impact Major Events may have on the Operator's Critical Business Services, Market Operations and Market Services; and

(d) the classification of types of Major Events according to the potential severity of the impacts referred to in paragraph (c); and

(e) escalation procedures that are appropriate to the classification referred to in paragraph (d); and

(f) the actions, arrangements and resources required to achieve the outcomes referred to in subrule (2); and

Note: The actions, arrangements and resources covered by this paragraph would include key operational functions and processes, staff, alternate suppliers/service providers, technology, alternative premises and other physical infrastructure.

(g) specific objectives for the time taken to achieve the outcomes referred to in paragraph (2)(b); and

(h) procedures for communicating during a Major Event with persons that may be impacted by the Major Event, for the purposes of ensuring those persons are adequately informed about:

(i) the nature and impact of the Major Event; and

(ii) the steps that are being taken or will be taken to manage the Major Event; and

(iii) the likely timing of the steps referred to in subparagraph (ii); and

(iv) the likely timing of the resumption of the usual operation of the Operator's Critical Business Services, Market Operations and Market Services; and

(i) any operational dependencies between the Operator and any other person that may affect the matters referred to in paragraphs (a) to (h).

(5) Without limiting paragraph (4)(i), an Operator must have in place adequate arrangements to ensure that the Operator is able to carry out its Business Continuity Plans with respect to any Critical Business Services the subject of an Outsourcing Arrangement.

Notification of an Incident or Major Event

(6) Without limiting paragraph (4)(h), an Operator must:

(a) notify ASIC immediately upon becoming aware of:

(i) an unexpected disruption to the usual operation of the Operator's Critical Business Services that may interfere with the fair, orderly or transparent operation of any Market or CGS Market (***Incident***); or

(ii) a Major Event; and

(b) notify other Operators, operators of Clearing Facilities and Participants that may be impacted by an Incident or a Major Event, as soon as practicable after becoming aware of the Incident or Major Event.

(7) If a notification is made under subrule (6), the Operator must within seven days of the notification provide ASIC with a written report detailing:

(a) the circumstances of the Incident or Major Event; and

(b) the steps taken to manage the Incident or Major Event.

Review, update and testing of plans

(8) An Operator must:

(a) review and test its Business Continuity Plans and the arrangements referred to in subrule (5):

(i) at a frequency and in a manner appropriate to the nature, scale and complexity of the Operator's Critical Business Services, Market Operations and Market Services and to the Operator's structure and location; and

(ii) at a minimum:

(A) each time there is a material change to the Operator's Critical Business Services, Market Operations and Market Services or to the Operator's structure and location; and

(B) as soon as practicable after the occurrence of a Major Event; and

(C) once every 12 months; and

(b) update the Business Continuity Plans as required to ensure they comply with subrules (1) to (4).

Documentation of plans and testing

(9) An Operator must document:

(a) its Business Continuity Plans; and

(b) the scope and results of all reviews and testing performed in accordance with subrule (8),

and must maintain that documentation for a period of at least seven years from the later of the date it is created or the date it is last amended.

Part 8A.6 Governance

8A.6.1 Responsibility for compliance

(1) An Operator must have appropriate governance arrangements and adequate financial, technological and human resources to comply with its obligations under this Chapter 8A.

(2) Without limiting subrule (1), the arrangements referred to in that subrule must include arrangements for the Operator's Board or senior management to have oversight of the establishment, implementation, maintenance, review, testing and documentation of the Operator's Business Continuity Plans.

Chapter 8B: Market Participants—Critical Business Services, Information Security and Business Continuity Plans

Part 8B.1 Application and Definitions

8B.1.1 Application of Chapter

This Chapter applies to:

(a) Participants of a Market on or through which offers to acquire or dispose of Equity Market Products are made or accepted;

(b) CGS Market Participants.

8B.1.2 Definitions

In this Chapter:

Business Continuity Plans has the meaning given by Rule 8B.4.1.

Critical Business Services, in relation to a Participant, means functions, infrastructure, processes or systems which in the event of failure to operate effectively, would or would be likely to cause significant disruption to the Participant's Participant Operations or materially impact the Participant's Participant Services.

> Note: Critical Business Services referred to in this definition would generally include but are not limited to, functions, infrastructure, processes and systems that deliver or support order acceptance, routing and entry, clearing and settlement of transactions, payments and deliveries of financial products and funds, accounting for or reconciling client money, trust accounts, securities and funds, confirmations and regulatory data reporting.

Critical Business Services Arrangements has the meaning given by Rule 8B.2.1.

Information Asset means information and information technology, including software, hardware and data (both soft and hard copy).

Major Event has the meaning given by Rule 8B.4.1.

Operator means an operator of a Market referred to in paragraph 8B.1.1(a) or of a CGS Market.

Outsourcing Arrangement means an arrangement between a Participant and another person (***Service Provider***) under which the Service Provider will provide, operate or support one or more of the Participant's Critical Business Services.

Participant means a participant referred to in paragraph 8B.1.1(a) or (b).

Participant Operations, in relation to a Participant, means the operations, activities or conduct of the Participant in connection with the Markets and CGS Markets of which it is a Participant.

Participant Services, in relation to a Participant, means the services provided by the Participant in connection with the Markets and CGS Markets of which it is a Participant.

Service Provider: has the meaning given in the definition of ***Outsourcing Arrangement***.

Part 8B.2 Critical Business Services

8B.2.1 Resilience, reliability, integrity and security

Adequate arrangements

(1) A Participant must have adequate arrangements (***Critical Business Services Arrangements***) to ensure the resilience, reliability, integrity and security of its Critical Business Services.

> Note: Arrangements referred to in subrule (1) would generally include, but are not limited to, policies, procedures and organisational resources including financial, human and technological resources.

(2) Without limiting subrule (1), a Participant's Critical Business Services Arrangements must include arrangements for:

(a) identifying Critical Business Services; and

(b) identifying, assessing, managing and monitoring for any risks to the resilience, reliability, integrity and security of Critical Business Services; and

(c) ensuring Critical Business Services have sufficient and scalable capacity for the Participant's ongoing and planned Participant Operations and Participant Services; and

(d) preventing unauthorised access to or use of Critical Business Services; and

(e) managing the implementation of new Critical Business Services and of changes to existing Critical Business Services in accordance with Rule 8B.2.2; and

(f) dealing with a Major Event in accordance with Part 8B.4 of these Rules; and

(g) managing Outsourcing Arrangements in relation to Critical Business Services in accordance with Rule 8B.2.3.

Review and change of arrangements

(3) A Participant must undertake a review of its Critical Business Services Arrangements:

(a) following each material change to its Critical Business Services; and

(b) at least once every 12 months,

and apply recommended changes to the Critical Business Services Arrangements arising from the review to ensure they comply with subrules (1) and (2).

Documentation of arrangements

(4) A Participant must document:

(a) its Critical Business Services Arrangements; and

(b) the scope and results of each review performed in accordance with subrule (3); and

(c) any changes applied to the Critical Business Services Arrangements as result of a review or otherwise,

and must maintain that documentation for a period of at least seven years from the later of the date it is created or the date it is last amended.

8B.2.2 Change management for Critical Business Services

(1) A Participant must have adequate arrangements to ensure that its Critical Business Services Arrangements continue to comply with subrule 8B.2.1(1) following the implementation of a new Critical Business Service or of a change to an existing Critical Business Service.

(2) Without limiting subrule (1), the arrangements referred to in that subrule must include arrangements for:

(a) testing new Critical Business Services or material changes to existing Critical Business Services before implementation; and

(b) communicating with persons that may be materially impacted by the implementation for the purposes of ensuring those persons are adequately

informed about the nature, timing and impact of the implementation a reasonable time before it occurs; and

(c) ensuring, to the extent reasonably practicable, that persons that may be materially impacted by the implementation are adequately prepared for the implementation before it occurs.

Note: Persons that may be materially impacted by the implementation may include ASIC, other Participants, Operators and the operators of licensed clearing and settlement facilities.

8B.2.3 Outsourcing of Critical Business Services

(1) A Participant that enters into an Outsourcing Arrangement must:

(a) before entering into the Outsourcing Arrangement, conduct due diligence enquiries for the purposes of ensuring the Service Provider has the ability and capacity to provide the services covered by the Outsourcing Arrangement effectively; and

(b) ensure that the Outsourcing Arrangement is contained in a documented legally binding agreement between the Participant and the Service Provider, that:

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

(ii) requires the Service Provider to give written notice to the Participant before the Service Provider:

(A) enters into any arrangement with another person (***Sub-Contractor***) under which the Sub-Contractor will provide services material to the provision by the Service Provider of the services covered by the Outsourcing Arrangement; or

(B) makes any other material change to the manner in which the services covered by the Outsourcing Arrangements are provided; and

(iii) deals with the circumstances and manner in which the Outsourcing Arrangement may be terminated; and

(iv) provides for the orderly transfer of services provided under the Outsourcing Arrangement to the Participant or another Service Provider in the event of termination of the Outsourcing Arrangement; and

(c) while the Outsourcing Arrangement is in place, monitor the performance of the Service Provider for the purposes of ensuring the Service Provider is providing the services covered by the Outsourcing Arrangement effectively and has the ability and capacity to continue to provide those services effectively; and

(d) have in place adequate arrangements to:

(i) identify any conflicts of interest between the Participant and the Service Provider, including conflicts involving Sub-Contractors and related entities of the Participant, Service Provider and any Sub-Contractor; and

(ii) manage any conflicts of interest which have been identified or could arise; and

(e) have in place adequate arrangements to ensure the Participant is able to comply with its obligations under the Act and these Rules in relation to the Critical Business Services the subject of an Outsourcing Arrangement including, without limitation, arrangements with the Service Provider to:

(i) ensure the resilience, reliability, integrity and security of those Critical Business Services in accordance with Rule 8B.2.1; and

(ii) ensure the confidentiality, integrity and availability of information obtained, held or used by the Participant in relation to those Critical Business Services in accordance with Part 8B.3 of these Rules; and

(iii) deal with a Major Event in accordance with Part 8B.4 of these Rules; and

Note: Such arrangements may include, without limitation, requirements on the Service Provider to:

(a) protect technology from security breaches and cyber-incidents; and
(b) protect proprietary and client-related information and software; and
(c) protect confidential, market-sensitive and personal information from intentional or inadvertent disclosure to unauthorised individuals; and
(d) establish, implement and maintain emergency procedures and a plan for disaster recovery with periodic testing of backup facilities.

(f) ensure that the Participant and its auditors are able to promptly, upon request, access books, records and other information of the Service Provider relating to the Critical Business Services; and

(g) ensure that ASIC has the same access to all books, records and other information relating to the Critical Business Services and maintained by the Service Provider, that ASIC would have if not for the Outsourcing Arrangement; and

(h) ensure that for each Outsourcing Arrangement, the Participant's Board or a director or senior manager have confirmed that they have complied with the Participant's obligations in this subrule and made a written attestation to that effect.

(2) The Participant must comply with subrule (1) in a manner that is appropriate to:

(a) the nature, complexity and risks of the Outsourcing Arrangement; and

(b) the materiality of the Outsourcing Arrangement to the Participant's Participant Operations and Participant Services.

(3) In determining for the purposes of subrule (1) whether the Service Provider has the ability and capacity to provide the services covered by the Outsourcing Arrangement effectively, the Participant must take into account the extent to which the Service Provider is providing the same or similar services to other Participants.

Part 8B.3 Information security

8B.3.1 Information security

(1) A Participant must have adequate arrangements to ensure the confidentiality, integrity and availability of information obtained, held or used by the Participant in relation to its Participant Operations and Participant Services.

(2) Without limiting subrule (1), the arrangements referred to in that subrule must include:

(a) arrangements to identify and document Information Assets that are integral to the provision of the Participant's Participant Operations and Participant Services; and

(b) controls, including automated controls, designed to prevent unauthorised access to Information Assets; and

(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.

(3) A Participant must have adequate arrangements to ensure the availability of access to data obtained, held or used by the Participant in its Participant Operations and Participant Services.

(4) Without limiting subrule (3), the arrangements referred to in that subrule must include arrangements designed to provide for the backup of the data and the timely recovery of the data in the event of any theft, corruption or loss of the data.

(5) A 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.

Part 8B.4 Business Continuity Plans

8B.4.1 Business continuity

Business Continuity Plans

(1) A Participant must establish, implement and maintain plans (***Business Continuity Plans***) for effectively responding to an event (***Major Event***) that would

or would be likely to cause significant disruption to the Participant's Participant Operations or materially impact the Participant's Participant Services.

Note: A Major Event may include the failure of a Critical Business Service, including one operated by a Service Provider, or an event such as a pandemic or influenza event, natural disaster, cyber-attack or power failure.

(2) A Participant's Business Continuity Plans must be designed to enable:

(a) continuity of the usual operation of the Participant's Critical Business Services, Participant Operations and Participant Services during a Major Event; and

(b) to the extent continuation of the usual operation of the Participant's Critical Business Services, Participant Operations and Participant Services during a Major Event is not possible, timely and orderly restoration of those usual operations following the Major Event.

(3) A Participant's Business Continuity Plans must be appropriate to the nature, scale and complexity of the Participant's Critical Business Services, Participant Operations and Participant Services and to the Participant's structure and location.

(4) Without limiting subrules (1) to (3), the Participant's Business Continuity Plans must identify and address:

(a) the type of Major Events that may impact the Participant's Critical Business Services, Participant Operations and Participant Services; and

(b) activation procedures including trigger conditions for enacting the Participant's Business Continuity Plans; and

(c) the potential impact Major Events may have on the Participant's Critical Business Services, Participant Operations and Participant Services; and

(d) the classification of types of Major Events according to the potential severity of the impacts referred to in paragraph (c); and

(e) escalation procedures that are appropriate to the classification referred to in paragraph (d); and

(f) the actions, arrangements and resources required to achieve the outcomes referred to in subrule (2); and

Note: The actions, arrangements and resources covered by this paragraph would include key operational functions and processes, staff, alternate suppliers/service providers, technology, alternative premises and other physical infrastructure.

(g) specific objectives for the time taken to achieve the outcomes referred to in paragraph (2)(b); and

(h) procedures for communicating during a Major Event with persons that may be impacted by the Major Event, for the purposes of ensuring those persons are adequately informed about:

(i) the nature and impact of the Major Event; and

(ii) the steps that are being taken or will be taken to manage the Major Event; and

(iii) the likely timing of the steps referred to in subparagraph (ii); and

(iv) the likely timing of the resumption of the usual operation of the Participant's Critical Business Services, Participant Operations and Participant Services; and

(i) any operational dependencies between the Participant and any other person that may affect the matters referred to in paragraphs (a) to (h).

(5) Without limiting paragraph (4)(i), a Participant must have in place adequate arrangements to ensure that the Participant is able to carry out its Business Continuity Plans with respect to any Critical Business Services the subject of an Outsourcing Arrangement.

Notification of a Major Event

(6) Without limiting paragraph (4)(h), a Participant must notify ASIC immediately upon becoming aware of a Major Event.

(7) If a notification is made under subrule (6), the Participant must within seven days of the notification provide ASIC with a written report detailing:

(a) the circumstances of the Major Event; and

(b) the steps taken to manage the Major Event.

Review, update and testing of plans

(8) A Participant must:

(a) review and test its Business Continuity Plans and the arrangements referred to in subrule (5):

(i) at a frequency and in a manner appropriate to the nature, scale and complexity of the Participant's Critical Business Services, Participant Operations and Participant Services and to the Participant's structure and location; and

(ii) at a minimum:

(A) each time there is a material change to the Participant's Critical Business Services, Participant Operations and Participant Services or to the Participant's structure and location; and

(B) as soon as practicable after the occurrence of a Major Event; and

(C) once every 12 months; and

(b) update the Business Continuity Plans as required to ensure they comply with subrules (1) to (4).

Documentation of plans and testing

(9) A Participant must document:

(a) its Business Continuity Plans; and

(b) the scope and results of all reviews and testing performed in accordance with subrule (8),

and must maintain that documentation for a period of at least seven years from the later of the date it is created or the date it is last amended.

Part 8B.5 Governance

8B.5.1 Responsibility for compliance

(1) A Participant must have appropriate governance arrangements and adequate financial, technological and human resources to comply with its obligation under this Chapter 8B.

(2) Without limiting subrule (1), the arrangements referred to in that subrule must include arrangements for the Participant's Board or senior management to have oversight of the establishment, implementation, maintenance, review, testing and documentation of the Participant's Business Continuity Plans.

Schedule 2—Amendments to the ASIC Market Integrity Rules (Futures Markets) 2017

1 After Chapter 8

Insert:

Chapter 8A: Market operators—Critical Business Services, Information Security and Business Continuity Plans

Part 8A.1 Application and Definitions

8A.1.1 Application of Chapter

This Chapter applies to Market operators.

8A.1.2 Definitions

In this Chapter:

Business Continuity Plans has the meaning given by Rule 8A.5.1.

Critical Business Services, in relation to a Market operator, means functions, infrastructure, processes or systems which in the event of failure to operate effectively, would or would be likely to cause significant disruption to the Market operator's Market Operations or materially impact the Market operator's Market Services.

> Note: Critical Business Services referred to in this definition would generally include but are not limited to, functions, infrastructure, processes and systems that deliver or support order entry, routing and matching, trade execution, dissemination of market data, trading risk management, market surveillance, reporting of executed trades to a clearing and settlement facility and regulatory data reporting.

Critical Business Services Arrangements has the meaning given by Rule 8A.3.1.

Incident has the meaning given by subparagraph 8A.5.1(6)(a)(i).

Information Asset means information and information technology, including software, hardware and data (both soft and hard copy).

Major Event has the meaning given by Rule 8A.5.1.

Market Operations, in relation to a Market operator, means the operations, activities and conduct of the Market operator's Market or of the Market operator in connection with that Market.

Market Services, in relation to a Market operator, means the services, data and associated products provided by the Market operator in connection with the Market operator's Market.

Outsourcing Arrangement means an arrangement between a Market operator and another person (***Service Provider***) under which the Service Provider will provide, operate or support one or more of the Market operator's Critical Business Services.

Service Provider: has the meaning given in the definition of ***Outsourcing Arrangement***.

Part 8A.2 Trading controls

8A.2.1 Market operator to have trading controls

A Market operator must have controls, including automated controls, that enable immediate suspension, limitation or prohibition of the entry by a Market Participant of Trading Messages where required for the purposes of ensuring the Market is fair, orderly and transparent.

Part 8A.3 Critical Business Services

8A.3.1 Resilience, reliability, integrity and security

Adequate arrangements

(1) A Market operator must have adequate arrangements (***Critical Business Services Arrangements***) to ensure the resilience, reliability, integrity and security of its Critical Business Services.

> Note: Arrangements referred to in subrule (1) would generally include, but are not limited to, policies, procedures and organisational resources including financial, human and technological resources.

(2) Without limiting subrule (1), a Market operator's Critical Business Services Arrangements must include arrangements for:

(a) identifying Critical Business Services; and

(b) identifying, assessing, managing and monitoring for any risks to the resilience, reliability, integrity and security of Critical Business Services; and

(c) ensuring Critical Business Services have sufficient and scalable capacity for ongoing and planned Market Operations and Market Services; and

(d) preventing unauthorised access to or use of Critical Business Services; and

(e) managing the implementation of new Critical Business Services and of changes to existing Critical Business Services in accordance with Rule 8A.3.2; and

(f) dealing with a Major Event in accordance with Part 8A.5 of these Rules; and

(g) managing Outsourcing Arrangements in relation to Critical Business Services in accordance with Rule 8A.3.3.

Review and change of arrangements

(3) A Market operator must undertake a review of its Critical Business Services Arrangements:

(a) following each material change to its Critical Business Services; and

(b) at least once every 12 months,

and apply recommended changes to the Critical Business Services Arrangements arising from the review to ensure they comply with subrules (1) and (2).

Documentation of arrangements

(4) A Market operator must document:

(a) its Critical Business Services Arrangements; and

(b) the scope and results of each review performed in accordance with subrule (3); and

(c) any changes applied to the Critical Business Services Arrangements as a result of the review or otherwise,

and must maintain that documentation for a period of at least seven years from the later of the date it is created or the date it is last amended.

8A.3.2 Change management for Critical Business Services

(1) A Market operator must have adequate arrangements to ensure that its Critical Business Services Arrangements continue to comply with subrule 8A.3.1(1) following the implementation of a new Critical Business Service or of a change to an existing Critical Business Service.

(2) Without limiting subrule (1), the arrangements referred to in that subrule must include arrangements for:

(a) testing new Critical Business Services or material changes to existing Critical Business Services before implementation; and

(b) communicating with persons that may be materially impacted by the implementation for the purposes of ensuring those persons are adequately informed about the nature, timing and impact of the implementation a reasonable time before it occurs; and

(c) ensuring, to the extent reasonably practicable, that persons that may be materially impacted by the implementation are adequately prepared for the implementation before it occurs.

Note: Persons that may be materially impacted by the implementation may include ASIC, Market Participants, other Market operators and the operators of licensed clearing and settlement facilities.

(3) Without limiting paragraph (2)(b), a Market operator must give written notice of the proposed implementation to ASIC a reasonable time before the implementation.

8A.3.3 Outsourcing of Critical Business Services

(1) A Market operator that enters into an Outsourcing Arrangement must:

(a) before entering into the Outsourcing Arrangement, conduct due diligence enquiries for the purposes of ensuring the Service Provider has the ability and capacity to provide the services covered by the Outsourcing Arrangement effectively; and

(b) ensure that the Outsourcing Arrangement is contained in a documented legally binding agreement between the Market operator and the Service Provider that:

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

(ii) requires the Service Provider to give written notice to the Market operator before the Service Provider:

(A) enters into any arrangement with another person (***Sub-Contractor***) under which the Sub-Contractor will provide services material to the provision by the Service Provider of the services covered by the Outsourcing Arrangement; and

(B) makes any other material change to the manner in which the services covered by the Outsourcing Arrangement are provided; and

(iii) deals with the circumstances and manner in which the Outsourcing Arrangement may be terminated; and

(iv) provides for the orderly transfer of services provided under the Outsourcing Arrangement to the Market operator or another Service Provider in the event of termination of the Outsourcing Arrangement; and

(c) while the Outsourcing Arrangement is in place, monitor the performance of the Service Provider for the purposes of ensuring the Service Provider is providing the services covered by the Outsourcing Arrangement effectively and has the ability and capacity to continue to provide those services effectively; and

(d) have in place adequate arrangements to:

(i) identify any conflicts of interest between the Market operator and the Service Provider, including conflicts involving Sub-Contractors and related entities of the Market operator, Service Provider and any Sub-Contractor; and

(ii) manage any conflicts of interest which have been identified or could arise; and

(e) have in place adequate arrangements to ensure the Market operator is able to comply with its obligations under the Act and these Rules in relation to the Critical Business Services the subject of an Outsourcing Arrangement including, without limitation, arrangements with the Service Provider to:

(i) ensure the resilience, reliability, integrity and security of those Critical Business Services in accordance with Rule 8A.3.1; and

(ii) ensure the confidentiality, integrity and availability of information obtained, held or used by the Market operator in relation to those Critical Business Services in accordance with Part 8A.4 of these Rules; and

(iii) deal with a Major Event in accordance with Part 8A.5 of these Rules; and

Note: Such arrangements may include, without limitation, requirements on the Service Provider to:

(a) protect technology from security breaches and cyber-incidents; and
(b) protect proprietary and client-related information and software; and
(c) protect confidential, market-sensitive and personal information from intentional or inadvertent disclosure to unauthorised individuals; and
(d) establish, implement and maintain emergency procedures and a plan for disaster recovery with periodic testing of backup facilities.

(f) ensure that the Market operator and its auditors are able to promptly, upon request, access books, records and other information of the Service Provider relating to the Critical Business Services; and

(g) ensure that ASIC has the same access to all books, records and other information relating to the Critical Business Services and maintained by the Service Provider, that ASIC would have if not for the Outsourcing Arrangement; and

(h) ensure that for each Outsourcing Arrangement, the Market operator's Board or a director or senior manager have confirmed that they have complied with the Market operator's obligations in this subrule and made a written attestation to that effect.

(2) The Market operator must comply with subrule (1) in a manner that is appropriate to:

(a) the nature, complexity and risks of the Outsourcing Arrangement; and

(b) the materiality of the Outsourcing Arrangement to the Market operator's Market Operations and Market Services.

(3) In determining for the purposes of subrule (1) whether the Service Provider has the ability and capacity to provide the services covered by the Outsourcing Arrangement effectively, the Market operator must take into account the extent to which the Service Provider is providing the same or similar services to other Market operators and Market Participants.

(4) A Market operator must give written notice to ASIC as soon as practicable after the Market operator enters into an Outsourcing Arrangement, and in any event no later than 20 business days after entering into the Outsourcing Arrangement.

Part 8A.4 Information security

8A.4.1 Information security

(1) A Market operator must have adequate arrangements to ensure the confidentiality, integrity and availability of information obtained, held or used by the Market operator in relation to its Market Operations and Market Services.

(2) Without limiting subrule (1), the arrangements referred to in that subrule must include:

(a) arrangements to identify and document Information Assets that are integral to the provision of the Market operator's Market Operations and Market Services; and

(b) controls, including automated controls, designed to prevent unauthorised access to Information Assets; and

(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.

(3) A Market operator must have adequate arrangements to ensure the availability of access to data obtained, held or used by the Market operator in its Market Operations and Market Services.

(4) Without limiting subrule (3), the arrangements referred to in that subrule must include arrangements designed to provide for the backup of the data and the timely recovery of the data in the event of any theft, corruption or loss of the data.

(5) A Market operator must notify ASIC in writing, as soon as possible and, in any case, no later than 72 hours, after becoming aware 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.

Part 8A.5 Business Continuity Plans

8A.5.1 Business continuity

Business Continuity Plans

(1) A Market operator must establish, implement and maintain plans (***Business Continuity Plans***) for effectively responding to an event (***Major Event***) that would or would be likely to cause significant disruption to the Market operator's Market Operations or materially impact the Market operator's Market Services.

> Note: A Major Event may include the failure of or disruption to a Critical Business Service, including one operated by a Service Provider, or an event such as a pandemic or influenza event, natural disaster, cyber-attack or power failure.

(2) A Market operator's Business Continuity Plans must be designed to enable:

(a) continuity of the usual operation of the Market operator's Critical Business Services, Market Operations and Market Services during a Major Event; and

(b) to the extent continuation of the usual operation of the Market operator's Critical Business Services, Market Operations and Market Services during a Major Event is not possible, timely and orderly restoration of those usual operations following the Major Event.

(3) A Market operator's Business Continuity Plans must be appropriate to the nature, scale and complexity of the Market operator's Critical Business Services, Market Operations and Market Services and to the Market operator's structure and location.

(4) Without limiting subrules (1) to (3), the Market operator's Business Continuity Plans must identify and address:

(a) the types of Major Events that may impact the Market operator's Critical Business Services, Market Operations and Market Services; and

(b) activation procedures including trigger conditions for enacting the Market operator's Business Continuity Plans; and

(c) the potential impact Major Events may have on the Market operator's Critical Business Services, Market Operations and Market Services; and

(d) the classification of types of Major Events according to the potential severity of the impacts referred to in paragraph (c); and

(e) escalation procedures that are appropriate to the classification referred to in paragraph (d); and

(f) the actions, arrangements and resources required to achieve the outcomes referred to in subrule (2); and

> Note: The actions, arrangements and resources covered by this paragraph would include key operational functions and processes, staff, alternate suppliers/service providers, technology, alternative premises and other physical infrastructure.

(g) specific objectives for the time taken to achieve the outcomes referred to in paragraph (2)(b); and

(h) procedures for communicating during a Major Event with persons that may be impacted by the Major Event, for the purposes of ensuring those persons are adequately informed about:

(i) the nature and impact of the Major Event; and

(ii) the steps that are being taken or will be taken to manage the Major Event; and

(iii) the likely timing of the steps referred to in subparagraph (ii); and

(iv) the likely timing of the resumption of the usual operation of the Market operator's Critical Business Services, Market Operations and Market Services; and

(i) any operational dependencies between the Market operator and any other person that may affect the matters referred to in paragraphs (a) to (h).

(5) Without limiting paragraph (4)(i), a Market operator must have in place adequate arrangements to ensure that the Market operator is able to carry out its Business Continuity Plans with respect to any Critical Business Services the subject of an Outsourcing Arrangement.

Notification of an Incident or Major Event

(6) Without limiting paragraph (4)(h), a Market operator must:

(a) notify ASIC immediately upon becoming aware of:

(i) an unexpected disruption to the usual operation of the Market operator's Critical Business Services that may interfere with the fair, orderly or transparent operation of any Market (***Incident***); or

(ii) a Major Event; and

(b) notify other Market operators, operators of Clearing Facilities and Market Participants that may be impacted by an Incident or a Major Event, as soon as practicable after becoming aware of the Incident or Major Event.

(7) If a notification is made under subrule (6), the Market operator must within seven days of the notification provide ASIC with a written report detailing:

(a) the circumstances of the Incident or Major Event; and

(b) the steps taken to manage the Incident or Major Event.

Review, update and testing of plans

(8) A Market operator must:

(a) review and test its Business Continuity Plans and the arrangements referred to in subrule (5):

(i) at a frequency and in a manner appropriate to the nature, scale and complexity of the Market operator's Critical Business Services, Market Operations and Market Services and to the Market operator's structure and location; and

(ii) at a minimum:

(A) each time there is a material change to the Market operator's Critical Business Services, Market Operations and Market Services or to the Market operator's structure and location; and

(B) as soon as practicable after the occurrence of a Major Event; and

(C) once every 12 months; and

(b) update the Business Continuity Plans as required to ensure they comply with subrules (1) to (4).

Documentation of plans and testing

(9) A Market operator must document:

(a) its Business Continuity Plans; and

(b) the scope and results of all reviews and testing performed in accordance with subrule (8),

and must maintain that documentation for a period of at least seven years from the later of the date it is created or the date it is last amended.

Part 8A.6 Governance

8A.6.1 Responsibility for compliance

(1) A Market operator must have appropriate governance arrangements and adequate financial, technological and human resources to comply with its obligations under this Chapter 8A.

(2) Without limiting subrule (1), the arrangements referred to in that subrule must include arrangements for the Market operator's Board or senior management to have oversight of the establishment, implementation, maintenance, review, testing and documentation of the Market operator's Business Continuity Plans.

Chapter 8B: Market Participants—Critical Business Services, Information Security and Business Continuity Plans

Part 8B.1 Application and Definitions

8B.1.1 Application of Chapter

This Chapter applies to Market Participants.

8B.1.2 Definitions

In this Chapter:

Business Continuity Plans has the meaning given by Rule 8B.4.1.

Critical Business Services, in relation to a Market Participant, means functions, infrastructure, processes or systems which in the event of failure to operate effectively, would or would be likely to cause significant disruption to the Market Participant's Participant Operations or materially impact the Market Participant's Participant Services.

> Note: Critical Business Services referred to in this definition would generally include but are not limited to, functions, infrastructure, processes and systems that deliver or support order acceptance, routing and entry, clearing and settlement of transactions, payments and deliveries of financial products and funds, accounting for or reconciling client money, trust accounts, securities and funds, confirmations and regulatory data reporting.

Critical Business Services Arrangements has the meaning given by Rule 8B.2.1.

Information Asset means information and information technology, including software, hardware and data (both soft and hard copy).

Major Event has the meaning given by Rule 8B.4.1.

Outsourcing Arrangement means an arrangement between a Market Participant and another person (***Service Provider***) under which the Service Provider will provide, operate or support one or more of the Market Participant's Critical Business Services.

Participant Operations, in relation to a Market Participant, means the operations, activities or conduct of the Market Participant in connection with each Market of which it is a Participant.

Participant Services, in relation to a Market Participant, means the services provided by the Market Participant in connection with each Market of which it is a Participant.

Service Provider: has the meaning given in the definition of ***Outsourcing Arrangement***.

Part 8B.2 Critical Business Services

8B.2.1 Resilience, reliability, integrity and security

Adequate arrangements

(1) A Market Participant must have adequate arrangements (***Critical Business Services Arrangements***) to ensure the resilience, reliability, integrity and security of its Critical Business Services.

> Note: Arrangements referred to in subrule (1) would generally include, but are not limited to, policies, procedures and organisational resources including financial, human and technological resources.

(2) Without limiting subrule (1), a Market Participant's Critical Business Services Arrangements must include arrangements for:

(a) identifying Critical Business Services; and

(b) identifying, assessing, managing and monitoring for any risks to the resilience, reliability, integrity and security of Critical Business Services; and

(c) ensuring Critical Business Services have sufficient and scalable capacity for the Market Participant's ongoing and planned Participant Operations and Participant Services; and

(d) preventing unauthorised access to or use of Critical Business Services; and

(e) managing the implementation of new Critical Business Services and of changes to existing Critical Business Services in accordance with Rule 8B.2.2; and

(f) dealing with a Major Event in accordance with Part 8B.4 of these Rules; and

(g) managing Outsourcing Arrangements in relation to Critical Business Services in accordance with Rule 8B.2.3.

Review and change of arrangements

(3) A Market Participant must undertake a review of its Critical Business Services Arrangements:

(a) following each material change to its Critical Business Services; and

(b) at least once every 12 months,

and apply recommended changes to the Critical Business Services Arrangements arising from the review to ensure they comply with subrules (1) and (2).

Documentation of arrangements

(4) A Market Participant must document:

(a) its Critical Business Services Arrangements; and

(b) the scope and results of each review performed in accordance with subrule (3); and

(c) any changes applied to the Critical Business Services Arrangements as result of a review or otherwise,

and must maintain that documentation for a period of at least seven years from the later of the date it is created or the date it is last amended.

8B.2.2 Change management for Critical Business Services

(1) A Market Participant must have adequate arrangements to ensure that its Critical Business Services Arrangements continue to comply with subrule 8B.2.1(1) following the implementation of a new Critical Business Service or of a change to an existing Critical Business Service.

(2) Without limiting subrule (1), the arrangements referred to in that subrule must include arrangements for:

(a) testing new Critical Business Services or material changes to existing Critical Business Services before implementation; and

(b) communicating with persons that may be materially impacted by the implementation for the purposes of ensuring those persons are adequately informed about the nature, timing and impact of the implementation a reasonable time before it occurs; and

(c) ensuring, to the extent reasonably practicable, that persons that may be materially impacted by the implementation are adequately prepared for the implementation before it occurs.

Note: Persons that may be materially impacted by the implementation may include ASIC, other Market Participants, Market operators and the operators of licensed clearing and settlement facilities.

8B.2.3 Outsourcing of Critical Business Services

(1) A Market Participant that enters into an Outsourcing Arrangement must:

(a) before entering into the Outsourcing Arrangement, conduct due diligence enquiries for the purposes of ensuring the Service Provider has the ability and

capacity to provide the services covered by the Outsourcing Arrangement effectively; and

(b) ensure that the Outsourcing Arrangement is contained in a documented legally binding agreement between the Market Participant and the Service Provider, that:

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

(ii) requires the Service Provider to give written notice to the Market Participant before the Service Provider:

(A) enters into any arrangement with another person (***Sub-Contractor***) under which the Sub-Contractor will provide services material to the provision by the Service Provider of the services covered by the Outsourcing Arrangement; or

(B) makes any other material change to the manner in which the services covered by the Outsourcing Arrangements are provided; and

(iii) deals with the circumstances and manner in which the Outsourcing Arrangement may be terminated; and

(iv) provides for the orderly transfer of services provided under the Outsourcing Arrangement to the Market Participant or another Service Provider in the event of termination of the Outsourcing Arrangement; and

(c) while the Outsourcing Arrangement is in place, monitor the performance of the Service Provider for the purposes of ensuring the Service Provider is providing the services covered by the Outsourcing Arrangement effectively and has the ability and capacity to continue to provide those services effectively; and

(d) have in place adequate arrangements to:

(i) identify any conflicts of interest between the Market Participant and the Service Provider, including conflicts involving Sub-Contractors and related entities of the Market Participant, Service Provider and any Sub-Contractor; and

(ii) manage any conflicts of interest which have been identified or could arise; and

(e) have in place adequate arrangements to ensure the Market Participant is able to comply with its obligations under the Act and these Rules in relation to the Critical Business Services the subject of an Outsourcing Arrangement including, without limitation, arrangements with the Service Provider to:

(i) ensure the resilience, reliability, integrity and security of those Critical Business Services in accordance with Rule 8B.2.1; and

(ii) ensure the confidentiality, integrity and availability of information obtained, held or used by the Market Participant in relation to those Critical Business Services in accordance with Part 8B.3 of these Rules; and

(iii) deal with a Major Event in accordance with Part 8B.4 of these Rules; and

Note: Such arrangements may include, without limitation, requirements on the Service Provider to:

(a) protect technology from security breaches and cyber-incidents; and
(b) protect proprietary and client-related information and software; and
(c) protect confidential, market-sensitive and personal information from intentional or inadvertent disclosure to unauthorised individuals; and
(d) establish, implement and maintain emergency procedures and a plan for disaster recovery with periodic testing of backup facilities.

(f) ensure that the Market Participant and its auditors are able to promptly, upon request, access books, records and other information of the Service Provider relating to the Critical Business Services; and

(g) ensure that ASIC has the same access to all books, records and other information relating to the Critical Business Services and maintained by the Service Provider, that ASIC would have if not for the Outsourcing Arrangement; and

(h) ensure that for each Outsourcing Arrangement, the Market Participant's Board or a director or senior manager have confirmed that they have complied with the Market Participant's obligations in this subrule and made a written attestation to that effect.

(2) The Market Participant must comply with subrule (1) in a manner that is appropriate to:

(a) the nature, complexity and risks of the Outsourcing Arrangement; and

(b) the materiality of the Outsourcing Arrangement to the Market Participant's Participant Operations and Participant Services.

(3) In determining for the purposes of subrule (1) whether the Service Provider has the ability and capacity to provide the services covered by the Outsourcing Arrangement effectively, the Market Participant must take into account the extent to which the Service Provider is providing the same or similar services to other Market Participants.

Part 8B.3 Information security

8B.3.1 Information security

(1) A Market Participant must have adequate arrangements to ensure the confidentiality, integrity and availability of information obtained, held or used by the Market Participant in relation to its Participant Operations and Participant Services.

(2) Without limiting subrule (1), the arrangements referred to in that subrule must include:

(a) arrangements to identify and document Information Assets that are integral to the provision of the Market Participant's Participant Operations and Participant Services; and

(b) controls, including automated controls, designed to prevent unauthorised access to Information Assets; and

(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.

(3) A Market Participant must have adequate arrangements to ensure the availability of access to data obtained, held or used by the Market Participant in its Participant Operations and Participant Services.

(4) Without limiting subrule (3), the arrangements referred to in that subrule must include arrangements designed to provide for the backup of the data and the timely recovery of the data in the event of any theft, corruption or loss of the data.

(5) 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.

Part 8B.4 Business Continuity Plans

8B.4.1 Business continuity

Business Continuity Plans

(1) A Market Participant must establish, implement and maintain plans (***Business Continuity Plans***) for effectively responding to an event (***Major Event***) that would or would be likely to cause significant disruption to the Market Participant's Participant Operations or materially impact the Market Participant's Participant Services.

Note: A Major Event may include the failure of a Critical Business Service, including one operated by a Service Provider, or an event such as a pandemic or influenza event, natural disaster, cyber-attack or power failure.

(2) A Market Participant's Business Continuity Plans must be designed to enable:

(a) continuity of the usual operation of the Market Participant's Critical Business Services, Participant Operations and Participant Services during a Major Event; and

(b) to the extent continuation of the usual operation of the Market Participant's Critical Business Services, Participant Operations and Participant Services during a Major Event is not possible, timely and orderly restoration of those usual operations following the Major Event.

(3) A Market Participant's Business Continuity Plans must be appropriate to the nature, scale and complexity of the Market Participant's Critical Business Services, Participant Operations and Participant Services and to the Market Participant's structure and location.

(4) Without limiting subrules (1) to (3), the Market Participant's Business Continuity Plans must identify and address:

(a) the type of Major Events that may impact the Market Participant's Critical Business Services, Participant Operations and Participant Services; and

(b) activation procedures including trigger conditions for enacting the Market Participant's Business Continuity Plans; and

(c) the potential impact Major Events may have on the Market Participant's Critical Business Services, Participant Operations and Participant Services; and

(d) the classification of types of Major Events according to the potential severity of the impacts referred to in paragraph (c); and

(e) escalation procedures that are appropriate to the classification referred to in paragraph (d); and

(f) the actions, arrangements and resources required to achieve the outcomes referred to in subrule (2); and

Note: The actions, arrangements and resources covered by this paragraph would include key operational functions and processes, staff, alternate suppliers/service providers, technology, alternative premises and other physical infrastructure.

(g) specific objectives for the time taken to achieve the outcomes referred to in paragraph (2)(b); and

(h) procedures for communicating during a Major Event with persons that may be impacted by the Major Event, for the purposes of ensuring those persons are adequately informed about:

(i) the nature and impact of the Major Event; and

(ii) the steps that are being taken or will be taken to manage the Major Event; and

(iii) the likely timing of the steps referred to in subparagraph (ii); and

(iv) the likely timing of the resumption of the usual operation of the Market Participant's Critical Business Services, Participant Operations and Participant Services; and

(i) any operational dependencies between the Market Participant and any other person that may affect the matters referred to in paragraphs (a) to (h).

(5) Without limiting paragraph (4)(i), a Market Participant must have in place adequate arrangements to ensure that the Market Participant is able to carry out its Business Continuity Plans with respect to any Critical Business Services the subject of an Outsourcing Arrangement.

Notification of a Major Event

(6) Without limiting paragraph (4)(h), a Market Participant must notify ASIC immediately upon becoming aware of a Major Event.

(7) If a notification is made under subrule (6), the Market Participant must within seven days of the notification provide ASIC with a written report detailing:

(a) the circumstances of the Major Event; and

(b) the steps taken to manage the Major Event.

Review, update and testing of plans

(8) A Market Participant must:

(a) review and test its Business Continuity Plans and the arrangements referred to in subrule (5):

(i) at a frequency and in a manner appropriate to the nature, scale and complexity of the Market Participant's Critical Business Services,

Participant Operations and Participant Services and to the Market Participant's structure and location; and

(ii) at a minimum:

(A) each time there is a material change to the Market Participant's Critical Business Services, Participant Operations and Participant Services or to the Market Participant's structure and location; and

(B) as soon as practicable after the occurrence of a Major Event; and

(C) once every 12 months; and

(b) update the Business Continuity Plans as required to ensure they comply with subrules (1) to (4).

Documentation of plans and testing

(9) A Market Participant must document:

(a) its Business Continuity Plans; and

(b) the scope and results of all reviews and testing performed in accordance with subrule (8),

and must maintain that documentation for a period of at least seven years from the later of the date it is created or the date it is last amended.

Part 8B.5 Governance

8B.5.1 Responsibility for compliance

(1) A Market Participant must have appropriate governance arrangements and adequate financial, technological and human resources to comply with its obligation under this Chapter 8B.

(2) Without limiting subrule (1), the arrangements referred to in that subrule must include arrangements for the Market Participant's Board or senior management to have oversight of the establishment, implementation, maintenance, review, testing and documentation of the Market Participant's Business Continuity Plans.