Proposed amendments to the ASIC Market Integrity Rules (Securities Markets) 2017 and ASIC Market Integrity Rules (Futures Markets) 2017

(Chapters 8A, 8B)

June 2019

These draft rules reflect the proposals in Consultation Paper 314 *Market integrity rules for technological and operational resilience* (CP 314).

If made, they would comprise amendments to the existing *ASIC Market Integrity Rules (Securities Markets) 2017* by:

- the insertion of new Chapters 8A and 8B after existing Chapter 8; and
- the repeal of existing Rule 9.1.3.

Similarly, the amendments would also be made to the existing *ASIC Market Integrity Rules (Futures Markets) 2017.*

The existing rules are available on the Federal Register of Legislation.

Contents

Chapter 8A: Market operators—Critical Systems and Business Continuity Plans

Part 8A.1 Application and definitions

8A.1.1 Application of Chapter

This Chapter, as inserted into the *ASIC Market Integrity Rules (Securities Markets) 2017* and the *ASIC Market Integrity Rules (Futures Markets) 2017*, will apply to each operator of a financial market to which those Rules apply.

8A.1.2 Definitions

In this Chapter:

Business Continuity Plan has the meaning given by Rule 8A.4.1.

Critical System, 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 Systems 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 Systems Arrangements has the meaning given by Rule 8A.3.1.

Incident has the meaning given by Rule 8A.4.1.

Incident Management Plan has the meaning given by Rule 8A.4.1.

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

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

Operator means each operator referred to in Rule 8A.1.1.

Outsourcing Arrangement means an arrangement between an Operator and another person under which the other person will provide, operate or support one or more of the Operator's Critical Systems.

Service Provider means a person that provides, operates or supports one or more of an Operator's Critical Systems under an Outsourcing Arrangement.

Part 8A.2 Fair access and trading controls

8A.2.1 Operator to provide fair access

Where a person in this jurisdiction seeks access to a Market or Market Services, the Operator must make available such access to the person:

(a) on reasonable commercial terms; and

(b) on a non-discriminatory basis.

8A.2.2 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 is fair, orderly and transparent.

Part 8A.3 Critical Systems

8A.3.1 Resilience, reliability, integrity and security

Adequate arrangements

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

> 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 (e.g. system controls).

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

(a) identifying Critical Systems; and

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

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

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

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

(f) dealing with an Incident or Major Event affecting Critical Systems in accordance with Part 8A.4 of these Rules; and

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

Review and change of arrangements

(3) An Operator must review its Critical Systems Arrangements:

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

(b) at least once every 12 months,

and change the Critical Systems Arrangements as required to ensure they comply with subrules (1) and (2).

Documentation of arrangements

(4) An Operator must document:

(a) its Critical Systems Arrangements; and

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

(c) any changes to the Critical Systems 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 Systems

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

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

(a) testing new Critical Systems or change to existing Critical Systems 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 of the Market, 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 Systems

(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 covered by a legally binding written contract 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 obtain the Operator's approval 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;

(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;

(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;

(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 potential conflicts of interest which have been identified or could arise;

(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 Systems 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 Systems in accordance with Rule 8A.3.1; and

(ii) ensure the confidentiality, integrity, security and availability of access to data stored in those Critical Systems in accordance with Rule 8A.3.4; and

(iii) deal with an Incident or Major Event affecting those Critical Systems in accordance with Part 8A.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 confidential, market-sensitive and personal information from intentional or inadvertent disclosure to unauthorised individuals; and
(c) establish 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 Systems; and

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

(h) ensure that for each Outsourcing Arrangement, the Operator's Board and senior management 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 a reasonable time before the Operator enters into an Outsourcing Arrangement.

8A.3.4 Risk management—Data and cyber risk

(1) An Operator must have adequate arrangements to ensure the confidentiality, integrity and security of data 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) controls, including automated controls, designed to prevent unauthorised access to the data; and

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

(c) arrangements designed to prevent the theft, loss or corruption of data.

(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 practicable on becoming aware of any:

(a) unauthorised access to or use of its Critical Systems that impacts the effective functioning of those systems; or

(b) unauthorised access to or use of market-sensitive, confidential or personal data.

Part 8A.4 Incident management and Business Continuity Plans

8A.4.1 Incident management and business continuity

Incident Management Plan and Business Continuity Plan

(1) An Operator must establish, maintain and implement:

(a) plans (***Incident Management Plans***) for dealing with an unexpected interruption to the usual operation of the Operator's Critical Systems (***Incident***); and

(b) plans (***Business Continuity Plans***) for dealing with an emergency or other event (***Major Event***) that causes significant disruption to the Operator's Market Operations or materially impacts the Operator's Market Services.

Note 1: A Major Event may include the failure of a Critical System, including one operated by a Service Provider, or an event such as a natural disaster, cyber-attack, power failure or major disruption to public transport. An Incident may, depending on its severity, constitute a Major Event.

Note 2: An Operator's Incident Management Plan and Business Continuity Plan may be separate or integrated plans.

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

(a) to the extent possible, continuation of the usual operation of Critical Systems, Market Operations and Market Services during an Incident or Major Event; and

(b) to the extent continuation of the usual operation of Critical Systems, Market Operations and Market Services during an Incident or Major Event is not possible, timely and orderly restoration of those usual operations following the Incident or Major Event.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Notification of Incident

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

(a) notify ASIC immediately upon becoming aware of:

(i) an Incident that may interfere with the fair, orderly or transparent operation of any Market; or

(ii) a Major Event; and

(b) notify other Operators, operators of Clearing Facilities and Participants that may be impacted by an Incident referred to in subparagraph (a)(i) or by 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.

It is proposed that Rule 9.1.3 of the ASIC Market Integrity Rules (Securities Markets) 2017, which requires Operators to notify of system outages, will be repealed.

Review, update and testing of plans

(8) An Operator must:

(a) review and test its Incident Management Plans, 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 Systems, 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 Systems, Market Operations and Market Services or to the Operator's structure and location; and

(B) in the case of the Business Continuity Plans, once every three months; and

(b) update the Incident Management Plans and 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 Incident Management Plans and 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.5 Governance

8A.5.1 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 and senior management to have oversight of the establishment, maintenance, implementation, review, testing and documentation of the Operator's Incident Management Plans and Business Continuity Plans.

Chapter 8B: Market Participants—Critical Systems and Business Continuity Plans

Part 8B.1 Application and definitions

8B.1.1 Application of Chapter

This Chapter, as inserted into the *ASIC Market Integrity Rules (Securities Markets) 2017* and the *ASIC Market Integrity Rules (Futures Markets) 2017*, will apply to each participant of a financial market to which those Rules apply.

8B.1.2 Definitions

In this Chapter:

Business Continuity Plan has the meaning given by Rule 8B.3.1.

Critical System, 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 1: Critical Systems 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 Systems Arrangements has the meaning given by Rule 8B.2.1.

Incident has the meaning given by Rule 8B.3.1.

Incident Management Plan has the meaning given by Rule 8B.3.1.

Major Event has the meaning given by Rule 8B.3.1.

Outsourcing Arrangement means an arrangement between a Participant and another person under which the other person will provide, operate or support one or more of the Participant's Critical Systems.

Participant means each Participant referred to in Rule 8B.1.1.

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

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

Service Provider means a person that provides, operates or supports one or more of a Participant's Critical Systems under an Outsourcing Arrangement.

Part 8B.2 Critical Systems

8B.2.1 Resilience, reliability, integrity and security

Adequate arrangements

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

> 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 (e.g. system controls).

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

(a) identifying Critical Systems; and

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

(c) ensuring Critical Systems 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 Systems; and

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

(f) dealing with an Incident or Major Event affecting Critical Systems in accordance with Part 8B.3 of these Rules; and

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

Review and change of arrangements

(3) A Participant must review its Critical Systems Arrangements:

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

(b) at least once every 12 months,

and change the Critical Systems Arrangements as required to ensure they comply with subrules (1) and (2).

Documentation of arrangements

(4) A Participant must document:

(a) its Critical Systems Arrangements; and

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

(c) any change to the Critical Systems 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 Systems

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

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

(a) testing new Critical Systems or changes to existing Critical Systems 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 of the Market, Market Operators and the operators of licensed clearing and settlement facilities.

8B.2.3 Outsourcing of Critical Systems

(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 covered by a legally binding written contract 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 obtain the Participant's approval 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 potential 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 Systems 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 Systems in accordance with Rule 8B.2.1; and

(ii) ensure the confidentiality, integrity, security and availability of access to data stored in those Critical Systems in accordance with Rule 8B.2.5; and

(iii) deal with an Incident or Major Event affecting those Critical Systems in accordance with Part 8B.3 of these Rules;

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 confidential, market-sensitive and personal information from intentional or inadvertent disclosure to unauthorised individuals; and
(c) establish 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 Systems; and

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

(h) ensure that for each Outsourcing Arrangement, the Participant's Board and senior management 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 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.

8B.2.4 Risk management—Data and cyber risk

(1) A Participant must have adequate arrangements to ensure the confidentiality, integrity and security of data 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) controls, including automated controls, designed to prevent unauthorised access to the data; and

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

(c) arrangements designed to prevent the theft, loss or corruption of data.

(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 Systems that impacts the effective functioning of those systems; or

(b) unauthorised access to or use of market-sensitive, confidential or personal data.

Part 8B.3 Incident management and Business Continuity Plans

8B.3.1 Incident management and business continuity

Incident Management Plan and Business Continuity Plan

(1) A Participant must establish, maintain and implement:

(a) plans (***Incident Management Plans***) for dealing with an unexpected interruption to the usual operation of the Participant's Critical Systems (***Incident***); and

(b) plans (***Business Continuity Plans***) for dealing with an emergency or other event (***Major Event***) that causes significant disruption to the Participant's Participant Operations or materially impacts the Participant's Participant Services.

Note 1: A Major Event may include the failure of a Critical System, including one operated by a Service Provider, or an event such as a natural disaster, cyber-attack, power failure or major disruption to public transport. An Incident may, depending on its severity, constitute a Major Event.

Note 2: An Operator's Incident Management Plan and Business Continuity Plan may be separate or integrated plans.

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

(a) to the extent possible, continuation of the usual operation of Critical Systems, Participant Operations and Participant Services during an Incident or Major Event; and

(b) to the extent continuation of the usual operation of Critical Systems, Participant Operations and Participant Services during an Incident or Major Event is not possible, timely and orderly restoration of those usual operations following the Incident or Major Event.

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

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

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

(b) the potential impact Incidents and Major Events may have on the Participant's Critical Systems, Participant Operations and Participant Services;

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

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

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

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

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

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

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

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

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

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

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

Notification of Incident

(6) Without limiting paragraph (4)(g), 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 Incident Management Plans, 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 Systems, 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 Critical Systems, Participant Operations and Participant Services or to the Participant's structure and location; and

(B) in the case of the Business Continuity Plans, once every 12 months; and

(b) update the Incident Management Plans and 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 Incident Management Plans and 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.4 Governance

8B.4.1 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 and senior management to have oversight of the establishment, maintenance, implementation, review, testing and documentation of the Participant's Incident Management Plans and Business Continuity Plans.