BUSINESS CONTINUITY AND DISASTER RECOVERY

The purpose of this Guidance Note	• To assist participants to understand the disaster recovery and business continuity arrangements they should have in place to meet their obligations under the ASX Clear Operating Rules
The main points it covers	• The key requirements that a participant's disaster recovery and business continuity arrangements should meet in order to be considered "adequate" for the purposes of the ASX Clear Operating Rules • How those requirements differ for "tier 1" and "tier 2" participants • The requirement for a participant to have a nominated business continuity officer responsible for disaster recovery and business continuity • The requirement for a participant to have an up to date infrastructure diagram of its current architecture • The requirement for a participant to maintain proper records of its key clearing and settlement systems and infrastructure • The connectivity requirements for a participant connecting to the clearing and settlement facilities • The requirement for a participant to notify ASX of any disruption that causes the participant to engage its BCP and also of any significant outage
Related materials you should read	• Guidance Note 1 *Admission as a Participant* • Guidance Note 3 *Changes in Participation* • Guidance Note 8 *Notification Obligations* • Guidance Note 9 *Offshoring and Outsourcing*

History: Guidance Note 10 amended 08/03/22. Previous versions of this Guidance Note were issued in 07/14, 06/15, 08/19, 12/19 and 10/20.

Table of contents

1. Introduction

This Guidance Note is published by ASX Clear Pty Limited ("ASX") to assist participants in ASX Clear to understand the disaster recovery and business continuity arrangements they should have in place to meet their obligations under the ASX Clear Operating Rules. Participants should also refer to the guidance in Guidance Note 1 about the organisational and technical resources it should have in place to prevent a disruption, including but not limited to active monitoring and reporting tools.

Under those rules, a participant is required at all times to maintain adequate disaster recovery and business continuity arrangements, having regard to the nature and extent of its operations, to ensure the timely recovery of its usual operations.[1]

It is noted that a participant who is no longer able to transmit clearing messages is entitled under the ASX Clear Operating Rules to request ASX to provide emergency assistance and, in particular, to request ASX to act as its agent to send and receive clearing messages on its behalf.[2] ASX, however, is only obliged to provide such assistance on a "reasonable endeavours" basis. The fact that ASX may provide this emergency assistance facility does not derogate from or mitigate the obligation of a participant to have adequate disaster recovery and business continuity arrangements for the timely recovery of its usual operations and participants should not consider this facility to be a part of those arrangements.

2. Participant tiering

ASX acknowledges that a "one size fits all" approach to business continuity and disaster recovery arrangements is neither practicable nor appropriate.

1 ASX Clear Operating Rules 4.1.1(g) and 4.2.1.

2 ASX Clear Operating Rule 6.9.1 and ASX Clear Operating Rules Procedure 6.9.

ASX therefore classifies its participants as "tier 1" and "tier 2" participants for the purposes of assessing the adequacy of their business continuity and disaster recovery arrangements. Higher standards apply to tier 1 participants than to tier 2 participants.

A **tier 1 participant** is a participant that:

- clears or expects to clear more than $10,000,000,000 of equities transactions per annum through the ASX Clear facility;
- clears or expects to clear more than 500,000 lots of ETOs per annum through the ASX Clear facility;
- acts as the clearer for 4 or more trading participants (including itself, if it is a trading participant, and any related bodies corporate that are also trading participants); or
- is advised by ASX that it is a tier 1 participant for the purposes of this Guidance Note.[3]

A **tier 2 participant** is any participant that is not a tier 1 participant.

Participants should review and assess their tier classification from time to time, particularly following any change in the nature or scale of their ASX Clear operations, to determine whether they need to upgrade their business continuity and disaster recovery arrangements in light of that change.

3. Terms used in this Guidance Note

The following terms used in this Guidance Note have the meanings assigned below:

allocation matrix – a document setting out which core personnel are to relocate to an alternate site or to work from home in the event of a disruption affecting a primary site.

alternate site – the site or sites at which a participant's ASX Clear operations will be carried out in the event of a disruption affecting a primary site. An alternate site may be occupied and operated by the participant or it may be a facility provided by a third party service provider. It may also be a shared facility.

ASX Clear operations – the systems, technology, staff, premises, equipment, business processes and other resources used by a participant in conducting its business as an ASX Clear participant. This includes, but is not limited to, payment arrangements with the participant's bank, risk management systems, client records, accounting records, and systems for reconciling client account information with the participant's accounting records.

business continuity arrangements – arrangements put in place to enable a participant to recover, resume and restore its ASX Clear operations, including processing of time-critical transactions, in the midst of, or following, an actual or potential disruption.

business continuity plan or **BCP** – a documented collection of plans and procedures setting out a participant's business continuity arrangements.

business impact analysis – an analysis of the effect that different types of disruption might have upon a participant's ASX Clear operations.

change management – processes for managing change to technology or other infrastructure to minimise unanticipated disruptions.

communications network – the telecommunication links between the participant and ASX, between the participant's different sites (including its primary and alternate sites), and between the participant and any party to whom it outsources any of its ASX Clear operations.

[3] In assessing whether a participant should be classified as a "tier 1 participant", ASX may have regard to the Reserve Bank of Australia's requirements and recommendations in the Financial Stability Standards for Financial Market Infrastructures. It may also have regard to the amount and type of clearing and settlement business conducted by related bodies corporate of the participant with ASX.

core personnel – the minimum set of staff with appropriate skills and experience required for a participant to recover and resume its ASX Clear operations in the event of a disruption.

critical ASX Clear operations – that part of a participant's ASX Clear operations that must be functioning to enable a participant to meet or support time critical obligations under the ASX Clear Operating Rules and, if the participant is also a participant of ASX Settlement, under the ASX Settlement Operating Rules, including settlement of transactions, movements of security holdings, collection and payment of margins, maintenance of proper client records and accounting records, and risk management.

cyber attack – an attempted or actual incident that either:

- uses computer technology or networks to commit or facilitate the commission of traditional crimes, such as fraud and forgery (for example, identity or data theft); or
- is directed at computers and computer systems or other information communication technologies (for example, hacking or denial of services).[4]

cyber resilience – the ability to prepare for, detect, respond to and recover from a cyber-attack.[5]

disaster recovery arrangements – a subset of a participant's business continuity arrangements relating to the recovery and resumption of technology systems following a natural or man-made disaster affecting those systems.

distributed denial of service or **DDoS** – activities that are designed to disrupt or degrade an organisation's online services such as their website, email and DNS services.[6]

disruption – an interruption to normal ASX Clear operations.

downtime – the period that a disruption lasts.

geographically remote – where a primary site and alternate site are in different locations with suitably different risk profiles.

incident management plan – a documented plan of action for use at the time of a disruption that typically covers the core personnel, resources, services and actions needed (including decision-making and communication processes) to deal with the disruption.

nominated business continuity officer – the meaning given in section 4.1.

outsourced – where a participant has part of its ASX Clear operations performed by someone else (including a related body corporate).

primary site – the site or sites at which business-as-usual processing for ASX Clear operations occurs.

recovery time objective or **RTO** – the target time within which ASX Clear operations are to be resumed following a disruption.

related body corporate – the same meaning as section 50 of the Corporations Act 2001 (Cth).

remote access – the ability for a staff member at a participant to log on to the systems used for the participant's ASX Clear operations and perform all necessary functions from a site other than the participant's primary or alternate sites (eg at the staff member's home).

---

4 As defined in ASIC Report 429: *Cyber resilience: Health check*, March 2015, available online at: http://download.asic.gov.au/media/3062900/rep429-published-19-march-2015-1.pdf.

5 *Ibid*.

6 As defined in the ASD publication: *Preparing for and Responding to Denial-of-Service Attacks*, available online at: https://www.cyber.gov.au/acsc/view-all-content/publications/preparing-and-responding-denial-service-attacks. DDoS activities are often directed to extracting a payment from the victim but they can also be used simply to cause disruption or to mask or distract attention away from other nefarious activities.

shared facility – a facility accommodating technology or people employed in a participant's ASX Clear operations which is shared with another business unit of the participant, a related body corporate or a third party.

significant outage – a disruption where a participant is unable or unlikely to meet the recovery time objective stated in its business continuity plan.

4. Key requirements

4.1. Nominated business continuity officer and core personnel

All participants must allocate overall responsibility for disaster recovery and business continuity to a nominated officer[7] ("nominated business continuity officer") who:

- is a senior member of the participant's management team with the appropriate delegated authority and the requisite qualifications, skills and experience to understand and validate the design and performance of the participant's disaster recovery and business continuity arrangements; and
- is responsible for overseeing the preparation, review, updating and approval of the participant's disaster recovery and business continuity arrangements and ensuring they meet ASX's requirements under the rules and this Guidance Note.

The nominated business continuity officer should:

- identify the core personnel needed to manage, recover and resume the participant's ASX Clear operations following a disruption and ensure they have the facilities they need to do so within the recovery time objective stated in their BCP.[8] This may involve them having an allocated work space at an alternate site which is configured and ready for their use and/or remote access;
- ensure that those core personnel have clearly defined roles and responsibilities under the BCP and participate in BCP fire drills to prepare them to perform those roles and responsibilities in the event of a disruption;
- keep an up-to-date allocation matrix indicating which core personnel are to relocate to an alternate site or to work from home in the event of a disruption affecting a primary site; and
- ensure that all relevant personnel receive awareness training on what to do in the event of a disruption.

The nominated business continuity officer may act as ASX's primary point of contact for discussions related to the participant's disaster recovery and business continuity arrangements and any disruptions that may occur, or may appoint another person with the requisite knowledge and skills (a "primary business continuity contact") to perform that role.

A participant should notify ASX within 10 business days of the appointment and any subsequent departure of its nominated business continuity officer and any other primary business continuity contact.

4.2. Infrastructure diagrams

All participants must have an up to date high level infrastructure diagram which represents the current state of the technology and communications infrastructure used to conduct its ASX Clear operations. The diagram must identify the location of all primary and alternate sites that house the participant's key technology components and personnel involved in its ASX Clear operations and the communication links (including the communication provider and details of primary and redundant links) between each of those sites.

---

7 The nominated business continuity officer may be from a related body corporate, including from overseas. However, in all cases, the nominated business continuity officer must understand the participant's business operations, as well as its obligations under the ASX Clear Operating Rules and Guidance Notes.

8 Again, the recovery time objective stated in the participant's BCP should conform to key requirement 4.6.

Where a participant's infrastructure is housed across multiple primary and/or alternate sites, the diagrams must clearly identify which elements of the ASX Clear operations are housed at or connected to each relevant site.

If the participant intends to make material changes to its technology or communications infrastructure[9] it should also prepare an infrastructure diagram which shows the planned future state.

The infrastructure diagrams for current state arrangements and, where applicable, future state arrangements, must be provided to ASX upon request.

4.3. Systems and technology records

All participants must have and maintain proper records of their key clearing and settlement systems and technology, including but not limited to records showing:

- hardware, software and infrastructure used to conduct its ASX Clear operations;
- asset ownership and location; and
- support and maintenance arrangements, including an indication of whether the arrangements are outsourced or offshored.

The records and supporting documentation must be provided to ASX upon request.

4.4. Replacement policy

All participants must have a clearly defined system and technology replacement policy which includes a process to identify when assets are nearing their end of life.

4.5. Business continuity plan

All participants should conduct a business impact analysis covering a full range of potential disruption scenarios to their ASX Clear operations and establish a business continuity plan (BCP) which seeks to ensure that their ASX Clear operations can be recovered and resumed following a disruption within the recovery time objective stated in their BCP.[10]

A participant's BCP, and any changes to it from time to time, should be signed off by the nominated business continuity officer and approved by the appropriate senior management body.[11]

A participant's BCP, at a minimum, should address the following disruption scenarios:

Loss of access / loss of site:

- a primary site outage with same-day recovery (eg because of a need to evacuate a building following a bomb threat or fire alarm);
- a sustained primary site outage (eg because of serious damage to a building);
- a loss of the primary electricity supply to, or key utilities such as gas and water at, a primary site for an extended period;
- where its operations are split across multiple primary sites, a loss of one site or of connectivity between sites;

[9] Participants who make material changes to their technology or communications should also be cognisant of their obligation to notify ASX of those changes pursuant to ASX Clear Operating Rule 4.7.1(d)(iii).

[10] Again, the recovery time objective stated in the participant's BCP should conform to key requirement 4.6.

[11] The appropriate body to approve a participant's BCP will vary, depending on the significance of the participant's ASX Clear operations compared to its other operations and its governance structure. If the participant's ASX Clear operations and related activities comprise its main business activity, it would generally be appropriate for the BCP to be approved by its board or a committee of the board.

- a major disruption to public transport or related infrastructure (such as the closure of a major road or bridge) affecting a primary site;

Loss of systems / technology:

- an internal system outage;
- the network of its primary telecommunication provider not being available for an extended period;
- if a participant has outsourced any of its ASX Clear operations to a third party, a system outage at, or a communication failure with, the third party;

Loss of staff / pandemic:

- a pandemic affecting the participant's staff or the staff of a party to whom it has outsourced some of its ASX Clear operations; and

Cyber:

- an attempted or actual cyber attack on data or technology which impacts the participant's ability to conduct its ASX Clear operations, including those elements outsourced or offshored.[12]

The participant should ensure its BCP is securely stored in locations known to, and that can be readily accessed by, all core personnel in the event of a disruption. If stored electronically, the participant should also ensure that hard copies are available in case access to the electronic version is not available during a disruption.

Copies of the BCP and related documentation should also be stored centrally to facilitate regular review, revision and approval.

4.6. Recovery time objective

In all cases, a tier 1 participant's BCP should specify an RTO following the initiation of its BCP of:

- a target of 2 hours (and no more than 4 hours) for critical ASX Clear operations; and
- no more than 4 hours for resumption of business-as-usual ASX Clear operations.

A tier 2 participant's BCP should specify an RTO following the initiation of its BCP of:

- a target of 4 hours (and no more than 6 hours) for critical ASX Clear operations; and
- no more than 6 hours for resumption of business-as-usual ASX Clear operations.

Participants which record different RTOs for systems and personnel should ensure that they both meet the required RTO in this Guidance Note.

ASX acknowledges that in some cyber-related incidents there may be exceptions to these RTOs, for example, where moving to an alternate site may risk propagating the cyber incident further into the network. However, in these cases, participants should design their BCP to enable safe resumption and completion of critical ASX Clear operations as close to the applicable RTO as possible.

Participants should aim to make a decision on whether or not to initiate their BCP as quickly as they reasonably can following a disruption so that it does not significantly extend the time during which their ASX Clear operations are down.

[12] Further guidance on offshoring and outsourcing arrangements can be found in ASX Clear Operating Rules Guidance Note 9 *Offshoring and Outsourcing*.

4.7. System resilience

All participants should comply with the following requirements:

- Technology should be configured and plans and processes should be in place so that, in the event of a disruption at a primary site, ASX Clear operations can be recovered and resumed at an alternate site with minimal downtime and within the recovery time objective stated in the participant's BCP.[13]
- A participant should have sufficient technology in place at its primary and alternate sites so that ASX Clear operations can occur at each location, independently of the other.
- The alternate site should be able to handle business-as-usual transaction volumes for a typical business day as well as any additional volumes associated with accumulation and queuing of transactions during a disruption.
- Technology housed at primary and alternate sites should be secure and adequately protected from fire, flood and water damage, and access should be controlled with appropriate security devices.
- Primary and alternate sites should each have an uninterruptible power supply and generator back-up to ensure a reasonable period of continuous supply of electricity in the event of an interruption to the primary electricity supply.
- Primary and alternate sites should use separate hardware and separate communication lines in order to avoid a single point of failure.
- Primary and alternate sites should be on common software versions and appropriate system and software documentation should be available at both sites.
- The participant should have access to a suitable test environment at primary or alternate sites for critical ASX Clear operations that is readily available to promptly reproduce disruptions to technology and to find resolutions to them.
- The participant should have error-message logs available at primary and alternate sites to facilitate prompt identification of the cause of disruptions to key systems or processes.
- A participant operating its data centres in an 'active-active' configuration should have access to appropriate monitoring tools to promptly identify replication issues, delays and backlogs in processing of transactions and raise alerts to ensure timely remediation.
- If an alternate site is a shared facility, the participant should ensure there are appropriate arrangements in place to preserve the confidentiality of client information.
- Where a participant's infrastructure is housed across multiple primary and/or alternate sites, the participant must maintain its system resilience across each site to ensure that it can continue its normal levels of business as a participant in the event of a disruption to one or more sites or a loss of connectivity.
- All participants should consider whether their communications network should have, at a minimum, dual communication lines into their working premises that are separated from one another in order to avoid a single point of failure. This also enhances cyber resilience in the event of a DDoS or other cyber attack. For internet-based services it is recommended, where practicable, that participants consider utilising two internet service providers to address these concerns.
- All participants should regularly review, at least once annually, how their systems and infrastructure can be designed to improve cyber resilience. ASX expects all participants to have chosen and aligned their

[13] Again, the recovery time objective stated in the participant's BCP should conform to key requirement 4.6.

arrangements to one or more of the latest global or national cyber standards and guidance.[14] The arrangements should be implemented at all primary and alternate sites to ensure maximum security across all sites and to facilitate continuity of their ASX Clear operations in the event of disruption, including a cyber attack.

ASX may, from time to time, determine specific technical requirements for participants to maintain adequate security and technical arrangements within the clearing and settlement facilities.

For tier 1 participants, an alternate site should also be geographically remote from any primary site. Any alternate site should be a safe distance from any primary site to mitigate any reasonably foreseeable event likely to impact the availability of all sites simultaneously. It is important for participants to consider any local factors that may impact the safe distance. For example, if a primary site is located in a local flood zone, the participant should locate any alternate site outside the flood zone.

4.8. Connectivity requirements

ASX imposes the following technical requirements for a participant to connect to the ASX Clear facility:

- connections must be in the name of the participant or a related body corporate;
- connections must be used exclusively for activities as a participant in ASX markets and facilities; and
- clearing gateways with direct connectivity to the facility must be located within Australia.

The requirements do not preclude a participant from entering into arrangements with third parties to co-locate their infrastructure within a shared data centre. However, a participant that uses a shared data centre must ensure themselves, and provide evidence to ASX, that there are no common[15] or single points of failure within the data centre.

4.9. Data recovery

All participants should configure their technology and have plans and processes in place so that in the event of a disruption at a primary site there is minimal loss of data relevant to their ASX Clear operations. This includes:

- maintaining and storing for an appropriate period a back-up of end-of-day production data away from the primary site;
- taking and storing for an appropriate period a start-of-day snapshot of production data;
- having the ability to identify the status of all clearing messages (and, if the participant is also a participant of ASX Settlement, any settlement messages) at the time of the disruption; and
- having the ability to identify any outstanding clearing transactions (and, if the participant is also a participant of ASX Settlement, any outstanding settlement transactions) at the time of recovery of their ASX Clear operations.

A tier 1 participant, and all participants operating their data centres in 'active–active' mode running real-time replication across multiple sites, should take and store for an appropriate period multiple intraday snapshots of production data.

4.10. Incident management plan

All participants should develop, maintain and practise a clearly defined and documented incident management plan which can be applied to each disruption scenario developed in accordance with key requirement 4.5. The incident

[14] For example, the National Institute of Standards and Technology Cybersecurity Framework (available at https://www.nist.gov/topics/cybersecurity) and the Australian Signals Directorate strategies to mitigate cyber security incidents (available at https://www.asd.gov.au/infosec/mitigationstrategies.htm).

[15] That is, infrastructure used by multiple users of the data centre.

management plan should clearly state roles, responsibilities and escalation arrangements for each disruption scenario. Management delegations and lines of succession should also be specified.

The incident management plan should include a communications plan which can be applied to each disruption scenario detailing what should be communicated, when it should be communicated and to whom, including staff, clients, ASX, ASIC and other regulators. It should also include an up-to-date contact list for key parties.

The incident management plan should be reviewed and tested at least annually to ensure that it remains current and adequate. It should be available in hard copy as well as electronically, and accessible at a participant's primary and alternate sites.

4.11. Incident management records

All participants must maintain proper records of disruptions impacting their ASX Clear operations including, but not limited to:

- the date and time the incident commenced, when it was identified and by whom;
- the date and time relevant stakeholders were contacted, including vendors, ASIC and ASX;
- where applicable, the date and time a decision was made to initiate the participant's BCP;
- the impact the incident had on its ASX Clear operations;
- a summary of how the incident was resolved;
- the date and time normal operations re-commenced;
- the date and time any backlog in processing ASX Clear transactions was completed;
- a summary of the root cause analysis and any corrective actions taken;
- where the disruption to its ASX Clear operations was material, a comprehensive post-incident review report; and
- a copy of any incident reports received from vendors and service providers.

This information and supporting documentation must be provided to ASX upon request.

4.12. BCP testing

A participant must test its disaster recovery and business continuity arrangements:

- at least once annually;
- as soon as practicable following any material change to its business,[16] or its disaster recovery and business continuity arrangements;[17] and
- as otherwise notified by ASX.[18]

At a minimum, the BCP testing should confirm:

- successful fail-over of technology from a primary site to an alternate site;

[16] This includes any material changes to software, hardware, communication lines, service providers, offshored or outsourced arrangements or technical support arrangements.

[17] ASX Clear Operating Rules Procedure 4.2.1.

[18] ASX Clear Operating Rule 4.2.1.

- successful fail-over of the communications network to an alternate site, ensuring connectivity is maintained to other participant sites, ASX, payment providers and any party to whom it outsources any of its ASX Clear operations;
- successful validation of connectivity, data and applications at alternate sites;
- the ability of users to access and log in to technology and applications at alternate sites, including the use of remote access where applicable;
- the ability of users to complete business-as-usual processes at alternate sites;
- the recovery solution provides sufficient capacity to handle business-as-usual transaction volumes for a typical business day as well as any additional volumes associated with accumulation and queuing of transactions during a disruption; and
- successful restoration of the production environment.

Participants should record and analyse the outcomes of all testing conducted in accordance with this key requirement, and specifically whether the stated RTO was met when tested. The final test outcomes, including any enhancements to the test plan, should be signed off by the nominated business continuity officer and reported to the appropriate senior management body.[19]

Participants that conduct a full fail-over to an alternate site following a disruption to their ASX Clear operations can treat that as a test of their business continuity arrangements, provided the fail-over is successful and confirms the matters mentioned above.

4.13. Outsourced or offshored operations

Under the ASX Clear Operating Rules, a participant is responsible for all actions and omissions of persons involved in its business as a participant.[20] This applies regardless of where the business activities are conducted and by whom. A participant is also required to have adequate resources and processes, including management supervision processes, to comply with its obligations as a participant under the ASX Clear Operating Rules.[21] This applies to all of a participant's activities, including any that it may have outsourced or offshored.[22] Hence a participant must have appropriate resources and processes to:

- develop its BCP with due consideration to the dependencies on, and recovery of, any processes, systems or infrastructure managed by third parties performing outsourced or offshored activities;
- ensure its service level agreement with any third party performing outsourced or offshored activities includes a requirement for the third party to have and maintain business continuity arrangements that are appropriate and complementary to the participant's business continuity arrangements, and that they are sufficient to enable the participant to meet the recovery time objective stated in the participant's BCP;[23] and
- supervise any outsourced or offshored activities to ensure they comply with the participant's obligations under the ASX Clear Operating Rules and this Guidance Note.

All infrastructure changes undertaken by a third party performing outsourced or offshored activities should be tracked and approved by the participant. Such changes should also be independently assessed by the participant to determine whether any updates to its BCP arrangements are required.

---

19 See note 11 above.

20 ASX Clear Operating Rule 4.17.1. This specifically includes, without limitation, its officers, employees, agents, representatives, consultants or advisers and those of any related bodies corporate who are involved in its activities as an ASX Clear participant.

21 ASX Clear Operating Rule 3.5.1. For these purposes, "resources" include financial, technological and human resources and "processes" include management supervision, training, compliance, risk management, business continuity and disaster recovery processes.

22 See ASX Clear Guidance Note 9 *Offshoring and Outsourcing*.

23 Again, the recovery time objective stated in the participant's BCP should conform to key requirement 4.6.

4.14. Change management

To avoid a business continuity event being triggered, all participants should have and comply with change management policies and procedures that are designed and function effectively to ensure that changes to its ASX Clear operations are thoroughly assessed, tested and authorised, and that appropriate disaster recovery and roll-back arrangements are in place, before changes are implemented.

All participants should establish a framework which ensures that they are made aware of all material and relevant system and infrastructure changes initiated by vendors or service providers that may impact their ASX Clear operations and that these too are subject to appropriate change management policies and procedures, are thoroughly assessed, tested and authorised, and that appropriate disaster recovery and roll-back arrangements are in place, before the changes are implemented.

Participants should not rely on vendors or service providers alone to conduct testing of system changes that may impact their ASX Clear operations. Participants must make their own independent assessment of the changes and the quality and extent of testing conducted by the vendor or service provider.

4.15. Notification requirements

All participants must include in their BCP a requirement to notify ASX of:

- any disruption that causes the participant to engage its BCP for its ASX Clear operations, as soon as reasonably practicable after it becomes aware of the disruption; and
- any significant outage impacting its ASX Clear operations, as soon as it becomes apparent that there is or is likely to be a significant outage and regardless of whether it has engaged its BCP.

The above notifications should be made to the relevant departments within ASX either via phone call or email.[24]

All participants must also notify ASX of the following matters via ASX Online:

- immediately of any significant breach of, or non-compliance with, the disaster recovery and business continuity requirements in the ASX Clear Operating Rules or Procedures (as interpreted in accordance with this Guidance Note),[25] using the 'Self Reporting including Significant Breach' form; and
- as soon as practicable after it has become aware of any fact or matter or intends to take any action that will or may affect its capacity to communicate reliably with CHESS or the Derivatives Clearing System, including (without limitation) any change to its interface with CHESS or the Derivatives Clearing System,[26] using the 'Capacity to Communicate with ASX' form.

Participants must notify ASX by email to review.team@asx.com.au within 10 business days of the appointment and any subsequent departure of their nominated business continuity officer and any other primary business continuity contact.

4.16. Independent review

Participants should consider having their disaster recovery and business continuity arrangements reviewed periodically by their compliance function, internal or external auditor, or another party independent of the business unit primarily responsible for overseeing the preparation, review, updating and approval of those arrangements.

[24] The relevant ASX department may change depending on the nature of the disruption or outage. Participants should maintain an up to date list of key ASX contacts for this purpose.

[25] ASX Clear Operating Rule 19.1A.1(a).

[26] ASX Clear Operating Rule 4.7.1(f) and ASX Clear Operating Rules Procedure 4.7.1.