Consultation on Guidance Note changes for ASX Clear, ASX Settlement, ASX Clear (Futures) and Austraclear participants

Proposed changes to Guidance Note 1 *Admission as a Participant*, and Guidance Note 10 *Business Continuity and Disaster Recovery* relating to business continuity and cyber resilience

8 March 2019

Invitation to comment

ASX is seeking submissions on the proposed guidance note amendments accompanying this paper.

Submissions are due by **Friday 3 May 2019** and should be sent by email to:
participants.compliance@asx.com.au
or by mail to:
ASX Limited
PO Box H224
Australia Square NSW 1215
Attention: Lyn Allsop-Guest

ASX would prefer to receive submissions in electronic form.

If you would like your submission, or any part of it, to be treated as confidential, please indicate this clearly. All submissions will be provided to regulators on request. Submissions may also be published on the ASX website, unless they are clearly marked as confidential or ASX considers that there are reasons not to do so.

Contacts

For general enquiries, please contact:

Lyn Allsop-Guest
Manager, Compliance Review and Investigations
E participants.compliance@asx.com.au

Contents

Introduction

This Consultation Paper seeks stakeholder input on ASX's proposal to update Guidance Notes 1 and 10 to provide contemporary guidance to clearing and settlement participants in relation to their business continuity arrangements and cyber resilience.

The proposed changes to Guidance Note 1 are relevant to participants in ASX Clear, ASX Clear (Futures) and ASX Settlement (other than specialist settlement participants). The proposed changes to Guidance Note 10 are relevant to participants in ASX Clear, ASX Clear (Futures), ASX Settlement (other than specialist settlement participants) and Austraclear (other than collateral manager special purpose participants, foreign currency settlement bank participants and special purpose participants permissioned for cash only transactions).

Amendments to Guidance Note 1

Background

ASX published Guidance Note 1 to assist entities applying to be admitted as a participant of the ASX Clear, ASX Settlement or ASX Clear (Futures)[1] facilities to understand the requirements for admission.

Those Guidance Notes set out ASX's expectations of the resources and processes that an entity applying to be admitted as a participant of these facilities must have in place before ASX will admit it. This includes a risk management framework for identifying and managing or mitigating the risks it will face as a participant.

Since participants are required to comply with the admission requirements on an ongoing basis, ASX expects that all participants will continue to have an acceptable risk management framework in place at all times.

Proposed amendments

ASX proposes to add the highlighted words below to the description of a participant's "key processes" in section 3.5 of Guidance Note 1 for the ASX Clear and ASX Clear (Futures) rulebooks and in section 3.4 of Guidance Note 1 for the ASX Settlement rulebook:[2]

> … [a participant's] "key processes" for these purposes would include:
>
> - …
> - its risk management framework,[3] that is, its general processes for identifying and managing or mitigating the risks it faces, ***including but not limited to market risk, liquidity risk, counterparty risk, operational risk and cyber risk***;[4]…

This minor revision seeks to clarify the types of risk that ASX expects a participant's risk management framework to address and, in particular, to specifically reference cyber risk.

It is ASX's expectation that a participant's existing risk management framework should already be designed to identify, manage and mitigate these types of risks and therefore ASX considers that this revision is unlikely to impose any material compliance burden on participants.

---

[1] There is currently no equivalent Guidance Note for Austraclear participants.
[2] ASX is proposing to make equivalent changes to section 3.5 of Guidance Note 1 for the ASX and ASX 24 rulebooks, but it is not intending to consult on the changes.
[3] This footnote in the amended Guidance Note will provide that applicants should have regard to the guidance given by ASIC about risk management systems in section D and Appendix 1 of ASIC Regulatory Guide 104 *Licensing: Meeting the general obligations*.
[4] This footnote in the amended Guidance Note will provide that applicants should have regard to the guidance given by ASIC about cyber resilience in ASIC Report 429; *Cyber resilience: Health check;* March 2015 available online at http://www.asic.gov.au/media/3062900/rep429-published-19-march-2015-1.pdf. Applicants should also consider the latest global standards on cyber, such as the National Institute of Standards and Technology Cybersecurity Framework (refer https://www.nist.gov/topics/cybersecurity), and any local guidance provided by Australian regulatory bodies and government departments, such as the Australian Signals Directorate (refer https://www.asd.gov.au/).

Effective date for the amendments

ASX proposes to make the changes to Guidance Note 1 in alignment with the changes to Guidance Note 10. This will be 6 months following the date of publication of the revised Guidance Notes.

Amendments to Guidance Note 10

Background

ASX published Guidance Note 10 to assist participants in the ASX Clear, ASX Settlement, ASX Clear (Futures) and Austraclear facilities to understand the minimum disaster recovery and business continuity arrangements they should have in place to meet their obligations under the operating rules. It sets out a number of 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 and ASX Settlement Operating Rules; and
- "appropriate complementary arrangements" for the purposes of the ASX Clear (Futures) Operating Rules and Austraclear Regulations.

ASX proposes to enhance Guidance Note 10 to reflect current regulatory and market expectations.

Proposed amendments

Proper records

ASX proposes to require participants to:

- maintain up to date high level infrastructure diagrams which represent the current state and, where applicable, future state of the technology and communications infrastructure used to conduct their ASX operations;
- maintain proper records of their key clearing and settlement systems and technology (including hardware, software and infrastructure used to conduct its ASX Clear operations, asset ownership and location, and support and maintenance arrangements; and
- have a clearly defined system and technology replacement policy which includes a process to identify when assets are nearing their end of life.

The proposed requirements to maintain high level infrastructure diagrams and proper records will ensure that the participant can, at all times, evidence the infrastructure arrangements it has in place to meet its obligations as a participant and that the records can be provided to ASX on request.

The proposed requirement to have a clearly defined system and technology replacement policy will assist participants to identify and manage ageing clearing and settlement infrastructure.

Incident management records

ASX proposes to require participants to maintain detailed records of disruptions impacting their ASX clearing and settlement operations. The guidance outlines key information that ASX expects to be recorded and provided to ASX upon request.

The proposed requirements will assist the participant to demonstrate to ASX how it has complied with its obligations when managing an incident which has impacted its ASX clearing and settlement operations.

Core personnel

ASX proposes to require participants to allocate overall responsibility for disaster recovery and business continuity to a nominated business continuity officer ("nominated officer"), who is a senior member of the management team familiar with ASX's requirements.

ASX expects that participants would already have identified key personnel with responsibility for business continuity and therefore considers that this requirement should have minimal impact on participants.

Participants will have a 6 months transition period after the publication of Guidance Note 10 to notify ASX of their nominated officer. Thereafter, they will be required to notify ASX of the appointment and any subsequent departure of the nominated officer within 10 business days.

Recovery time objective (RTO)

ASX proposes to clarify the RTO requirements for all participants. Specifically, ASX proposes to amend Guidance Note 10 to require that a participant's business continuity plan (BCP) should specify the relevant RTO following the initiation of its BCP:

- for a tier 1 participant[5], 2 hours for critical ASX clearing and settlement operations and 4 hours for the resumption of business as usual operations; and
- for a tier 2 participant[6], 4 hours for critical ASX clearing and settlement operations and 6 hours for resumption of business as usual operations.

Participants will be expected to carry out a gap analysis as to their ability to meet these RTOs and to develop plans to address any gaps identified within 6 months of the date of publication of the revisions to Guidance Note 10. The plan should outline the necessary steps to meet the relevant RTO within a further 12 months. ASX therefore expects all participants to achieve the relevant RTO within 18 months of the date of publication of the revised 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.

The proposed change to the RTO for critical clearing and settlement systems, which was previously prescribed as 'preferably 2 hours' or 'preferably 4 hours' for tier 1 and tier 2 participants respectively, will provide greater clarity and certainty around ASX's expectations. Achieving the required RTO will also ensure that participants in the ASX clearing and settlement facilities have a higher degree of operational reliability.

System resilience

Given the ever-evolving threat of cyber attacks, ASX believes it is critical for participants to continually review their cyber resilience arrangements. To this end, ASX proposes to enhance the guidance in Guidance Note 10 on system resilience.

ASX believes there are sufficient global and national standards and guidance for participants on cyber resilience and therefore it does not intend to impose prescriptive cyber resilience requirements at this time.

Instead, ASX is proposing to require participants to align their cyber resilience arrangements to one or more of the latest global or national cyber standards and guidance.[7] ASX expects these arrangements to be implemented across all sites to ensure maximum security across sites at which the participant undertakes any part of its business as an ASX participant.

Participants should be prepared to confirm the standards or guidance to which they have aligned their frameworks within the 6 months transition period following publication of the Guidance Note.

---

[5] Refer to existing Guidance Note 10, 'Participant tiering' for guidance on how ASX classifies tier 1 and tier 2 participants.
[6] *Ibid*
[7] Including but not limited to the good practice guidance published by ASIC about cyber resilience (available online at http://www.asic.gov.au/regulatory-resources/digital-transformation/cyber-resilience/), the latest global standards on cyber, such as the National Institute of Standards and Technology Cybersecurity Framework (available at https://www.nist.gov/topics/cybersecurity), and any local guidance provided by Australian regulatory bodies and Government departments, such as the Australian Signals Directorate (refer https://www.asd.gov.au/).

To mitigate the risk of cyber attacks, ASX is proposing that all participants consider whether their communications networks have any single points of failure. ASX is also proposing that participants regularly, and at least once annually, review how their systems and infrastructure can be designed to improve cyber resilience.

Change management

To avoid a disruption to a participant's ASX clearing and settlement operations, ASX is proposing that 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 clearing and settlement operations are thoroughly assessed, tested and authorised, and that appropriate disaster recovery and roll-back arrangements are in place, before changes are implemented.

ASX is also proposing that all participants should establish a framework which ensures that they are made aware of all system and infrastructure changes initiated by vendors or service providers[8] that may impact their ASX clearing and settlement 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. In other words, participants should not rely on vendors or service providers alone to conduct testing of system changes.

Independent review

ASX proposes that 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.

Connectivity requirements

ASX is proposing to expand the guidance in Guidance Note 10 to articulate existing connectivity requirements for participants connecting to the ASX Clear, ASX Settlement and ASX Clear (Futures) facilities.

Other minor enhancements

ASX is proposing a number of other minor enhancements to Guidance Note 10. These are included in the Guidance Notes annexed to this Consultation Paper:

Annexure 1: Changes to ASX Clear Guidance Note 10.
Annexure 2: Changes to ASX Settlement Guidance Note 10.
Annexure 3: Changes to ASX Clear (Futures) Guidance Note 10.
Annexure 4: Changes to Austraclear Guidance Note 10.

Transition period

Subject to consultation feedback, other than in relation to the proposed changes to RTOs, ASX is proposing a 6 month transition period for participants to align their business continuity arrangements with the revised guidance in Guidance Note 10. That period will commence on the date of publication of the revised Guidance Notes.

In the case of the proposed changes to RTOs, as indicated previously, ASX expects participants to carry out a gap analysis within 6 months of the date of publication of the revised Guidance Notes and then to implement a plan to meet the required RTO within a further 12 months.

Issues for consultation

The primary purpose of this consultation is to seek feedback on the proposed updates to Guidance Notes 1 and 10 from participants in the ASX Clear, ASX Settlement, ASX Clear (Futures) and Austraclear facilities.

[8] Participants of ASX Clear, ASX Settlement and ASX Clear (Futures) should also have regard to Guidance Note 9 *Offshoring and Outsourcing.*

ASX is interested to receive comments on:

- whether participants agree with ASX's proposal not to impose prescriptive requirements on how participants should manage cyber risk and instead to require participants to align their cyber resilience arrangements to one or more of the latest global or national cyber standards and guidance;
- whether the proposed transition arrangements mentioned above are sufficient for participants to align their current business continuity arrangements with the updated guidance in Guidance Note 10.

Due date for submissions

Please provide all comments on the draft amendments to Guidance Notes 1 and 10 in writing by the close of business on **Friday 3 May 2019.**

by email to:

participants.compliance@asx.com.au

or by mail to:

ASX Limited
PO Box H224
Australia Square NSW 1215
Attention: Lyn Allsop-Guest

ASX would prefer to receive submissions in electronic form.

If you would like your submission, or any part of it, to be treated as confidential, please indicate this clearly. All submissions will be provided to regulators on request. Submissions may also be published on the ASX website, unless they are clearly marked as confidential or ASX considers that there are reasons not to do so.

Annexures

asx_clear_guidance_note_10 consultation.docx
asx_settlement_guidance_note_10 consultation.docx
asx_clear_futures_guidance_note_10 consultation.docx
austraclear_system_guidance_note_10 consultation.docx

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 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 DD/MM/18. Previous versions of this Guidance Note were issued in 07/14 and 06/15.

Important notice: ASX has published this Guidance Note to assist participants to understand and comply with their obligations under the ASX Clear Operating Rules. It sets out ASX's interpretation of the ASX Clear Operating Rules and how ASX is likely to enforce those rules. Nothing in this Guidance Note necessarily binds ASX in the application of the ASX Clear Operating Rules in a particular case. In issuing this Guidance Note, ASX is not providing legal advice and participants should obtain their own advice from a qualified professional person in respect of their obligations. ASX may withdraw or replace this Guidance Note at any time without further notice to any person.

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 transactions 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.

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.

[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.

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.

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).

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.

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 activities*, October 2014, available online at: https://www.asd.gov.au/publications/protect/preparing-for-responding-to-ddos-activities.htm. 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.

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 officer and core personnel

All participants must allocate overall responsibility for disaster recovery and business continuity to a nominated business continuity officer[7] (nominated 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;
- is responsible for overseeing the preparation, review, updating and approval ofthe participant's disaster recovery and business continuity arrangements and ensuring they meet ASX's requirements under the rules and this Guidance Note; and
- will act as ASX's first point of contact for discussions related to the participant's disaster recovery and business continuity arrangements and any disruptions that may occur.

The nominated 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.

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.

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.

[7] The nominated officer may be from a related body corporate, including from overseas. However, in all cases, the nominated 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.

[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).

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 officer and approved by the appropriate senior management body.[11]

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

- an internal system outage;
- 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;
- 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]
- 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);
- the network of its primary telecommunication provider not being available for an extended period;
- a loss of the primary electricity supply to, or key utilities such as gas and water at, a primary site for an extended period;

[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.

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

- where its operations are split across multiple primary sites, a loss of one site or of connectivity between sites;
- a major disruption to public transport or related infrastructure (such as the closure of a major road or bridge) affecting a primary site; and
- a pandemic affecting the participant's staff or the staff of a party to whom it has outsourced some of its ASX Clear operations.

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 no more than:

- 2 hours for critical ASX Clear operations; and
- 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 no more than:

- 4 hours for critical ASX Clear operations; and
- 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.

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.

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

- 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 and 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 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.

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:

[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).

- connections must be in the name of the participant;
- connections must be used exclusively for the participant's 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 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;

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

- 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;
- 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

[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.

enhancements to the test plan, should be signed off by the nominated 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.

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 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. Participants must make their own independent assessment of the changes and the quality and extent of testing conducted by the vendor or service provider.

---

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.

4.15. 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.

All participants must also notify ASX:

- within 10 business days of the appointment and any subsequent departure of their nominated business continuity officer;[24]
- 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] 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]

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] This notification should be emailed to participants.compliance@asx.com.au.

[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.

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 Settlement 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 Settlement Operating Rules • How those requirements differ for "tier 1" and "tier 2" participants • The requirement for a participant to have a nominated 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 DD/MM/YY. Previous versions of this Guidance Note were issued in 07/14, 06/15 and 10/15.

Important notice: ASX has published this Guidance Note to assist participants to understand and comply with their obligations under the ASX Settlement Operating Rules. It sets out ASX's interpretation of the ASX Settlement Operating Rules and how ASX is likely to enforce those rules. Nothing in this Guidance Note necessarily binds ASX in the application of the ASX Settlement Operating Rules in a particular case. In issuing this Guidance Note, ASX is not providing legal advice and participants should obtain their own advice from a qualified professional person in respect of their obligations. ASX may withdraw or replace this Guidance Note at any time without further notice to any person.

Table of contents

1. Introduction

This Guidance Note is published by ASX Settlement Pty Ltd ("ASX") to assist participants in ASX Settlement to understand the disaster recovery and business continuity arrangements they should have in place to meet their obligations under the ASX Settlement Operating Rules. Participants should also have regard 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]

This Guidance Note does not apply to specialist settlement participants. Guidance on the activities of specialist settlement participants can be found in ASX Settlement Rules Guidance Note 14 *Specialist Settlement Participants.*

2. Participant tiering

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

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.

ASX Settlement participants that are also ASX Clear participants should refer to the guidance provided in ASX Clear Operating Rules Guidance Note 9 to determine their tier.

A **tier 1 participant** is a participant that is a general settlement participant[2] and:

1 ASX Settlement Operating Rules 4.18.1 and 6.21.1.

2 As defined in ASX Settlement Operating Rule 2.13.

- processes or expects to process more than $3,000,000,000 of transactions through the ASX Settlement facility per annum; 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. This includes a product issuer settlement participant using the mFund settlement service and an account 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 Settlement 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 Settlement 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 Settlement operations – the systems, technology, staff, premises, equipment, business processes and other resources used by a participant in conducting its business and performing its obligations under the ASX Settlement Operating Rules.

business continuity arrangements – arrangements put in place to enable a participant to recover, resume and restore its ASX Settlement 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 Settlement 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 Settlement operations.

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

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

cyber attack – an attempted or actual incident that either:

[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.

- 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 Settlement 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.

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

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

recovery time objective or RTO – the target time within which ASX Settlement 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 Settlement 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).

shared facility – a facility accommodating technology or people employed in a participant's ASX Settlement 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 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 activities*, October 2014, available online at: https://www.asd.gov.au/publications/protect/preparing-for-responding-to-ddos-activities.htm. 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.

4. Key requirements

4.1. Nominated officer and core personnel

All participants must allocate overall responsibility for disaster recovery and business continuity to a nominated business continuity officer[7] (nominated 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;
- 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; and
- will act as ASX's first point of contact for discussions related to the participant's disaster recovery and business continuity arrangements and any disruptions that may occur.

The nominated officer should:

- identify the core personnel needed to manage, recover and resume the participant's ASX Settlement 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 even 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.

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 Settlement 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 Settlement operations and the communication links (including the communication provider and details of primary and redundant links) between each of those sites.

Where a participant's infrastructure is housed across multiple primary and/or alternate sites, the diagrams must clearly identify which elements of the ASX Settlement 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.

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

[8] Again, the recovery time objective stated in the participant's BCP should conform to key requirement 4.5.

[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 Settlement Operating Rule 4.6.1d.

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 Settlement 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.

4.3.1. 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.

4.4. Business continuity plan

All participants should conduct a business impact analysis covering a full range of potential disruption scenarios to their ASX Settlement operations and establish a business continuity plan (BCP) which seeks to ensure that their ASX Settlement 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 officer and approved by the appropriate senior management body.[11]

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

- an internal system outage;
- if a participant has outsourced any of its ASX Settlement operations to a third party, a system outage at, or a communication failure with, the third party;
- an attempted or actual cyber attack on data or technology which impacts the participant's ability to conduct its ASX Settlement operations, including those elements outsourced or offshored; [12]
- 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);
- the network of its primary telecommunication provider not being available for an extended period;
- 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;

[10] Again, the recovery time objective stated in the participant's BCP should conform to key requirement 4.5.

[11] The appropriate body to approve a participant's BCP will vary, depending on the significance of the participant's ASX Settlement operations compared to its other operations and its governance structure. If the participant's ASX Settlement 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.

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

- a major disruption to public transport or related infrastructure (such as the closure of a major road or bridge) affecting a primary site; and
- a pandemic affecting the participant's staff or the staff of a party to whom it has outsourced some of its ASX Settlement operations.

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.

4.5. Recovery time objective

In all cases, a tier 1 participant's BCP should specify an RTO following the initiation of its BCP of no more than:

- 2 hours for critical ASX Settlement operations; and
- 4 hours for resumption of business-as-usual ASX Settlement operations.

A tier 2 participant's BCP should specify an RTO following the initiation of its BCP of no more than:

- 4 hours for critical ASX Settlement operations; and
- 6 hours for resumption of business-as-usual ASX Settlement 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 Settlement 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 Settlement operations are down.

4.6. 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 Settlement 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 Settlement 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.

[13] Again, the recovery time objective stated in the participant's BCP should conform to key requirement 4.5.

- 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 and alternate sites for critical ASX Settlement 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 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 Settlement operations in the event of disruption, including a cyber attack.

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.

4.7. Connectivity requirements

ASX Settlement participants that are not also participants of an ASX market or clearing facility must connect to the ASX Settlement facility using a connection that is supported by CHESS. This is determined by ASX on a case by case basis and is assessed by ASX having regard to the size and nature of the participant's ASX Settlement business.

[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).

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.

4.8. 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 Settlement 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 settlement messages at the time of the disruption; and
- having the ability to identify any outstanding settlement transactions at the time of recovery of their ASX Settlement 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.

4.9. 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 4.4. The incident 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.

4.10. Incident management records

All participants must maintain proper records of disruptions impacting their ASX Settlement 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 Settlement 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 Settlement transactions was completed;

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

- a summary of the root cause analysis and any corrective actions taken;
- where the disruption to its ASX Settlement 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.

4.11. BCP testing

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

- at least once annually; and
- 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;
- 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 Settlement 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 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 Settlement operations can treat that as a test of their business continuity arrangements, provided the fail-over is successful and confirms the matters mentioned above.

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

[17] ASX Settlement Operating Rule 6.21.1.

[18] Ibid.

[19] See note 11 above.

4.12. Outsourced or offshored operations

Under the ASX Settlement 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 Settlement 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 Settlement 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.

4.13. 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 Settlement 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 relevant system and infrastructure changes initiated by vendors or service providers that may impact their ASX Settlement 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. Participants must make their own independent assessment of the changes and the quality and extent of testing conducted by the vendor or service provider.

4.14. 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 Settlement operations, promptly after it becomes aware of the disruption; and
- any significant outage impacting its ASX Settlement 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.

---

20 ASX Settlement Operating Rule 6.2.1. 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 Settlement participant.

21 ASX Settlement Operating Rule 4.18.1. 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 Settlement Guidance Note 9 *Offshoring and Outsourcing*.

23 Again, the recovery time objective stated in the participant's BCP should conform to key requirement 4.5.

All participants must also notify ASX:

- within 10 business days of the appointment and any subsequent departure of their nominated business continuity officer;[24]
- immediately of any significant breach of, or non-compliance with, the disaster recovery and business continuity requirements in the ASX Settlement Operating Rules or Procedures (as interpreted in accordance with this Guidance Note);[25] 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, including (without limitation) any change to its interface with CHESS.[26]

4.15. 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] This notification should be emailed to participants.compliance@asx.com.au.

[25] ASX Settlement Operating Rule 12.18.1(j).

[26] ASX Settlement Operating Rule 16.1.1(c).

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 (Futures) 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 "appropriate complementary arrangements" for the purposes of the ASX Clear (Futures) Operating Rules • How those requirements differ for "tier 1" and "tier 2" participants • The requirement for a participant to have a nominated 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 DD/MM/19. Previous versions of this Guidance Note were issued in 07/14, 06/15 and 8/15.

Important notice: ASX has published this Guidance Note to assist participants to understand and comply with their obligations under the ASX Clear (Futures) Operating Rules. It sets out ASX's interpretation of the ASX Clear (Futures) Operating Rules and how ASX is likely to enforce those rules. Nothing in this Guidance Note necessarily binds ASX in the application of the ASX Clear (Futures) Operating Rules in a particular case. In issuing this Guidance Note, ASX is not providing legal advice and participants should obtain their own advice from a qualified professional person in respect of their obligations. ASX may withdraw or replace this Guidance Note at any time without further notice to any person.

Table of contents

1. Introduction

This Guidance Note is published by ASX Clear (Futures) Pty Ltd ("ASX") to assist participants in ASX Clear (Futures) to understand the disaster recovery and business continuity arrangements they should have in place to meet their obligations under the ASX Clear (Futures) 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 appropriate complementary business continuity arrangements to enable it to meet its ongoing obligations as a clearing participant pursuant to the ASX Clear (Futures) Operating Rules.[1]

2. Participant tiering

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

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 500,000 transactions per annum through the ASX Clear (Futures) facility;
- is a guarantor clearing participant; or

[1] ASX Clear (Futures) Operating Rule 4.2.

- is advised by ASX that it is a tier 1 participant for the purposes of this Guidance Note.[2]

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 (Futures) 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 (Futures) 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 (Futures) operations – the systems, technology, staff, premises, equipment, business processes and other resources used by a participant in conducting its business as an ASX Clear (Futures) 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 (Futures) 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 (Futures) 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 (Futures) operations.

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

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).[3]

[2] 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.

[3] 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.

cyber resilience – the ability to prepare for, detect, respond to and recover from a cyber-attack.[4]

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.[5]

disruption – an interruption to normal ASX Clear (Futures) 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.

outsourced – where a participant has part of its ASX Clear (Futures) 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 (Futures) operations occurs.

recovery time objective or **RTO** – the target time within which ASX Clear (Futures) 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 (Futures) 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).

shared facility – a facility accommodating technology or people employed in a participant's ASX Clear (Futures) operations which is shared with another business unit of the participant, a related body corporate, or staff employed by 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 officer and core personnel

All participants must allocate overall responsibility for disaster recovery and business continuity to a nominated business continuity officer[6] (nominated 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

4 *Ibid*.

5 As defined in the ASD publication: *Preparing for and responding to Denial of Service activities*, October 2014, available online at: https://www.asd.gov.au/publications/protect/preparing-for-responding-to-ddos-activities.htm. 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.

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

- 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; and
- will act as ASX's first point of contact for discussions related to the participant's disaster recovery and business continuity arrangements and any disruptions that may occur.

The nominated officer should:

- identify the core personnel needed to manage, recover and resume the participant's ASX Clear (Futures) operations following a disruption and ensure they have the facilities they need to do so within the recovery time objective stated in their BCP.[7] 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.

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 (Futures) 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 (Futures) operations and the communication links (including the communication provider and details of primary and redundant links) between each of those sites.

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 (Futures) operations are housed at or connected to each relevant site.

If the participant intends to make material changes to its technology or communications infrastructure[8] 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 (Futures) 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.

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

[8] 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 (Futures) Operating Rule 4.14(db).

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 (Futures) operations and establish a business continuity plan (BCP) which seeks to ensure that their ASX Clear (Futures) operations can be recovered and resumed following a disruption within the recovery time objective stated in their BCP.[9]

A participant's BCP, and any changes to it from time to time, should be signed off by the nominated officer and approved by the appropriate senior management body.[10]

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

- an internal system outage;
- if a participant has outsourced any of its ASX Clear (Futures) operations to a third party, a system outage at, or a communication failure with, the third party;
- an attempted or actual cyber attack on data or technology which impacts the participant's ability to conduct its ASX Clear (Futures) operations, including those elements outsourced or offshored;[11]
- 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);
- the network of its primary telecommunication provider not being available for an extended period;
- 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;
- a major disruption to public transport or related infrastructure (such as the closure of a major road or bridge) affecting a primary site; and
- a pandemic affecting the participant's staff or the staff of a party to whom it has outsourced some of its ASX Clear (Futures) operations.

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.

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

10 The appropriate body to approve a participant's BCP will vary, depending on the significance of the participant's ASX Clear (Futures) operations compared to its other operations and its governance structure. If the participant's ASX Clear (Futures) 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.

11 Further guidance on offshoring and outsourcing arrangements can be found in ASX Clear (Futures) Operating Rules Guidance Note 9 *Offshoring and Outsourcing*.

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 no more than:

- 2 hours for critical ASX Clear (Futures) operations; and
- 4 hours for resumption of business-as-usual ASX Clear (Futures) operations.

A tier 2 participant's BCP should specify an RTO following the initiation of its BCP of no more than:

- 4 hours for critical ASX Clear (Futures) operations; and
- 6 hours for resumption of business-as-usual ASX Clear (Futures) 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 (Futures) 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 (Futures) operations are down.

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 (Futures) operations can be recovered and resumed at an alternate site with minimal downtime and within the recovery time objective stated in their BCP.[12]
- A participant should have sufficient technology in place at its primary and alternate sites so that ASX Clear (Futures) 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 and alternate sites for critical ASX Clear (Futures) operations that is readily available to promptly reproduce disruptions to technology and to find resolutions to them.

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

- 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 arrangements to one or more of the latest global or national cyber standards and guidance.[13] 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 (Futures) operations in the event of disruption, including a cyber attack.

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 (Futures) facility:

- connections must be in the name of the participant;
- connections must be used exclusively for the participant's 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[14] or single points of failure within the data centre.

[13] 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).

[14] That is, infrastructure used by multiple users of 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 (Futures) 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 open positions at the time of the disruption; and
- having the ability to identify any outstanding clearing house payments for both house and client accounts at the time of recovery of their ASX Clear (Futures) 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 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 (Futures) 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 (Futures) 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 (Futures) transactions was completed;
- a summary of the root cause analysis and any corrective actions taken;
- where the disruption to its ASX Clear (Futures) 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 should test its disaster recovery and business continuity arrangements:

- at least once annually; and
- as soon as practicable following any material change to its business[15], or its disaster recovery and business continuity arrangements; and
- as otherwise notified by ASX.[16]

At a minimum, the BCP testing should confirm:

- successful fail-over of technology from a primary site to an alternate site;
- 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 (Futures) operations;
- successful validation of connectivity, data and applications at the 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 officer and reported to the appropriate senior management body.[17]

Participants that conduct a full fail-over to an alternate site following a disruption to their ASX Clear (Futures) 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 (Futures) Operating Rules, a participant is responsible for all actions and omissions of persons involved in its business as a participant.[18] 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 (Futures) Operating

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

[16] ASX Clear (Futures) Operating Rules 4.2.

[17] See note 10 above.

[18] ASX Clear (Futures) Operating Rule 4.11A. 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.

Rules.[19] This applies to all of a participant's activities, including any that it may have outsourced or offshored.[20] 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 their BCP,[21] 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.

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 (Futures) 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 relevant system and infrastructure changes initiated by vendors or service providers that may impact their ASX Clear (Futures) 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. 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, as soon as reasonably practicable after it becomes aware of the disruption; and
- any significant outage impacting its ASX Clear (Futures) 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.

All participants must also notify ASX:

- within 10 business days of the appointment and any subsequent departure of their nominated business continuity officer;[22]

[19] ASX Clear (Futures) Operating Rule 4.2(e). 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.

[20] See ASX Clear (Futures) Guidance Note 9 *Offshoring and Outsourcing*.

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

[22] This notification should be emailed to participants.compliance@asx.com.au.

- immediately of any significant breach of, or non-compliance with, the disaster recovery and business continuity requirements in the ASX Clear (Futures) Operating Rules or Procedures (as interpreted in accordance with this Guidance Note);[23] 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 the Exchange System.[24]

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.

[23] ASX Clear (Futures) Operating Rule 4.11B.

[24] ASX Clear (Futures) Operating Rule 4.14(o). "Exchange System" is defined in Part 01 of the ASX Clear (Futures) Operating Rules and means any system, including the clearing system, computer system or other electronic system (including the Licensed Software and the Exchange Equipment) utilised by ASX Clear (Futures) or any of its Related Bodies Corporate from time to time in connection with any business of ASX Clear (Futures) or any of its Related Bodies Corporate.

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 Austraclear Regulations
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 "appropriate complementary" arrangements for the purposes of the Austraclear Regulations • How those requirements differ for "tier 1" and "tier 2" participants • The requirement for a participant to have a nominated 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 Austraclear systems and infrastructure • The requirement for a participant to notify Austraclear of any disruption that causes the participant to engage its BCP and also of any significant outage
Related materials you should read	• Nil.

History: Guidance Note 10 amended //DD/MM/19. Previous versions of this Guidance Note were issued in 10/14 and 06/15.

Important notice: ASX has published this Guidance Note to assist participants to understand and comply with their obligations under the Austraclear Regulations. It sets out ASX's interpretation of the Austraclear Regulations and how ASX is likely to enforce those regulations. Nothing in this Guidance Note necessarily binds ASX in the application of the Austraclear Regulations in a particular case. In issuing this Guidance Note, ASX is not providing legal advice and participants should obtain their own advice from a qualified professional person in respect of their obligations. ASX may withdraw or replace this Guidance Note at any time without further notice to any person.

Table of contents

1. Introduction

This Guidance Note is published by Austraclear Limited ("Austraclear") to assist participants in Austraclear to understand the business continuity arrangements they should have in place to meet their obligations under the Austraclear Regulations.

Under those regulations, all participants are required to maintain, in a form satisfactory to Austraclear, operational capacity and appropriate complementary business continuity arrangements to enable them to meet their ongoing obligations in a timely manner.[1]

It is noted that a participant is entitled under the Austraclear Regulations to request Austraclear to enter valid instructions permitted under the regulations in to the Austraclear System on its behalf.[2] Austraclear, however, is only obliged to provide such assistance on a "reasonable endeavours" basis. The fact that the Austraclear Regulations permit Austraclear to enter dealings for which it has received valid instruction 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 provision to be a part of those arrangements.

This Guidance Note does not apply to special purpose participants including:

- collateral managers;[3]
- approved foreign currency settlement banks;[4] and
- special purpose participants permissioned only for cash transactions.

[1] Austraclear Regulations 2.4(b)(i) and (iii). If a participant ceases to satisfy the eligibility requirements set out in Regulation 2.4, its status as a participant may be suspended (Austraclear Regulation 3.10(a)(ii)).

[2] Austraclear Regulation 6.2 and Austraclear Procedures Determinations and Practice Note 6.2.

[3] These participants must comply with the detailed business continuity requirements outlined in the relevant Regulations specific to their participant status - Austraclear Regulation 28.15 (Collateral Manager).

[4] These participants must comply with the detailed business continuity requirements outlined in the relevant Regulations specific to their participant status - Austraclear Regulation 29.3 (Foreign Currency Settlement Bank).

2. Participant tiering

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

Austraclear therefore classifies its participants as "tier 1" and "tier 2" participants for the purposes of assessing the appropriateness 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 Participating Bank;
- a Full Participant; or
- a participant that:
    - executes on average over the course of a year more than 100 transactions per day through Austraclear (including transactions executed as a proxy for others);
    - has more than A$1 billion in holdings in Austraclear (including holdings held as a proxy for others);
    - has been accepted as a participant under Regulation 2.7 to connect to the Austraclear System via the ANNI network;[5] or
    - is advised by Austraclear that it is a tier 1 participant for the purposes of this Guidance Note.[6]

A **tier 2 participant** is a participant that is not a tier 1 participant.[7]

Participants should review and assess their tier classification from time to time, particularly following any change in the nature or scale of their Austraclear 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 Austraclear 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. In the case of a tier 2 participant, an alternate site may include a location with an internet connection.

ANNI network means the Austraclear National Network Infrastructure (ANNI) which provides a dedicated fully routed network connection with end-to-end TCP/IP connectivity to access the Austraclear system, RITS and RBNZ services. A dedicated ANNI connection is required for participants with A$1 billion in holdings or who execute more than 100 transactions per day. This connection has previously been referred to as a premium connection, ASX Net or Host to Host lite and may be changed from time to time at Austraclear's discretion.

---

5 Austraclear determines the security and access requirements for the System in accordance with Regulation 3.1.1. A participant is taken to be accepted to access the Austraclear System via the ANNI network if it applied for such connectivity through the Participant Details Form submitted to Austraclear pursuant to Regulation 2.5(c) and that application was accepted under Regulation 2.7.

6 In assessing whether a participant should be classified as a "tier 1 participant", Austraclear 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 business conducted by related bodies corporate of the participant with Austraclear.

7 This will generally include most Associate Participants, Public Trust Participants and Special Purpose Participants accepted as a participant under Regulation 2.7 to access the Austraclear System via an internet connection rather than via the ANNI network.

Austraclear operations – the systems, technology, staff, premises, equipment, business processes and other resources used by a participant in conducting its business as an Austraclear Regulations. 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 Austraclear 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 Austraclear 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 Austraclear, 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 Austraclear operations.

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

critical Austraclear operations – that part of a participant's Austraclear operations that must be functioning to enable a participant to meet or support time critical obligations under the Austraclear Regulations including settlement of transactions, and maintenance of proper client records and accounting records.

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).[8]

cyber resilience – the ability to prepare for, detect, respond to and recover from a cyber-attack.[9]

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.[10]

disruption – an interruption to normal Austraclear operations.

digital certificate – a system used to authenticate user access to the Austraclear System, pursuant to Regulation 3.15 and Schedule D of the Regulations.

downtime – the period that a disruption lasts.

---

8 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.

9 *Ibid*.

10 As defined in the ASD publication: *Preparing for and responding to Denial of Service activities*, October 2014, available online at: https://www.asd.gov.au/publications/protect/preparing-for-responding-to-ddos-activities.htm. 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.

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.

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

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

recovery time objective or RTO – the target time within which Austraclear 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 Austraclear 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).

securID token – a token facilitating the public and private key infrastructure used to access the Austraclear System, pursuant to Regulation 3.15 and Schedule D of the Regulations.

shared facility – a facility accommodating technology or people employed in a participant's Austraclear 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.

All other capitalised terms have the same definition given to them in Austraclear Regulation 1.1.

4. Key requirements

4.1. Nominated officer and core personnel

All participants must allocate overall responsibility for disaster recovery and business continuity to a nominated business continuity officer[11] (nominated 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;
- 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 regulations and this Guidance Note; and
- will act as ASX's first point of contact for discussions related to the participant's disaster recovery and business continuity arrangements and any disruptions that may occur.

The nominated officer should:

- identify the core personnel needed to manage, recover and resume the participant's Austraclear operations following a disruption and ensure they have the facilities they need to do so within the recovery time objective

[11] The nominated officer may be from a related body corporate, including from overseas. However, in all cases, the nominated officer must understand the participant's business operations, as well as its obligations under the Austraclear Regulations and Guidance Notes.

stated in their BCP.[12] 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.

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 Austraclear 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 Austraclear operations and the communication links (including the communication provider and details of primary and redundant links) between each of those sites.

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

If a participant intends to make material changes to its technology or communications infrastructure 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

If participants are using other systems to connect to the Austraclear system, participants must have and maintain proper records of those key systems and technology, including but not limited to records showing:

- hardware, software and infrastructure used to conduct its Austraclear 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

Tier 1 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 potential disruption scenarios to their Austraclear operations and establish a business continuity plan (BCP) which seeks to ensure that their Austraclear operations can be recovered and resumed following a disruption within the recovery time objective stated in their BCP.[13]

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

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

A participant's BCP, and any changes to it from time to time, should be signed off by the nominated officer and approved by the appropriate senior management body.[14]

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

- an internal system outage;
- a sustained primary site outage (eg because of serious damage to a building); and
- the network of its primary telecommunication provider not being available for an extended period.

In the case of a tier 1 participant, the business impact analysis should cover a full range of potential disruption scenarios to its Austraclear operations, including the following additional disruption scenarios:

- if a participant has outsourced any of its Austraclear operations to a third party, a system outage at, or a communication failure with, the third party;
- an attempted or actual cyber attack on data or technology which impacts the participant's ability to conduct its Austraclear operations, including those elements outsourced;
- 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 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;
- a major disruption to public transport or related infrastructure (such as the closure of a major road or bridge) affecting a primary site; and
- a pandemic affecting the participant's staff or the staff of a party to whom it has outsourced some of its Austraclear operations.

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 no more than:

- 2 hours for critical Austraclear operations; and
- 4 hours for resumption of business-as-usual Austraclear operations.

A tier 2 participant's BCP should specify an RTO following the initiation of its BCP of no more than:

- 4 hours for critical Austraclear operations; and
- 6 hours for resumption of business-as-usual Austraclear operations.

[14] The appropriate body to approve a participant's BCP will vary, depending on the significance of the participant's Austraclear operations compared to its other operations and its governance structure. If the participant's Austraclear 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.

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 Austraclear 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 Austraclear operations are down.

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, Austraclear 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.[15]
- A participant should have sufficient technology in place at its primary and alternate sites so that Austraclear operations can occur at each location, independently of the other. This includes the availability of securID tokens and up-to-date back-up digital certificates required to access the Austraclear System.
- 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.
- A participant 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 arrangements to one or more of the latest global or national cyber standards and guidance.[16] The arrangements should be implemented at all primary and alternate sites to ensure maximum security across all sites and to facilitate continuity of their Austraclear operations in the event of disruption, including a cyber attack.

The following additional requirements apply to tier 1 participants:

- 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 and alternate sites for all critical Austraclear operations that is readily available to promptly reproduce disruptions to technology and to find resolutions to them.

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

[16] 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).

- 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.
- An alternate site should 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.
- A participant 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 admitted to settle securities transactions also consider utilising two internet service providers to address these concerns.

4.8. Incident management plan

A tier 1 participant 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 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, Austraclear, 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.

A tier 2 participant need not have a detailed incident management plan but should maintain an up-to-date contact list for key parties that can be used in case of a disruption event. The list should be reviewed at least annually to ensure it remains current and adequate.

4.9. Incident management records

Tier 1 participants must maintain proper records of disruptions impacting their Austraclear 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, other regulators 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 Austraclear 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 Austraclear transactions was completed;
- a summary of the root cause analysis and any corrective actions taken;
- where the disruption to its Austraclear 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.

4.10. BCP testing

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

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

At a minimum, the BCP testing should confirm:

- 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; and
- the ability of users to complete business-as-usual processes at alternate sites.

In the case of Tier 1 Participants, the test should also confirm:

- successful fail-over of technology from a primary site to an alternate site;
- successful fail-over of the communications network to an alternate site, ensuring connectivity is maintained to other participant sites, Austraclear, payment providers and any party to whom it outsources any of its Austraclear operations;
- 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 officer and reported to the appropriate senior management body. [17]

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

[17] See note 14 above.

4.11. Outsourced operations

A participant that has outsourced any of its Austraclear operations to someone else should ensure its service level agreement with any third party performing outsourced 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.[18] The participant should supervise any outsourced activities to ensure they comply with the participant's obligations under the Austraclear Regulations and this Guidance Note.

4.12. 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 Austraclear operations are thoroughly assessed, tested and authorised, and that appropriate disaster recovery and roll-back arrangements are in place, before changes are implemented.

Participants should establish a framework which ensures that they are made aware of all relevant system and infrastructure changes initiated by vendors or service providers that may impact their Austraclear 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. Participants must make their own independent assessment of the changes and the quality and extent of testing conducted by the vendor or service provider.

4.13. Notification requirements

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

- any disruption that causes the participant to engage its BCP for its Austraclear operations, as soon as reasonably practicable after it becomes aware of the disruption; and
- any significant outage impacting its Austraclear 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.

All participants must also notify ASX:

- as soon as practicable of any significant breach of, or non-compliance with, the disaster recovery and business continuity requirements in the Austraclear Regulations (as interpreted in accordance with this Guidance Note);[19]
- 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 connect to the Austraclear system; and
- within 10 business days of the appointment and any subsequent departure of their nominated business continuity officer.

4.14. 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, updateing and approval of those arrangements.

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

[19] Austraclear Regulation 17.2(a2)