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 • Austraclear's requirement for the 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	• 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 15/06/15. A previous version of this Guidance Note was issued in 10/14.

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 rules. 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]

This Guidance Note does not apply to collateral manager special purpose participants and foreign currency settlement bank participants. These participants must comply with the detailed business continuity requirements outlined in the relevant Regulations specific to their participant status.[2]

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);

[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 28.15 (Collateral Manager) and Austraclear Regulation 29.3 (Foreign Currency Settlement Bank).

- 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;[3] or
- is advised by Austraclear that it is a tier 1 participant for the purposes of this Guidance Note.[4]

A **tier 2 participant** is a participant that is not a tier 1 participant.[5]

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 the 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 the 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.

Austraclear operations – the technology, staff, premises, equipment, business processes and other resources used by a participant in conducting its business and performing its obligations under the Austraclear Regulations. This includes, but is not limited to, payment arrangements with the participant's bank, client 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 continue its Austraclear operations 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.

---

[3] 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.

[4] 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 amount and type of business conducted by related bodies corporate of the participant with Austraclear.

[5] 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.

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.

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).[6]

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.

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.

geographically remote – where the primary site and alternate site are in different locations with suitably different risk profiles. Generally speaking, the alternate site should be at least 5 kilometres away from the primary site and on a separate power grid. However, it is important for participants to consider any local factors that may impact the required distance. For example, if a participant's primary site is located in a local flood zone that extends for more than 5 kilometres, the participant should locate its alternate site outside the flood zone.

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 – 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 shared by staff employed in a participant's Austraclear operations and staff employed in another business unit of the participant or of 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.

[6] As defined in ASIC Report 429: *Cyber resilience: Health check*, March 2015, available online at: http://download.asic.gov.au/media/3042176/rep429-published-19-march-2015.pdf.

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

4. Key requirements

4.1. 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.[7]

The BCP should be signed off at senior management level and 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 the primary and alternate sites.

At a minimum, the BCP 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 the third party;
- an attempted or actual cyber attack on data or technology required to conduct its Austraclear operations, including those elements outsourced;[8]
- 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 a primary site for an extended period;
- 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.

4.2. Recovery time objective

A tier 1 participant's BCP should specify a recovery time objective of not more than 4 hours following the initiation of its BCP, and preferably only 2 hours.

A tier 2 participant's BCP should specify a recovery time objective of not more than 6 hours following the initiation of its BCP, and preferably only 4 hours.

Within that period, the participant should have been able to resume its business-as-usual Austraclear operations and also completed the processing of all transactions affected by the disruption.

7 The recovery time objective stated in the participant's BCP should conform to key requirement 4.2.

8 Further guidance on offshoring and outsourcing arrangements can be found in Austraclear Regulations Guidance Note 9 *Offshoring and Outsourcing*.

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.

4.3. 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.[9]
- Sufficient technology should be in place at the 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.
- Technology housed at the 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.

The following additional requirements apply to tier 1 participants:

- The 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.
- The primary and alternate sites should use separate hardware and separate communication lines in order to avoid a single point of failure.
- The 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 for all critical technology to seek to reproduce disruptions to technology and to find resolutions to them.
- The alternate site should be able to handle any additional volumes associated with accumulation of transactions during a disruption.
- If an alternate site is a shared facility, the participant should ensure there are appropriate arrangements in place to preserve the confidentiality of any confidential client information.
- An alternate site should be geographically remote from any primary site.
- The communications network should have dual line redundancy using diverse paths and preferably alternate telecommunication providers, where practicable, to eliminate single points of failure.

4.4. Core personnel

All participants should identify the core personnel needed to recover and resume their Austraclear operations following a disruption and provide them with the facilities they need to do so within the recovery time objective stated in their BCP.[10] 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 from an alternate location including any items which facilitate remote access, such as securID tokens and up-to-date back-up digital certificates.

[9] Again, the recovery time objective stated in the participant's BCP should conform to key requirement 4.2.

[10] Again, the recovery time objective stated in the participant's BCP should conform to key requirement 4.2.

A tier 1 participant should 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 the primary site.

4.5. 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 4.1. 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.

4.6. 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 or its disaster recovery and business continuity arrangements

Participants should record and analyse the outcomes of all testing conducted in accordance with this key requirement.

At a minimum, the test should confirm:

- successful validation of connectivity, data and applications at an alternate site;
- the ability of users to access and log in to technology and applications at an alternate site, including the use of remote access where applicable; and
- the ability of users to complete business-as-usual processes at an alternate site.

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

- successful fail-over of technology from the primary site to the alternate site;
- successful fail-over of the communications network to the 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 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.

4.7. Outsourced operations

A participant that has outsourced any of its Austraclear operations to someone else should have a service level agreement with that party to ensure that their business continuity arrangements 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.[11]

4.8. Change management

All participants should have and comply with change management policies and procedures that are designed and function 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.

4.9. Notification requirements

All participants should notify Austraclear 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, as soon as it becomes apparent that it is or is likely to be a significant outage.

[11] Again, the recovery time objective stated in the participant's BCP should conform to key requirement 4.2.