# 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<br>• How those requirements differ for "tier 1" and "tier 2" participants<br>• The requirement for a participant to have a nominated business continuity officer responsible for disaster recovery and business continuity<br>• The requirement for a participant to have an up to date infrastructure diagram of its current architecture<br>• The requirement for a participant to maintain proper records of its key Austraclear systems and infrastructure<br>• 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 20/12/19. Previous versions of this Guidance Note were issued in 10/14, 06/15 and 08/19.

**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** **2**
**2. Participant tiering** **3**
**3. Terms used in this Guidance Note** **3**
**4. Key requirements** **5**
4.1. Nominated business continuity officer and core personnel 5
4.2. Infrastructure diagrams 6
4.3. Systems and technology records 6
4.4. Replacement policy 6
4.5. Business continuity plan 6
4.6. Recovery time objective 8
4.7. System resilience 8
4.8. Incident management plan 9
4.9. Incident management records 10
4.10. BCP testing 10
4.11. Outsourced operations 11
4.12. Change management 11
4.13. Notification requirements 11
4.14. Independent review 12

# 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 business continuity officer and core personnel

All participants must allocate overall responsibility for disaster recovery and business continuity to a nominated officer[11] ("nominated business continuity officer") who:

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

The nominated business continuity 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 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;

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

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

- 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.

When initiating contact with a participant regarding disaster recovery and business continuity arrangements, representatives of Austraclear would in the first instance contact one of the participant's authorised signatories to confirm the identity of the nominated business continuity officer. Subsequent discussions regarding business continuity and disaster recovery arrangements would then be held between representatives of Austraclear and the nominated business continuity officer.

### 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 Austraclear 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 Austraclear 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]

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

**Loss of access / loss of site:**

- a primary site outage with same-day recovery (eg because of a need to evacuate a building following a bomb threat or fire alarm);
- a 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;

**Loss of systems / technology:**

- 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;

**Loss of staff / pandemic:**

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

**Cyber:**

- 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 or offshored.

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.

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

[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.

### 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.

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

Austraclear 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. Austraclear 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:

[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).

- 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.
- 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.

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

### 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 Austraclear;
- 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 Austraclear 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 Austraclear.

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 business continuity 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.

### 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 material and 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 that may impact their Austraclear operations. Participants must make their own independent assessment of the changes and the quality and extent of testing conducted by the vendor or service provider.

### 4.13. 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 Austraclear:

[17] See note 14 above.

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

- 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] 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 connect to the Austraclear system.

### 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, updating and approval of those arrangements.

[19] Austraclear Regulation 17.2(a2)