|  |
| --- |
| January 2020 |
|  |

Following publication of revised Guidance Note 10 (GN10) *Business Continuity and Disaster Recovery[[1]](#footnote-1)*, Austraclear participants, with the exception of Special-Purpose Participants, are expected to comply with all changes other than changes to the RTO[[2]](#footnote-2), by March 2020. Participants may be required to provide evidence of how they are complying with GN10 upon request.

For the purpose of GN10, Special Purpose Participants include:

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

To assist participants in carrying out their assessments and/or evidencing their compliance, please refer to the self‑assessment form below. (Participants are not obliged to use this self‑assessment and may design a form tailored to their own business and processes). This form covers key requirements that are applicable to relevant Austraclear participants. If participants are also a participant of other ASX markets or facilities they may complete a single form for all participations or separate forms as they deem appropriate, noting there are minor variances in the requirements for Austraclear.

This self-assessment form will assist participants to:

* document the assessment of their current business continuity and disaster recovery arrangements against the key requirements of GN10;
* identify requirements that are partially aligned or not aligned;
* record the remediation action taken to align to the requirements; and
* evidence the results of the gap analysis and the independent review process.

### **Instructions for completion:**

In using this self‑assessment the participant should:

* where connecting to Austraclear via proxy, arrange for the self-assessment to be completed by the proxy.
* select a rating of ‘Fully aligned’, ‘Partially aligned’ or ‘Not aligned’ that accurately reflects its current level of alignment to the relevant requirement (or, where relevant, ‘Not applicable’); and
* where a rating of ‘Partially aligned’ or ‘Not aligned’ is selected, include details to specify which aspect of the requirement is not fully aligned, and provide details of remediation action taken/planned to align to the arrangements, including targeted completion date (where applicable).

Participants are *not* required to submit the completed self‑assessment form to Austraclear upon completion. However, participants should be aware that Austraclear may, at any time, request a copy of their self‑assessment (including any supporting information used for the purposes of assessing the participant’s level of alignment and remediation actions planned to meet the requirements). If participants do not use this form, they must, on request, provide similar evidence to the satisfaction of Austraclear.

|  |  |
| --- | --- |
| **Abbreviations used** |  |
| BC | Business Continuity |
| BCP | Business Continuity Plan |
| DR | Disaster Recovery |
| RTO | Recovery Time Objective |

### **Self‑Assessment – Austraclear Regulation Guidance Note 10 - Key Requirements for Business Continuity and Disaster Recovery Arrangements**

|  |  |  |
| --- | --- | --- |
| **Information Required** | | **Response** |
| **2. Proxy information and participant tiering** | | |
| **2.1** | If your participant has delegated access to another participant to act as its proxy for its connectivity to Austraclear, confirm the details of your proxy. | Proxy Name:  Proxy mnemonic:  Where a proxy completes this self-assessment on behalf of your participant, it is recommended that your participant requests a copy of the completed self-assessment form and retains this for its own records. |
| **2.2** | Confirm your participant’s tiering | Tier 1  Tier 2 |
| **2.3** | When did your participant last conduct a review to verify its tiering? | Date of the last review: Click or tap to enter a date.  The classification was updated as the result of the last review undertaken:  Yes  No |

This form does not reproduce the full details of each key requirement in GN10.   
Participants are expected to review the full details of each key requirement when completing the self‑assessment.

|  | KEY REQUIREMENT | LEVEL OF ALIGNMENT  Fully aligned (F)  Partially aligned (P)  Not aligned (N) Not applicable (N/A) | REMEDIATION  Provide details for each ‘Partially aligned’ or ‘Not aligned’ response.  Where relevant, include details of plans and timeframes to achieve a level of alignment of ‘F’ |
| --- | --- | --- | --- |
| 4.1 Nominated business continuity officer and core personnel  Note: 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. | | | |
| Nominated business continuity officer: | | | |
| 4.1.1 | Appointed | F  P  N |  |
| 4.1.2 | Delegated authority | F  P  N |  |
| 4.1.3 | Requisite qualification, skills and experience | F  P  N |  |
| 4.1.4 | Aware of responsibilities under GN10 | F  P  N |  |
| 4.1.5 | Required core personnel identified | F  P  N |  |
| 4.1.6 | Ensure facilities are available for core personnel within RTO following event of disruption | F  P  N |  |
| 4.1.7 | Ensure clearly defined roles and responsibilities for core personnel under the BCP, tested as part of BCP fire drills | F  P  N |  |
| 4.1.8 | Ensure allocation matrix maintained | F  P  N |  |
| 4.1.9 | Ensure awareness training conducted for all relevant personnel | F  P  N |  |
| 4.2 Infrastructure diagrams | | | |
| 4.2.1 | Accurately reflect the current state of the technology and communication infrastructure for Austraclear operations | F  P  N |  |
| 4.2.2 | Identify all primary and alternate sites housing technology components, personnel and communication links between each site | F  P  N |  |
| 4.2.3 | Clearly identify elements (i.e. technology and personnel) of Austraclear operations at each site | F  P  N |  |
| 4.2.4 | Reflect plans for proposed material changes to technology and communication infrastructure | F  P  N  N/A |  |
| 4.3 Systems and technology records | | | |
| 4.3.1 | Proper records are retained and available to be provided to Austraclear upon request | F  P  N |  |
| 4.4 Replacement policy | | | |
| 4.4.1 | Tier 1 : system and technology replacement policy developed with process to identify assets nearing end of life | F  P  N  N/A – Tier 2 |  |
| 4.5 Business continuity plan | | | |
| 4.5.1 | Business impact analysis conducted covering a range of potential disruption scenarios specific to Austraclear operations | F  P  N |  |
| 4.5.2 | BCP designed to ensure that recovery and resumption of Austraclear operations following disruption is aligned with stated RTO | F  P  N |  |
| 4.5.3 | Signed off by nominated business continuity officer and approved by senior management body | F  P  N |  |
| 4.5.4 | Securely and centrally stored and can be readily accessed (both hard and soft copies) | F  P  N |  |
| 4.5.5 | Addresses, at a minimum:   * + 1. Internal system outage     2. Sustained primary site outage     3. Network of primary telecommunications provider not being available for extended period | 1. F  P  N 2. F  P  N 3. F  P  N |  |
|  | Tier 1 only: refer to 4.5.6 – 4.5.9 (inclusive): | N/A – Tier 2 : proceed to 4.6 |  |
| 4.5.6 | Meets “Loss of access / loss of site” scenarios   1. Primary site outage with same-day recovery 2. Loss of primary electricity supply/key utilities to a primary site for extended period 3. In the event of multiple primary sites, loss of one site/connectivity between split sites 4. Major disruption to public transport / infrastructure | 1. F  P  N 2. F  P  N 3. F  P  N 4. F  P  N |  |
| 4.5.7 | Meets “Loss of systems / technology” scenario   1. System outage /communication failure with third party (if outsourcing) | 1. F  P  N  N/A |  |
| 4.5.8 | Meets “Loss of staff / pandemic” scenario | F  P  N |  |
| 4.5.9 | Meets the “Cyber” scenario | F  P  N |  |
| 4.6 Recovery time objective | | | |
| 4.6.1 | Tier 1:  BCP specifies RTO following initiation of BCP of no more than 2 hours for critical Austraclear operations | F  P  N  N/A – Tier 2 |  |
| 4.6.2 | Tier 1:  BCP specifies RTO following initiation of BCP of no more than 4 hours for resumption of business‑as‑usual Austraclear operations | F  P  N  N/A – Tier 2 |  |
| 4.6.3 | Tier 2:  BCP specifies RTO following initiation of BCP of no more than 4 hours for critical Austraclear operations | F  P  N  N/A – Tier 1 |  |
| 4.6.4 | Tier 2:  BCP specifies RTO following initiation of BCP of no more than 6 hours for resumption of business‑as‑usual Austraclear operations | F  P  N  N/A – Tier 1 |  |
| 4.6.5 | In cyber incidents, BCP design enables safe resumption and completion of critical Austraclear operations as close to applicable RTO as possible | F  P  N |  |
| 4.6.6 | Framework to ensure decision making process is timely following a disruption | F  P  N |  |
| 4.7 System resilience | | | |
| 4.7.1 | Technology is configured and plans and processes established to allow Austraclear operations to be recovered and resumed at an alternate site with minimal downtime and within the RTO | F  P  N |  |
| 4.7.2 | Sufficient technology to enable Austraclear operations to occur at each location, independently | F  P  N |  |
| 4.7.3 | Alternate site can handle business‑as‑usual volumes and any additional volume associated with the disruption | F  P  N |  |
| 4.7.4 | Technology at all sites is secured and adequately protected | F  P  N |  |
| 4.7.5 | Conduct a review, at least annually, to assess how the system and infrastructure can be designed to improve cyber resilience. | F  P  N |  |
| 4.7.6 | BC arrangements are:   1. aligned with one or more of the latest global or national cyber standards and guidance 2. implemented at all primary and alternate sites | 1. F  P  N 2. F  P  N |  |
|  | Tier 1 only: refer to 4.7.7 – 4.7.16 (inclusive): | N/A – Tier 2 : proceed to 4.8 |  |
| 4.7.7 | Sites have a continuous power supply and generator back-up for a reasonable period | F  P  N |  |
| 4.7.8 | Sites have separate hardware and communication lines to avoid single points of failure | F  P  N |  |
| 4.7.9 | Sites are on common software versions with access to appropriate system and software documentation as required | F  P  N |  |
| 4.7.10 | Suitable test environment readily available at primary and alternate sites | F  P  N |  |
| 4.7.11 | Error-message logs available at primary and alternate sites | F  P  N |  |
| 4.7.12 | If data centres operate in an ‘active-active’ configuration, appropriate monitoring tools are readily available | F  P  N  N/A |  |
| 4.7.13 | If using a shared facility, appropriate arrangements to preserve the confidentiality of client information | F  P  N  N/A |  |
| 4.7.14 | System resilience maintained across and between all sites to continue business as usual activity in the event of a disruption or loss of connectivity to one or more site | F  P  N |  |
| 4.7.15 | An alternate site is geographically remote to any primary site. | F  P  N |  |
| 4.7.16 | Dual communication lines and internet services providers to avoid a single point of failure | F  P  N |  |
| 4.8 Incident management plan | | | |
| 4.8.1 | Tier 2:  Have an up-to-date contact list for a disruption event, and review the list annually | F  P  N  N/A – Tier 1: proceed to  4.8.2 – 4.8.5 (inclusive) |  |
|  | Tier 1 only: refer to 4.8.2 – 4.8.5 (inclusive): | N/A – Tier 2: proceed to 4.10 |  |
| 4.8.2 | Clearly defined and documented incident management plan addressing disruption scenarios identified | F  P  N |  |
| 4.8.3 | Incident management plan includes a communications plan applicable for each disruption scenario, with up‑to‑date contact list for key parties | F  P  N |  |
| 4.8.4 | Reviewed and tested at least annually | F  P  N |  |
| 4.8.5 | Available in electronic and hard copies, and accessible at all primary and alternate sites | F  P  N |  |
| 4.9 Incident management records | | | |
| 4.9.1 | Tier 1:  Proper records of disruptions impacting Austraclear operations are maintained | F  P  N  N/A – Tier 2 |  |
| 4.10 BCP testing | | | |
| 4.10.1 | Testing is conducted at least once annually | F  P  N |  |
| 4.10.2 | Testing is conducted as soon as practicable following any material change | F  P  N |  |
| 4.10.3 | Testing is conducted as soon as practicable following notification by Austraclear | F  P  N |  |
| 4.10.4 | The BCP testing confirms the scenarios listed including (at a minimum): |  |  |
| All participants:   1. Validation of connectivity, data and applications at alternate sites 2. Confirmed user access to technology and applications at alternate sites (including remote access) 3. Business-as-usual processes completed at alternate sites. | 1. F  P  N 2. F  P  N 3. F  P  N |  |
| Tier 1 only: refer to iv. – vii. (inclusive) | N/A – Tier 2: proceed to 4.10.5 |  |
| iv. Technology fail-over from primary to alternate site  v. Comms network fail-over to alternate site  vi. Sufficient capacity to handle business-as-usual and additional volumes accumulated  vii. Successful restoration of the production environment | iv.  F  P  N  v.  F  P  N  vi.  F  P  N  vii.  F  P  N |  |
| 4.10.5 | Outcomes of testing recorded and analysed, specifically including confirmation that the RTO was met | F  P  N |  |
| 4.10.6 | The final test outcomes, including any enhancements to the test plan, are signed off by the nominated business continuity officer and properly reported | F  P  N |  |
| 4.11 Outsourced or offshored operations | | | |
| 4.11.1 | Any part of Austraclear operations has been outsourced or offshored | Yes – proceed to 4.11.2  No - proceed to 4.12 |  |
| 4.11.2 | Has appropriate resources and processes to ensure service level agreements require a third party to have and maintain appropriate and complimentary BC arrangements that allow the participant’s RTO to be met | F  P  N |  |
| 4.11.3 | Has appropriate resources and processes to supervise any outsourced or offshored activities | F  P  N |  |
| 4.12 Change management | | | |
| 4.12.1 | Change management policies and procedures designed effectively to ensure that changes to Austraclear operations are assessed, tested, authorised and appropriate DR arrangements are in place prior to implementation | F  P  N |  |
| 4.12.2 | Framework in place to identify material and relevant changes made by vendors or service providers impacting Austraclear operations and to ensure these are subject to change management policies and procedures | F  P  N |  |
| 4.12.3 | Independent assessment of changes made and testing conducted by vendors or service providers | F  P  N |  |
| 4.13 Notification requirements | | | |
| 4.13.1 | BCP includes notification requirements to Austraclear of relevant disruptions, outages, significant breaches / events of non-compliance and / or actions impacting capacity to connect to the Austraclear system | F  P  N |  |
| 4.13.2 | Policies and procedures incorporate compliance notification obligations | F  P  N |  |
| 4.14 Independent review | | | |
| 4.14.1 | DR and BC arrangements are independently reviewed on a periodic basis | F  P  N |  |

1. Changes to GN10 for Austraclear Regulations were published by ASX on 5 August 2019 and on 20 December 2019. [↑](#footnote-ref-1)
2. Transition arrangements for implementing the target RTO are outlined in the report *Results of Consultation on Guidance Note changes for ASX Clear, ASX Settlement, ASX Clear (Futures) and Austraclear participants*, published on 5 August 2019 and available on [asx.com.au](https://www.asx.com.au/regulation/public-consultations.htm). [↑](#footnote-ref-2)
3. A collateral manager must comply with the business continuity requirements in Austraclear Regulation 28.15(c). [↑](#footnote-ref-3)
4. A foreign currency settlement bank must comply with the business continuity requirements in Austraclear Regulation 29.3. [↑](#footnote-ref-4)