NZX Guidance Note

Business continuity and disaster recovery

November 2025

The purpose of this Guidance Note is to provide guidance to NZX Participants in relation to business continuity plan requirements encompassed by the Participant Rules, Derivatives Market Rules and Clearing & Settlement Rules.

Contents

This Guidance Note has been issued by NZX to promote market certainty and assist market participants. This Guidance Note sets out NZX's general approach to the subject, but is not to be regarded as a definitive statement of the application of the Participant Rules, Derivatives Market Rules or Clearing & Settlement Rules in every situation. Examples set out in this Guidance Note are limited and are not designed to cover all eventualities. NZX may replace Guidance Notes and Practice Notes at any time and an NZX Participant should ensure it has the most recent versions of these documents. Guidance Notes do not constitute legal advice. NZX recommends that NZX Participants take advice from qualified persons.

1. Introduction

The purpose of this Guidance Note is to provide guidance and best practice information for Participants in respect of the NZX Limited (**NZX**) and New Zealand Clearing Limited (**CHO**) business continuity plan and disaster recovery requirements, including:

- matters that should be considered when developing business continuity plans (**BCPs**) and disaster recovery arrangements, including threat and impact analysis;
- key content requirements for business continuity plans;
- development of disaster recovery arrangements; and
- NZX and CHO powers when Participants wish to be reconnected to systems provided by NZX or CHO after an event.

BCPs and disaster recovery arrangements are a key part of addressing operational risk within a Participant's business. BCPs should aim to minimise the consequences of a disruption to a Participant's business, and disaster recovery arrangements should provide for the swift recovery of key functions.

1.1 Scope of this Guidance Note

This Guidance Note provides additional guidance to Participants to support their compliance with the requirements of:

- Rule 8.12 of the NZX Participant Rules (the **Participant Rules**);
- Rule 4.15 of the NZX Derivatives Market Rules (the **Derivatives Rules**); and
- Rule 2.17 of the CHO Clearing and Settlement Rules (the **C&S Rules**);

collectively "**Rules"** for the purpose of the Guidance Note.[1]

References to Participants in this Guidance Note include:

- a Market Participant as defined in the Participant Rules;
- a Participant as defined in the Derivatives Rules; and
- a Clearing Participant as defined in the C&S Rules;

collectively "**Participants"** for the purpose of the Guidance Note.

Capitalised terms which are not defined in this Guidance Note have the same meanings as given to them in the above Rules.

Under Participant Rule 21.4.1, Derivatives Rule 14.14.1 and C&S Rule 6.13.1, NZX and CHO may act by and through NZX Regulation Limited (**NZ RegCo**) in performing any function or

[1] Where applicable the Guidance Note also references the relevant Derivatives Market Procedures (the **Derivatives Procedures**) and the Clearing and Settlement Procedures (the **C&S Procedures**).

discharging any power set out in the Rules. References in this Guidance Note to NZX therefore also include NZ RegCo in relation to any regulatory activity or discretion.

2. Background

The Rules require a Participant to have and maintain adequate BCP and disaster recovery arrangements in relation to its role as a Participant. Participants maintaining robust BCPs and disaster recovery arrangements is essential for the stability and resiliency of the wider financial markets' ecosystem.

The Rules contain high-level principles based requirements for the development of BCPs and disaster recovery arrangements, and prescriptive requirements relating to the contents of a BCP.

A Participant's BCP should provide a structure by which its operations that are relevant to its role as a Participant can continue to operate during a disruption, which includes outlining roles and responsibilities, key systems and processes, workarounds where appropriate, and recovery priorities. The development and implementation of a BCP should support a Participant's resiliency if it is faced with a disruption.

Participants must also have disaster recovery arrangements, which are arrangements to be implemented should continuation of its operations relevant to its role as a Participant not be possible. This may include processes for moving to alternative sites or systems, with such plans aiming to recover a Participant's operations as quickly as possible when faced with an operational outage.

While there is a growing business dependency on technology, and as such technology resources will be a significant component of BCP and disaster recovery, we consider BCP arrangements should be wider than technology and extend to non-technological resources.

3. Threat and impact analysis

Participant Rule 8.12.2, Derivatives Rule 4.15.2, C&S Rule 2.17.2

Each [Participant] must identify and consider major threats that may result in short, medium, and long term disruptions of its [Broking Business / operations that are relevant to its role as a Participant] when developing the arrangements required by [Participant Rule 8.12.1, Derivatives Rule 4.15.1, and C&S Rule 2.17.1], and the possible impacts of those threats. This includes, but is not limited to, threats that may arise as a result of the Participant's dependency on critical third-party providers.

For a Participant to have in place robust BCPs and disaster recovery arrangements, it must first identify the major threats facing its business as it relates to its role as a Participant, consider the possible impacts of these threats, and develop arrangements for managing situations if and when such threats arise. Comprehensive threat and impact analysis should support Participant resiliency and allow a Participant to respond promptly to crisis situations.

The types of threats that may be relevant to a Participant's business will vary, however some scenarios may include:

- partial or total loss of systems.
- loss of key personnel.
- failure of a critical third-party provider impacting the Participant's ability to conduct its operations.
- short or long-term loss of access to premises or facilities.

NZX does not require a Participant's BCP or disaster recovery arrangements to identify the threats specific to its business, however threat identification should be conducted regularly to ensure its BCP and disaster recovery arrangements are fit for purpose.

As part of this threat identification and impact analysis, Participants must assess dependencies on critical third-party providers. Participants should be identifying third-parties that provide services that are critical to its role as a Participant. Where a Participant identifies a dependency on a third-party, a Participant should consider whether it is appropriate to engage with that third-party provider as part of the development of the Participant's BCP and disaster recovery arrangements (including considering factors that may contribute to a Participant's reasonable recovery objectives – see section 4.3 below for more information). NZX also recommends that Participants consider dependencies, and threats that arise as a result of such dependencies, on other parties in the wider financial markets eco-system, beyond those that provide services directly.

4. Key requirements for BCPs

NZX acknowledges that there is no 'one size fits all' approach to business continuity plans and considers that arrangements should be appropriate to the size, scope, and complexity of a Participant's business. The Rules contain minimum content requirements that Participants should address in their BCPs, which we have provided further guidance on below.

4.1 Management framework

Participant Rule 8.12.3, Derivatives Rule 4.15.3, C&S Rule 2.17.3

As a minimum, a [Participant's] business continuity plan must address the following matters…

(a) The management framework for implementing the Participant's business continuity plan, including defining the roles and responsibilities of the Participant's board and senior management (as relevant) in relation to the design, implementation, functioning and review of the plan, and provides that the plan must be subject to the oversight of the [Compliance Manager, Responsible Executive, Responsible Person, or Managing Principal].

Participants must ensure their BCPs define the roles and responsibilities of the Participant's board and senior management (as relevant) in relation to the design, implementation, functioning, and review of the BCP.

A Participant's board and senior management are collectively responsible for ensuring the appropriateness of a Participant's business continuity arrangements. The degree of board involvement in relation to the design, implementation, functioning and review of a Participant's BCP will differ depending on the size and complexity of that Participant's business.

NZX does not expect a Participant's board to be involved in the operational aspects of its BCP.

Participants must also ensure that BCPs are subject to the oversight of the relevant person (i.e., Compliance Manager, Responsible Executive, or Responsible Person).

The management framework in a Participant's BCP should:

- identify the core roles needed to manage, recover, and resume the Participant's operations following a disruption; and
- ensure that the personnel required to fill these roles have clearly defined roles and responsibilities under the BCP.

NZX recommends that Participants also consider the training requirements for core personnel to ensure that they have sufficient knowledge of what to do in the event of a disruption, and ensure that core personnel are included in any testing that is undertaken (see section 4.6 below).

Participants must also ensure that they appoint an emergency contact person for NZX and CHO to contact in the case of emergency, and make sure NZX and CHO have up to date contact details for this person.[2] It is best practice for Participants to ensure that emergency contact persons are of a sufficient seniority to take appropriate action in an emergency, for example the Participant's Managing Principal, Responsible Executive or Responsible Person.

4.2 Services or functions to be maintained

Participant Rule 8.12.3, Derivatives Rule 4.15.3, C&S Rule 2.17.3

As a minimum, a [Participant's] business continuity plan should address the following matters…

(b) The services or functions to be maintained by the business continuity plan;

(c) the processes, procedures, and resource requirements to enable the services and functions identified at (b) above to be performed, including people, systems, and other assets and arrangements for how these resources will be obtained during a disruption.

A Participant must ensure its BCP set out the services and functions to be maintained by the arrangements.

[2] Participant Rule 3.28, Derivatives Rule 4.15.4, C&S Rule 2.17.4.

A Participant should assess which services and functions are relevant to its role as a Participant and ensure that these are appropriately provided for in the BCP. These services and functions may include, but are not limited to:

- data communication lines
- routers
- gateways
- open interface sessions
- databases and archives / storage
- payment facility access
- site access and contingency
- accounting systems, and
- client services functions, including client access to funds.

A Participant must also ensure that its BCP includes processes and procedures to enable these services and functions to be performed in the case of a disruption, including arrangements for how the resources critical to performing these services and functions will be obtained. This may include, where appropriate, workarounds in the case certain systems or resources are not available.

4.3 Recovery priorities

Participant Rule 8.12.3, Derivatives Rule 4.15.3, C&S Rule 2.17.3

As a minimum, a [Participant's] business continuity plan should address the following matters…

(d) the recovery priorities for that [Participant's] services or functions affected by a disruption

A Participant must ensure that its BCP addresses the Participant's recovery priorities for the services or functions that have been affected by the disruption.

When developing recovery priorities, a Participant should consider the services and functions relevant to its role as a Participant and determine minimum levels of service for these functions. Recovery priorities should reflect the risk a Participant represents to the operation of the wider ecosystem.

It is best practice for BCPs to include prioritisation of the Participant's services functions and functions. For example, a Participant might prioritise functions as follows: (1) trading and settlement functions to be recovered first as "critical", (2) email, workflow, and risk management

to be recovered second as “important”, and (3) research and administration to be recovered last and only if warranted as “non-critical”.[3]

While Participants are not required to specify recovery time objectives (**RTOs**),[4] it is best practice for a Participant’s BCP and disaster recovery arrangements to contain RTOs sufficient to permit the Participant to return to normal operations within a reasonable time. A “reasonable time” will differ depending on the nature of a Participant’s business, however when making an assessment as to what is reasonable Participants should consider:

- the below RTOs in relation to NZX or CHO systems, and
- any contractual arrangements that a Participant has with its critical third-party providers that are relevant to that Participant’s own recovery after a disruption.

NZX and CHO system RTOs

System	RTO
NASDAQ ME	1 hour
BaNCS	2 hours
SWIFT	2 hours

Note that the RTOs outlined above are subject to change.

4.4 Communication arrangements

Participant Rule 8.12.3, Derivatives Rule 4.15.3, C&S Rule 2.17.3

As a minimum, a [Participant’s] business continuity plan should address the following matters…

(e) communication arrangements in relation to a disruption and how details of a disruption will be communicated to internal and external parties

A Participant must ensure that its BCP addresses communication arrangements in relation to a disruption and sets out how details of that disruption will be communicated to internal and external parties. Arrangements should include documented procedures for communicating with:

- internal contacts (e.g., staff, senior management and board)
- clients / customers

[3] Market Intermediary Business Continuity and Recovery Planning, IOSCO FR32/2015.

[4] An RTO is the maximum acceptable amount of time to take restoring a system, application, or business process to normal operations after a disruption.

- NZX / CHO
- regulators (including NZ RegCo)
- critical service providers (identified during threat analysis, see section 3 above)

A Participant should consider whether, given the size and complexity of its business, it is appropriate to include internal call cascades and/or call trees to ensure communication to critical personnel during a disruption occurs.

4.5 Integrity of information

Participant Rule 8.12.3, Derivatives Rule 4.15.3, C&S Rule 2.17.3

As a minimum, a [Participant's] business continuity plan should address the following matters…

(f) processes for determining the integrity of any information relevant to [its role as a Participant] / [the Participant's Broking Business] affected by a disruption;

A Participant must ensure that its BCP contains processes for determining the integrity of any information relevant to its role a Participant that is affected by a disruption.

The purpose of these processes is for a Participant to assess whether the integrity of data being held by the Participant has been degraded as a result of the disruption, and to ensure that any degradation is resolved as part of the recovery from a disruption.

NZX /CHO may request information from a Participant in relation to the steps it has taken to assess the integrity of its data, in order to establish whether or not the Participant has identified and remedied any issues, to determine the risk of reconnecting the Participant to NZX/CHO systems. For further information on information requests, see section 6 below.

4.6 Testing and review

Participant Rule 8.12.3, Derivatives Rule 4.15.3, C&S Rule 2.17.3

As a minimum, a [Participant's] business continuity plan should address the following matters…

(g) processes for undertaking periodic testing of the adequacy and effectiveness of the business continuity plan.

…

Participant Rule 8.12.4, Derivatives Rule 4.15.5, C&S Rule 2.17.5

Each [Participant] must review the contents of its business continuity plan at least annually, and in any case as soon as reasonably practicable if there is a material change in the [Participant's] business location, structure, or operations.

Participants are required to have processes for periodically testing their BCPs. The cadence of this testing will depend on the size, scope and complexity of the Participant's business, however best practice is to ensure BCPs are tested at least annually. Testing might include using mock drills, training exercises, or tabletop exercises, and may tie into more general staff training around BCP awareness. It is best practice for a Participant to ensure its disaster recovery arrangements are also tested at least annually.

A Participant must also ensure that the contents of its BCP is reviewed at least annually, or after material changes to the Participant's business location, structure, or operations. NZX/CHO also considers it best practice for a Participant to review its BCP after a major incident, generally as part of a wider post-incident review.

Participants should have processes to ensure that any learnings obtained as a result of testing are incorporated into this review, and updates made to the BCP as appropriate.

5. Disaster recovery

While a Participant's BCP should focus on how its business continues to operate during a disruption, a Participant must also ensure it has adequate disaster recovery arrangements for situations where a Participant is unable to continue business operations, for example due to the failure of a critical system.

Robust disaster recovery arrangements support a Participant's redundancy strategies and should aim to reduce downtime where operations have been disrupted. A Participant's disaster recovery arrangements should cover technology systems that are critical to its role as a Participant.

Disaster recovery arrangements will vary depending on the complexity of a Participant's business, but NZX expects arrangements to cover situations where the Participant's systems and processes are unavailable. This may include (but is not limited to):

- failovers for critical systems
- disaster recovery sites
- data backup options

A Participant a should ensure it has appropriate and up-to-date documentation supporting its disaster recovery arrangements, including provisions for periodically testing these arrangements and ensuring that any output from such testing is considered as learning for uplift.

6. NZX powers in relation to disconnected Participants

Participant Rule 8.13, Derivatives Rule 4.16, C&S Rule 2.18

Where a [Participant] is unable to access systems provided by [NZX / CHO], [NZX / CHO] may require that [Participant] to provide information to it to enable [NZX/CHO] to determine whether reconnecting that [Participant] will compromise the integrity of [any NZX market / the Settlement System]. [NZX / CHO] retains complete discretion as to whether to reconnect a [Participant] to any of [NZX's / CHO's] systems.

The power to request information from a Participant before reconnecting the Participant to systems provided by NZX or CHO is aimed at allowing NZX/CHO to assess whether reconnecting a Participant will threaten the integrity of NZX's markets or the Settlement System.

Information that may be requested after a disconnection will be unique to the circumstances of that disconnection, however, is likely to include details of what caused the disruption as well as the steps the Participant has taken to remedy the cause.

In situations where the disconnection was caused by a serious event that NZX/CHO considers could have a contagion impact on the integrity of NZX's markets or the Settlement System (for example, a cyber-attack), an attestation may be required from a Participant to enable NZX /CHO to assess the risk of reconnection.

An attestation should be provided by someone authorised by the Participant with sufficient visibility of both the event that caused the disruption, and the impacts the event has had on the Participant's system. The person providing the attestation may differ depending on the nature of the event.

While the precise contents of the attestation will depend on the nature of the event, NZX/CHO may require that the attestation include information such as:

a) providing a timeline of the incident, along with the impact of the incident on services, data, servers, and other key parts of the Participant's operations;

b) details of the remediation activity already undertaken by the Participant, including any aspects that have not yet been remediated;

c) a certification to NZX or CHO that the Participant has:

   i. identified and assessed the type and extent of the event that caused the disruption; and

   ii. restored affected systems to a known and trusted state, and that such systems are appropriately protected.

NZX or CHO may also request additional evidence or a demonstration (where appropriate) of the integrity of the Participant's systems requiring remediation, to allow NZX or CHO to assess the risk to NZX/CHO's systems of reconnection.

In some scenarios, a disconnected Participant may also be required to confirm that it has obtained a third-party assurance report which confirms that the Participant has undertaken

appropriate remediation steps to restore and protect the affected systems. This requirement is expected to be limited to scenarios where there has been a high-impact, or systemic event, which raises risk to wider eco-system stability. In assessing whether third-party assurance should be required, NZX or CHO will consider the risks posed by the reconnection, including risks to other Participants, against the impact of any delay such requirement will have on the disconnected Participant's reconnection.

The requirement for a disconnected Participant to provide an attestation to NZX or CHO prior to reconnection reflects the systemically important nature of the systems operated by NZX and CHO, and the impact that a disruption to these systems could have on the wider financial eco-system.