Description of
Business Continuity Management & Disaster Recovery

Nasdaq Nordics & Baltics
Date: 2022-06-15

This document is valid for the legal entities:
Nasdaq Stockholm AB
Nasdaq Copenhagen A/S
Nasdaq Helsinki Ltd
Nasdaq Iceland h.f.
Nasdaq Tallinn AS
Nasdaq Riga AS
AB Nasdaq Vilnius
Nasdaq Oslo ASA
Nasdaq Clearing AB

Table of Contents

1 Document Data

1.1 Document Validity

This document is valid for the legal entities:

- Nasdaq Stockholm AB
- Nasdaq Copenhagen A/S
- Nasdaq Helsinki Ltd
- Nasdaq Iceland h.f.
- Nasdaq Tallinn AS
- Nasdaq Riga AS
- AB Nasdaq Vilnius
- Nasdaq Oslo ASA
- Nasdaq Clearing AB

The above listed entities use common trading systems, clearing system and related systems which enable efficient cross-border trading, cross membership, and one source for Nordic and Baltic market data.

In this document, Nasdaq refers to Nasdaq Nordic and Nasdaq Baltic:

Nasdaq Nordic refers to the Nordic exchanges and the clearing house:

- Nasdaq Stockholm AB
- Nasdaq Copenhagen A/S
- Nasdaq Helsinki Ltd
- Nasdaq Iceland h.f
- Nasdaq Oslo ASA
- Nasdaq Clearing AB

Nasdaq Baltic refers to the Baltic exchanges:

- Nasdaq Tallinn AS
- Nasdaq Riga AS
- AB Nasdaq Vilnius

The document is valid for the following legal entities:

Legal entity	**Markets**
Nasdaq Stockholm AB	Stockholm Equities (including Oslo equities) Stockholm Derivatives market (including derivatives on Swedish, Danish, Finnish and Norwegian equities and indices) Stockholm Fixed Income
Nasdaq Copenhagen A/S	Copenhagen Equities Copenhagen Fixed Income
Nasdaq Helsinki Ltd	Helsinki Equities Helsinki Fixed Income
Nasdaq Iceland h.f.	Iceland Equities Iceland Fixed Income
Nasdaq Tallinn AS	Tallinn Equities Tallinn Fixed Income

Nasdaq Riga AS	Riga Equities Riga Fixed Income
AB Nasdaq Vilnius	Vilnius Equities Vilnius Fixed Income
Nasdaq Oslo ASA	Commodity Derivatives

Legal entity	**Clearing of:**
Nasdaq Clearing AB	Stockholm Equity and Index derivatives (including derivatives on Swedish, Danish, Finnish and Norwegian equities and indices) Stockholm Fixed Income derivatives (including derivatives on Swedish, Danish and Norwegian debt securities) Commodity derivatives

This document applies to the operation of the following systems:

System	**Markets**
INET Nordics Trading system for the Nordic and Baltic equities markets.	Stockholm Equities (including Oslo equities) Copenhagen Equities Helsinki Equities Iceland Equities Tallinn Equities Riga Equities Vilnius Equities
Genium INET Trading Trading system for the fixed income, and the commodity markets.	Stockholm Fixed Income Copenhagen Fixed Income Helsinki Fixed Income Iceland Fixed Income Tallinn Fixed Income Riga Fixed Income Vilnius Fixed Income Commodity Derivatives
NDTS (Nordic Derivatives Trading System) Trading system for the derivatives markets.	Stockholm Equity and Index Derivatives on Swedish, Danish, Finnish and Norwegian equities and indices
Genium Market Info Market data distribution system, for the market data product Genium Consolidated Feed (GCF). GCF disseminates consolidated real-time data from all Nasdaq Stockholm source systems.	Market data from all above markets

System	**Products**
Genium INET Clearing Clearing system for the equity, index, fixed income and commodity derivatives.	Stockholm Equity and Indices derivatives (including derivatives on Swedish, Danish, Finnish and Norwegian equities and indices)

	Stockholm Fixed Income derivatives (including derivatives on Swedish, Danish and Norwegian debt securities) Commodity derivatives

System	Products
CMS Collateral management system for the equity, index, fixed income and commodity derivatives.Safekeeping of securities posted as collateral to Nasdaq Clearing.	Stockholm Equity and Indices derivatives (including derivatives on Swedish, Danish, Finnish and Norwegian equities and indices) Stockholm Fixed Income derivatives (including derivatives on Swedish, Danish and Norwegian debt securities) Commodity derivatives
CMS WEB Web front end used by customers to access custody-related information. Through the CMS Web application, a user can access custody-related information including complete management of collateral. The CMS Web application also holds margin requirements and collateral evaluation information from the clearing system	Stockholm Equity and Indices derivatives (including derivatives on Swedish, Danish, Finnish and Norwegian equities and indices) Stockholm Fixed Income derivatives (including derivatives on Swedish, Danish and Norwegian debt securities) Commodity derivatives

1.2 Document Objectives

This document describes the routines, organizations and arrangements that apply for maintaining continuity of business, key operation of Nasdaq's trading, clearing and other relevant systems in the event of disruption. It explains the Nasdaq organization for managing system disturbances, emergency and crisis situations, how the Business Continuity Plan is applied, and what features the Disaster Recovery sites offer. Furthermore it describes load testing and failover functionality, as well as testing performed to maintain the arrangements above.

The purpose of the document is to provide information for audits or queries from external organizations.

1.3 Audience

The intended audience for this document is participants, information vendors, and regulatory or supervisory bodies.

2 Introduction

It is of utmost importance for Nasdaq to provide solid and robust systems and procedures for the operation of the markets; including trading, clearing and other relevant systems. Any system disturbance or emergency must be addressed and resolved within the shortest time possible.

As a consequence, Nasdaq has made extensive efforts and spent significant resources on dedicated organizations, routines and system solutions to maintain continuity of business and minimize the impact of system disturbances or emergencies.

3 Emergency Management

Nasdaq has a 24/7 organization ready to act in case of incidents or emergencies affecting Nasdaq's systems, facilities and staff. The organization includes Incident Management, Emergency Response and Crisis Management. Business Continuity and Disaster Recovery Plans can be initiated on several levels.

4 Disaster Recovery

The Disaster Recovery Plan (DRP) is not a single document but consists of plans for each Nasdaq Nordic critical system platform, named Emergency Recovery Manuals. In this document the Emergency Recovery Manuals are collectively referred to as the DRP. The DRP contains procedures for recovery and continuation of systems and services used by Nasdaq Nordic. The DRP focuses on the technology that supports critical business processes.

4.1 System Redundancy and Failover

Nasdaq's trading and clearing systems are designed to provide redundancy and failover functionality. The failover solution depends on the type of system and component involved. This is described in the following chapters (see 4.2 - 4.5).

4.2 Primary and Secondary Sites

Nasdaq distributes its production systems on two separate sites with independent infrastructure, including their own power supply in order to ensure protection from power grid blackouts. The primary site is located in the Stockholm area, approx. 30 km from the secondary site. The secondary site acts as a standby site, where systems and processes can be promoted to run as primary. From a connectivity standpoint the sites are equal. Customers are able to connect to either/both the primary or secondary site, thus being able to reduce their risk and lessen the impact of a system disturbance affecting one site. Both locations have a high security level both in terms of physical protection from fire or water etc., as well as any unauthorized access or other external threats.

4.3 System Failover Procedures

In the event of a serious system disturbance, making the primary site unable to continue operating, system operation will need to failover to the secondary site. The failover procedure differs between systems; it is partly manual for INET, Genium INET,CMS and NDTS, but automatic for Genium Market Info. Failover functionality is divided into failover of back-end systems or components thereof, and failover of customer connections. Again, the behavior is different depending on which system and which protocols/API that are affected. Below is a concise description of the failover functionality per system and protocol/API.

4.3.1 INET Nordics

The INET Nordic central system components run on the primary site. The central systems on the secondary site are in hot standby mode, meaning that data is mirrored and sequencing synchronized in real time. The FIX, OUCH and ITCH protocol connectors are active and available on both sites. OUCH and ITCH allow concurrent logons to primary and secondary site, and FIX allows logon to either primary or to secondary port at a time.

4.3.1.1 FIX

The FIX protocol offers one FIX account use of ports on the primary or on the secondary site one at a time. FIX solution is hot-hot, meaning that FIX ports on both sites are on a listening state, and an instant failover with synchronized sequencing between primary and secondary site is available at any time. Failover is a client-initiated process, and a logon made toward the secondary port will force a logoff if there is a client connected to the primary port (or vice versa). Customers are advised to use the ports on the primary site for the lowest latency.

In the event of a primary site failure, the FIX ports on the secondary site will not be possible to use until the routing engine is running in primary mode on the secondary site.

4.3.1.2 OUCH

The OUCH protocol offers one OUCH account concurrent use of ports on the primary and secondary site. Both OUCH ports will accept orders and cancel requests, and outbound messages will be sent on each port. Customers are advised to use the ports on the primary site for the lowest latency. In this configuration, a failover will be seamless as the secondary connection is immediately available.

In the event of a primary site failure, the OUCH ports on the secondary site will not be possible to use until the matching engine is running in primary mode on the secondary site.

4.3.1.3 ITCH

The ITCH protocol offers one ITCH account concurrent use of ports on the primary and secondary site. Market data messaging can be received on both ITCH ports. Customers are advised to use the ports on the primary site for the lowest latency. In this configuration, a failover will be seamless as the secondary connection is immediately available.

In the event of a primary site failure, the ITCH ports on the secondary site will not be possible to use until the matching engine is running in primary mode on the secondary site.

4.3.1.4 Co-Location services

Co-location customers have both the primary and the secondary ports located on the primary site. These customers are offered to enhance their Business Continuity plans by purchasing co-location cabinets and power at the secondary (i.e. disaster recovery) site.

In the event of a primary site failure, the FIX, OUCH and ITCH ports on the disaster recovery site will not be possible to use until the routing and/or matching engine are running in primary mode on the disaster recovery site.

4.3.2 Genium INET

The Genium INET central system components run on the primary site. The central systems on the secondary site are in hot standby mode, meaning that data is mirrored and sequencing synchronized in real time. The OMnet Gateways are active and available on both sites.

4.3.2.1 OMnet

OMnet Gateways offers redundancy in two layers. The customers connect to single IP and port on a load balancer, which distributes the connection to one out of several physical OMnet Gateway behind it.

An individual OMnet Gateway failure will lead to loss of service for the customers connected to it. When the customer reconnects, the load balancer will direct the connection to another OMnet Gateway.
A failure of the connection between the OMnet Gateway and the transaction router that connects to the central system will cause a failover to another transaction router. The failover is automatic.

In the event of a primary site failure, customers will need to connect to the secondary site.

4.3.2.2 FIX

FIX failover is available in two phases, 1) between FIX gateways on the primary site, and 2) if the primary site is unavailable, to the secondary site:

The FIX gateways on the primary site are configured in pairs. Both FIX gateways in a pair are hosting primary connections. The corresponding secondary port is configured on the other FIX gateway. Customers are only able to connect to the primary port. In the event of a FIX gateway failure, the secondary ports will be enabled for connection. The FIX sequence numbers are shared between the FIX gateways, enabling a customer to continue on the secondary connection.

In the event of a primary site failure, the FIX gateways on the secondary site will be enabled for customer connections. Customers would need to connect to their primary port on the secondary site. The FIX gateways are in cold standby, meaning that sequence numbers from the primary site are not known, The FIX sessions are created as new sessions and customers need to reset the sequence numbers to 1. There are no secondary FIX gateways on the secondary site.

4.3.2.3 ITCH

The ITCH protocol offers one ITCH account concurrent use of ports on the primary and secondary site. Market data messaging can be received on both ITCH ports. Customers are advised to use the ports on the primary site for the lowest latency. In this configuration, a failover will be seamless as the secondary connection is immediately available.

In the event of a primary site failure, the ITCH ports on the secondary site will not be possible to use until the matching engine is running in primary mode on the secondary site.

4.3.2.4 Co-Location services

Co-location customers have both the primary and the secondary ports located on the primary site. These customers are offered to enhance their Business Continuity plans by purchasing cabinets and power at the secondary (i.e. disaster recovery) site.

OMnet is available on both sites. In the event of a primary site failure, the FIX and ITCH ports on the disaster recovery site will not be possible to use until the routing and/or matching engine are running in primary mode on the disaster recovery site.

4.3.3 NDTS

The NDTS Nordic central system components run on the primary site. The central systems on the secondary site are in hot standby mode, meaning that data is mirrored, and sequencing synchronized in real time. The FIX and OUCH protocol connectors are active and available on both sites.

4.3.3.1 FIX

The FIX protocol offers one FIX account use of ports on the primary or on the secondary site one at a time. FIX solution is hot-hot, meaning that FIX ports on both sites are on a listening state, and an instant failover with synchronized sequencing between primary and secondary site is available at any time. Failover is a client-initiated process, and a logon made toward the secondary port will force a logoff if there is a client connected to the primary port (or vice versa). Customers are advised to use the ports on the primary site for the lowest latency.

In the event of a primary site failure, the FIX ports on the secondary site will not be possible to use until the routing engine is running in primary mode on the secondary site.

4.3.3.2 OUCH

The OUCH protocol offers one OUCH account concurrent use of ports on the primary and secondary site. Both OUCH ports will accept orders and cancel requests, and outbound messages will be sent on each port. Customers are advised to use the ports on the primary site for the lowest latency. In this configuration, a failover will be seamless as the secondary connection is immediately available.

In the event of a primary site failure, the OUCH ports on the secondary site will not be possible to use until the matching engine is running in primary mode on the secondary site.

4.3.3.3 ITCH

The ITCH protocol offers one ITCH account concurrent use of ports on the primary and secondary site. Market data messaging can be received on both ITCH ports. Customers are advised to use the ports on the primary site for the lowest latency. In this configuration, a failover will be seamless as the secondary connection is immediately available.

In the event of a primary site failure, the ITCH ports on the secondary site will not be possible to use until the matching engine is running in primary mode on the secondary site.

4.3.3.4 Co-Location services

Co-location customers have both the primary and the secondary ports located on the primary site. These customers are offered to enhance their Business Continuity plans by purchasing co-location cabinets and power at the secondary (i.e. disaster recovery) site.

In the event of a primary site failure, the FIX, OUCH and ITCH ports on the disaster recovery site will not be possible to use until the routing and/or matching engine are running in primary mode on the disaster recovery site.

4.3.4 Genium Market Info

Genium Market Info (GMI) offers concurrent connections to receive the Genium Consolidated Feed. The Genium Market Info central system runs as a primary instance on the primary site, with a secondary instance on the secondary site. Data is replicated real time to the secondary instance, making the Genium Consolidated Feed available to customers connecting to either site.

INET, Genium INET and GIC are the main sources of raw market data to Genium Market Info. The services on the Genium Market Info central system are separated per source, enabling backend redundancy on a per source basis. As an example, INET and GIC could be sources from one site, while Genium INET could come from the other site. Irrespectively, the Genium Market Info system and hence the Genium Consolidated Feed is available on both sites.

4.3.4.1 TIP

Genium Market Info offers concurrent connections to receive the Genium Consolidated Feed through the TIP protocol.

4.3.5 CMS

The CMS system is designed to provide redundancy and failover functionality.
The CMS central system components run on the primary site. The central systems on the secondary site are in hot standby mode.

4.4 Testing Site Functionality and Failover

As a baseline, the current exchange and clearing systems have undergone thorough failover tests as part of the pre-production integration tests.
To exercise procedures and safeguard against possible errors in configuration, full primary site failover tests in the production systems are performed on a yearly basis.
For systems with linear development, central system component failover tests are performed as part of the required testing in conjunction with a major software release. Major releases are typically done 1 – 4 times per year. Testing does not interfere with normal exchange trading activity.

4.5. Customer Failover Testing

Failover functionality is available for all protocols/API. As mentioned in 4.2 and 4.3, customers can connect to either or both of the primary and secondary sites. It is important that customers can verify that their applications and their failover arrangements work as expected. To what extent this can be done in the production system depends on the type of system they connect to.

Customers are recommended to implement failover capacity in their applications. Certification of application failover capacity is offered but it's not a mandatory requirement.

4.5.1. INET Nordics

Full site failover tests in the INET Nordic production systems are performed on a yearly basis. These tests are both internal as well as a yearly offered external opportunity for members.

Customers are advised to test failover procedures in the INET Nordic test system (NTF). System generated failover events are performed according to a weekly schedule. For the current failover setup please check schedule on the member extranet.

4.5.2. Genium INET

Full site failover tests in the Genium INET production system are performed on a yearly basis; participants and the financial market infrastructure are invited to test connectivity.

Customer failover testing can be performed and verified by the customers by dropping the connection to the primary site. If a customer should wish to simulate a failover without their own intervention, they can contact Nasdaq business operations for a forced shutdown of the chosen connection.

4.5.3. NDTS

Full site failover tests in the NDTS production systems are performed on a yearly basis. These tests are internal as well as a yearly offered external opportunity for members.

Customers are advised to test failover procedures in the NDTS test system (NTF). System generated failover events are performed according to a weekly schedule. For the current failover setup please check schedule on the member extranet.

4.5.4. Genium Market Info

Full site failover tests in the GMI production systems are performed on a yearly basis. These tests are internal.
Genium Market Info offers concurrent connections to receive the Genium Consolidated Feed. Customers are recommended to connect to both sites in order to not lose any data. Failover can be tested and verified by customers by shutting down their own primary connections and switch to receiving data from the secondary connection, or in case of only connecting to the primary, reconnect to the secondary site. If a customer should wish to simulate a failover without their own intervention, they can contact Nasdaq business operations for a forced shutdown of the chosen connection.

4.5.5. CMS

Full site failover tests in the CMS production system are performed on a yearly basis; clearing participants are invited to test connectivity for CMS WEB.

5. Business Continuity Plan

Nasdaq Business Continuity Plan documentation (BCP) sets forth objectives and procedures for maintaining continuity of business and keeping business critical functions operating in a contingency mode in the event of an emergency situation. This includes procedures for relocation to the Contingency Office.

The complete BCP consists of a number of detailed documents and procedures describing:

- All business-critical processes
- Business impact analysis
- Internal and external communication details
- Evacuation and relocation plans
- Strategies for outage scenarios
- Test procedures and for different scenarios and Contingency Office

5.1. Contingency Office

In case of an emergency situation resulting in evacuation of the Nasdaq offices, the business operation will relocate to the relevant Contingency Offices depending on which unit is affected. The office facilities and equipment is configured for maintaining the business operations with limited staffing. In an emergency situation additional operational personnel can log in and work from their homes or other location via their laptops and VPN connections.

5.2. Critical Business Processes

A thorough analysis has been performed to identify a number of business-critical processes such as, but not limited to: technical support, surveillance and operations; trade support; trading surveillance; clearing, settlement, collateral and risk management. For each process the maximal acceptable outage time has been decided and deadlines and fixed delivery schedules have been determined.

5.3. Business Impact Analysis

Business Impact Analysis (BIA) assessment determines and evaluates the potential effects of an interruption to business-critical processes as a result of disaster, accident or emergency. In addition to establishing acceptable outage times for each process, each risk event has a response plan outlining how to recover and uphold the process. BIA assessment also includes critical business processes in each location, as well as systems and applications supporting these processes.

5.4. Testing of the Contingency Office

To ensure that all business-critical processes can be performed from the Contingency Office, all relevant business applications have been installed on a number of desktop computers. Capacity to perform critical processes from Contingency Office together with operability of hardware and software are tested bi-annually. Employees handling these processes visit the site on a rotating basis and execute critical routines and verify the function of relevant hardware and software. Any issues detected during the testing are reported and resolved.

5.5. Communication Plans

In order to ensure regular updates to both internal and external parties in the event of a disaster, communication rules and processes are included and aligned in all emergency response and crisis management plans. It constitutes a framework for internal and external communication, and although the applicability will vary depending on the situation, this includes:

- Internal communication relating to:
    - Emergency Response Team
    - Crisis Management Team
    - Line management
    - Internal Support Functions
    - Affected staff

- External communication relating to:
    - Customers (including members, vendors and listed companies)
    - Contractors and suppliers
    - Media
    - Authorities
    - Regulators
    - Central Banks
    - CSD’s
    - CCP’s
    - Industry organizations

5.6. Education and Training of Staff

All staff belonging to Incident Management, Emergency Response and Crisis Management organizations undergo training in the relevant procedures, and periodically participate in tests and exercises. Line managers, supported by Risk Officers/Group Risk Management, are responsible for training staff on the BCP procedures.