

BUSINESS CONTINUITY MANAGEMENT

Disclosure

2026



TABLE OF CONTENTS

Abstract.....	3
1 CONTINUITY STRATEGY	4
1.1 Business Continuity Approach	5
1.1.1 IT Systems Architecture	5
1.1.2 Staff distribution	6
2 CONTROL MEASURES	7
2.1 Risk control measures	8
2.1.1 Preventive measures	8
2.1.2 Reactive measures	9
2.1.3 Roles and responsibilities	9
3 TESTING	10
3.1 Testing and exercising.....	11
4 Faq	12
4.1 Frequently Asked Questions	13

Abstract

MTS has developed and endorsed a Business Continuity Management System ("BCMS") that essentially defines how MTS will respond to events that significantly disrupt our business. Therefore, the scope of this document is to outline the most relevant aspects of our BCMS.

In short, MTS plans to quickly recover and resume business operations after a significant business disruption and respond by safeguarding its employees and property, making a financial and operational assessment, protecting the firm's books and records, and allowing our customers to transact business. Our Business Continuity Plan ("BCP"), in particular, is designed to permit our firm to resume operations as quickly as possible, given the scope and severity of the significant business disruption.

MTS Business Continuity arrangements, as described further down in this document, address, among others: data backup and recovery; all mission critical systems; financial and operational assessments; alternative communications with customers, employees, and regulators; alternate physical location of employees, including remote working (work from home, smart working) in case of prolonged unavailability of our offices; critical supplier, regulatory reporting.

Very importantly, MTS is also subject to and complies with a number of regulations and technical standards pertaining to business continuity, within different jurisdictions (e.g. DORA, MiFID II RTS 7, the Bank of Italy Market Infrastructure Business Continuity Guidelines, and CONSOB Regolamento Mercati).

Contacting Us – If, after a significant business disruption you cannot contact us as you usually do at [+44 (0)20 7076 0000 (London) +39 02 72426945 (Milan) / mts.clientservices@euronext.com], you should call our alternative number: +39 335 1007014.

For more information – If you have questions about our business continuity planning, you can contact us at mts.clientservices@euronext.com.

Note: when used in this document "MTS" is deemed to refer to MTS S.p.A., MTS France, EuroMTSLimited and MTS SEF Inc.

1 CONTINUITY STRATEGY

1.1 Business Continuity Approach

MTS Business Continuity Management System ("BCMS") is a critical component of its enterprise resiliency strategy and is designed to plan for, respond to, and recover from business interruptions, with a view to minimize their impact and facilitate service continuity both within recovery time objectives and based on prioritization of business objectives and operations. MTS's BCMS is designed in accordance with applicable regulatory requirements, including Regulation (EU) 2022/2554 (DORA), MiFID II and its implementing Regulation (EU) 2017/578 (RTS 7), the Bank of Italy Market Infrastructure Business Continuity Guidelines (Provvedimento del 22 dicembre 2017), and CONSOB Regolamento Mercati, as well as international standards and industry best practices including ISO 22301.

Amongst the other things, this is made possible by two main elements of a technical and organisational nature: the architecture of our IT systems and the distribution of the MTS staff involved in service delivery and business.

1.1.1 IT Systems Architecture

MTS' IT systems are based on a redundant architecture distributed across two Data Centres in two different geographical location. The data centers are setup in a warm-standby model, and in the event of a full (or partial) primary site failure all the services or parts of them can be activated from the secondary site. MTS targets a Recovery Time Objective (RTO) of within 2 hours and a Recovery Point Objective (RPO) close to zero for its critical services.

The 'real time' data replication, in addition to enabling prompt re-starts in the event of disaster recovery (RTOs within 2 hours), ensures maximum back-up of all production data at both operating locations (RPOs close to 0).

In any case, MTS operates a highly available service that has full redundancy and resilience built within its primary data center. It can withstand the loss of multiple components with minimal interruption, thus minimising the likelihood of having to resort to the secondary site.

New releases are always promoted in a dedicated test environment, prior to production, in order to assess the adequacy of processing capacity and of guarantee system.

1.1.2 Staff distribution

The central processing systems at both primary and secondary locations are continuously active, and monitored.

As suggested by applicable guidelines, in the event of unavailability of an MTS office, MTS staff can operate from alternative sites, such as other offices located in other geographical areas. MTS staff can also work from home or remotely from alternative locations, in secure conditions.

Both application development and systems management staff can work on a mobile basis with suitable security and encryption procedures for technical, application and “production support” interventions. For this purpose, the staff receives automatic reports when the central systems detects a level of severity exceeding set thresholds.

2 CONTROL MEASURES

2.1 Risk control measures

MTS has adopted a BCM framework with a number of risk control measures to ensure Business Continuity objectives are met:

- **Preventive measures**, capable of reducing both likelihood and impact of possible incidents;
- **Reactive measures**, capable of restoring the processes provided quickly enough to avoid negative consequences for the financial system.

2.1.1 Preventive measures

These measures include:

- **Business Impact Analysis (BIA)**, that identifies, quantifies and qualifies the critical processes relevant for business continuity and determines the impacts which may be caused in case of lack of availability of the resources related to those processes. The BIA is carried out following a detailed mapping of MTS business processes.
- **Business Continuity Risk Analysis**, to identify so-called Single Points of Failure, i.e. risk elements that can jeopardize recovery of operations. Counter-measures are identified in order to ensure recovery within the desired timeframe.
- **Monitoring and measurement** of the Business Continuity Management System.

The Business Continuity arrangements of MTS and its Business Continuity Management System, are subject to internal revision and internal and external yearly audits to assess its suitability for company requirements, the changes in architecture and the revised continuity management techniques.

Furthermore, MTS is subject to and complies with a number of regulations and technical standards pertaining to business continuity, within different jurisdictions (e.g. MiFID RTS 7, Bank of Italy Market Infrastructure Business Continuity Guidelines, etc).

MTS's Business Continuity and Disaster Recovery arrangements are subject to annual independent review by the Euronext Group Internal Audit function. The most recent audit, conducted in November 2025, returned an overall Satisfactory rating. The most recent Disaster Recovery test, conducted in May 2026, confirmed that all success criteria were met, including an RTO of under 2 hours and an RPO close to zero achieved.

2.1.2 Reactive measures

These measures include:

- **Incident Management Procedure**, which helps the relevant teams of MTS to investigate, record and resolve service interruptions or malfunctionings.
- **Crisis Management Procedure**, which has predefined steps to involve and communicate with several audience groups during a crisis event. These groups include (but are not limited to) staff, executive management, clients, critical third-party service providers, authorities, regulators and the public.
- **Disaster Recovery Plan (DRP)**, which focuses on the availability or impact to the company's data centers, systems and servers.
- **Business Continuity Plan (BCP)**, which documents procedures for responding to a disruptive incident and how MTS will continue or recover its critical activities within a predetermined timeframe. It covers the following risk scenarios:
 - Unavailability/denial of access to work place;
 - Unavailability of critical IT services;
 - Unavailability of critical staff;
 - Unavailability of critical third-party service providers
 - Cyber incidents affecting the availability, integrity or confidentiality of ICT systems, including ransomware and supply chain attacks.

2.1.3 Roles and responsibilities

MTS has defined clear roles and responsibilities to ensure an effective functioning of Business Continuity activities and oversight.

Main roles include:

- Crisis Management Team;
- Business Continuity Management Team;
- Business Continuity Manager;
- Business Continuity Coordinators/ Process Owners;
- Critical Staff;
- Critical 3rd Party Providers.

Ultimate accountability for the BCMS rests with the Board of Directors, which approves the Business Continuity strategy and is informed at least annually of the outcomes of testing and internal review.

3 TESTING

3.1 Testing and exercising

Regular testing takes place throughout the year as per policy; this includes a large number of tests that simulate the unavailability of IT infrastructures as well as the unavailability of staff, buildings and critical providers.

The following tests/exercises are part of the periodic testing schedule:

- Staff notification test (quarterly);
- Remote access test (quarterly);
- Crisis Management/Escalation process test (yearly);
- Workload shift exercise (yearly);
- Systems Disaster Recovery tests (yearly);
- Plan Walkthrough (yearly).

In addition, MTS conducts or participates in threat-led penetration testing exercises where required under DORA, and documents test results in accordance with applicable regulatory reporting obligations.

MTS also participates in external market-wide exercises (e.g. Bank of Italy CODISE).

4 FAQ

4.1 Frequently Asked Questions

Q1 What is the scope of MTS's Business Continuity Management System?

MTS's BCMS covers all critical business processes and supporting ICT systems across its market infrastructure services. It applies to MTS S.p.A., MTS France, EuroMTS Limited and MTS SEF Inc., and addresses disruption scenarios including facility unavailability, ICT system failures, staff unavailability, and critical supplier disruption.

Q2 What are MTS's Recovery Time and Recovery Point Objectives?

MTS targets a Recovery Time Objective (RTO) of within 2 hours and a Recovery Point Objective (RPO) close to zero for its critical services, consistent with applicable regulatory standards including Mifid2 and the Bank of Italy Market Infrastructure Business Continuity Guidelines.

Q3 What regulations govern MTS's business continuity arrangements?

MTS's BCMS is designed in compliance with applicable laws and regulations, including: Regulation (EU) 2022/2554 (DORA); MiFID II and its implementing Regulation (EU) 2017/578 (RTS 7); the Bank of Italy Market Infrastructure Business Continuity Guidelines (Provvedimento del 22 dicembre 2017); and CONSOB Regolamento Mercati. MTS monitors regulatory developments across all jurisdictions in which it operates to maintain ongoing compliance.

Q4 How frequently does MTS test its continuity arrangements?

MTS conducts a structured programme of tests throughout the year, including quarterly staff notification and remote access tests, and annual crisis management, workload shift, disaster recovery, and plan walkthrough exercises. MTS also participates in external market-wide exercises, including the Bank of Italy CODISE exercise.

Q5 Can I participate to the annual Disaster Recovery test on MTS Trading platforms?

Yes, Markets Participants, ISV and SW vendors are strongly encouraged to attend and actively participate in the DR exercise.

Q6 What is MTS's approach to managing third-party and supplier risk?

MTS assesses the business continuity arrangements of its critical suppliers as part of its vendor risk management process, both at onboarding and on an ongoing annual basis for identified critical third-parties. Contractual requirements for continuity and recovery are established with critical third-party providers, in line with DORA requirements on ICT third-party risk management.

Q7 Who is responsible for MTS's Business Continuity programme?

The Business Continuity Manager, operating within the MTS IT Governance team, has operational responsibility for maintaining and updating the BCMS. The Crisis Management Team leads response activities during a disruption. Ultimate accountability rests with the Board of Directors, which approves the continuity strategy and receives annual reporting on BCMS performance.

Q8 How can clients contact MTS during a significant business disruption?

Clients may use the following contact points:

- London: +44 (0)20 7076 0000
- Milan: +39 02 72426945
- Alternative: +39 335 1007014
- Email: **mts.clientservices@euronext.com**

For further information on MTS's Business Continuity arrangements, please contact **mts.clientservices@euronext.com**.

Q9 How do MTS communicate with its external stakeholders during a significant business disruption?

MTS endeavour to notify its external stakeholders as soon as possible via email and through updates of its corporate website **www.mtsmarkets.com** . Regular status updates will be communicated via the same means.

To request your email address to be included in the relevant Distribution List(s), please contact **mts.clientservices@euronext.com**.



www.mtsmarkets.com