Business Continuity Policy

Version	5.0
Version Date	5 June 2026
Approved by	Board of Directors of OMIClear
Classification	Public

Versions Index

Date	Version	Description of the Modifications
2012/12/07	1.0	Initial version
2014/04/24	1.1	Changes to the Crisis Management Team in accordance with the Board of Directors' decision of 24 April 2014
2014/11/27	2.0	Full revision of the document
2016/10/17	2.1	Regular revision. Inclusion of the Chief Risk Officer (CRO)
2018/07/26	2.2	Regular revision. Contact info update
2019/10/16	3.0	Full Revision, including the translation of the document into Portuguese
2022/10/26	3.1	Regular Revision.
2024/11/26	4.0	Review and alignment with Commission Delegated Regulation (EU) 2024/1774 of 13 March 2024, supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to regulatory technical standards specifying the tools, methods, processes, and policies for ICT risk management and the simplified ICT risk management framework (DORA). Addition of the "annual" frequency in section 4.
2026/06/05	5.0	Specification of the various BCMS operational activities and review of the responsibilities assigned to each role involved.

Table of Contents

1. Purpose, Scope, and Audience

This Policy aims to establish the principles and rules applicable to OMIClear's Business Continuity Management, in order to ensure the continuity of its critical activities, minimizing the impact of disruptive incidents, and promoting organizational resilience.

This Policy falls within the scope of the Business Continuity Management System (BCMS) and applies to all functions performed by OMIClear whose unavailability may significantly impact its operations.

The audience of this Policy includes all OMIClear stakeholders (internal and external) involved in the BCMS.

2. Related Documents

- ISO 22301:2019 Standard;
- ISO/IEC 27002:2022 Standard;
- Regulation (EU) No 648/2012 of the European Parliament and of the Council of 4 July 2012;
- Commission Delegated Regulation (EU) No 153/2013 of 19 December 2012;
- Commission Delegated Regulation (EU) 2024/1774 of 13 March 2024;
- Decree-Law No. 357-C/2007 of 31 October, as republished by Decree-Law No. 109-H/2021 of 10 December;
- Information Security Policy.

3. Business Continuity Management

3.1 Objetive

OMIClear's strategic objective is to be equipped with a comprehensive set of tools to ensure its ability to provide an adequate response to a disruptive incident affecting its critical business functions and the supporting resources on which the normal operation of the organization depends, thereby minimizing the potential negative impacts such situations may cause to the organization.

To achieve this objective, OMIClear is committed to implementing a BCMS based on the ISO 22301:2019 standard, which is interconnected with an Information Security Management System (ISMS), and follows the guidance of applicable European legislation within the scope of MiFID II, namely Delegated Regulation (RTS 7), which concerns organizational requirements applicable to any Regulated Market, as well as Regulation (EU) 2016/1011. In this way, the aim is to ensure the recovery of OMIClear's critical functions within a maximum period of 2 hours, and that the maximum amount of data that may be lost is as close as possible to zero, in accordance with its business model, thus ensuring compliance with regulatory requirements, particularly European, to which OMIClear is subject, such as:

- Regulation (EU) No 1227/2011 of the European Parliament and of the Council;
- Commission Implementing Regulation (EU) No 1348/2014 of 17 December 2014;
- Directive 2014/65/EU (MiFID II) of the European Parliament and of the Council of 15 May 2014;
- Regulation (EU) No 600/2014 (MiFIR) of the European Parliament and of the Council, adopted on 15 May 2014;
- Commission Delegated Regulation (EU) 2017/584 of 14 July 2016;
- Commission Delegated Regulation (EU) 2017/590 of 28 July 2016;

- Regulation (EU) 2016/1011 of the European Parliament and of the Council of 8 June 2016;
- Commission Delegated Regulation (EU) 2024/1774 of 13 March 2024.

3.2 Scope

The scope of the BCMS covers all organizational units, functions, processes, and supporting resources that contribute to achieving OMIClear's strategic and operational objectives.

More specifically, the scope of the BCMS is as follows:

A) Organizational Units

The following organizational units are included within the scope of the BCMS:

- Chairman and Vice-Chairman;
- Chief Operating Officer (COO);
- Clearing Department;
- Risk Department;
- Chief Technology Officer;
- Chief Audit Officer;
- Chief Compliance Officer.

These organizational units are part of OMIClear's organizational structure, as set out in its annual statement accounts.

B) Functions

The scope of the BCMS includes all business functions carried out by OMIClear, including support functions, management, and provision of services.

C) Supporting Resources

The scope of the BCMS includes the following resources that support OMIClear's functions:

- **Facilities:** All facilities where the organization's functions are carried out;
- **Personnel:** All staff members belonging to the Organizational Units and responsible for performing the organization's functions;
- **Support Services:** All support services required for the execution of functions, including equipment, information, ICT infrastructure, service providers, among others.

3.3 BCMS Operationalization

The operationalization of the BCMS involves several stages, namely:

A) Business Impact Analysis (BIA)

This corresponds to the first stage of BCMS operationalization and aims, through impact analyses based on predefined criteria, to identify the critical business functions that support the organization's operations, their supporting resources, and the recovery objectives for those functions.

B) Risk Analysis

Based on the resources identified in the previous stage, this step aims to identify the associated threats and vulnerabilities and to assess the risk of occurrence of disruptive events and the resulting unavailability of the organization's critical resources.

C) Strategies and Solutions

Based on the results of the previous two stages, this step aims to define strategies and solutions structured across three phases of a disruptive event, in particular:

- Before: strategies and solutions to mitigate the risks identified and not accepted by the organization;
- During: strategies and solutions to ensure the continuity of the critical functions identified in the BIA;
- After: strategies and solutions to ensure the return to normal operations.

D) Plans

Based on the strategies and solutions defined for the "during" and "after" phases of a disruptive event, this step aims to establish response plans, detailing the activities to be carried out to achieve the defined strategies and solutions, and the individuals responsible for executing those activities.

E) Exercises and Testing

This stage aims to test the plans defined in the previous step through the simulation of disruptive scenarios, and to validate whether the activities included enable effective recovery from a disruptive event, as well as whether responsibilities are clearly assigned to all involved parties.

3.4 Roles and Responsibilities

3.4.1 Board of Directors

The Board of Directors of OMIClear ultimately holds overall responsibility for the BCMS, and in particular for:

- Approving and ensuring the periodic review of the Business Continuity Policy, Plans, Methodologies, and other supporting BCMS documentation;
- Ensuring the alignment of Business Continuity with OMIClear's strategic objectives;
- Overseeing the effectiveness of the BCMS.

3.4.2 Senior Management

OMIClear's Senior Management, comprising the areas defined in the Government Arrangements Procedure, is responsible for:

- Defining the BCMS strategy and objectives;
- Ensuring that the BCMS is established, implemented, and maintained;
- Ensuring the availability of adequate resources to achieve the objectives;
- Monitoring the performance and effectiveness of the BCMS in order to ensure the achievement of its objectives;
- Ensuring reporting to the Board of Directors on any relevant matters within the scope of the BCMS.

3.4.3 Crisis Manager

The OMIClear Crisis Manager (OMIClear's Chief Operating Officer) is responsible for managing disruptive incidents, namely:

- Deciding on the activation and deactivation of the Business Continuity Plans and the respective Recovery Manuals;
- Coordinating the incident response and recovery activities;
- Ensuring access to alternative facilities and the necessary resources;
- Managing internal and external communications;
- Ensuring coordination with relevant external entities.

3.4.4 Business Continuity Manager

The Business Continuity Manager is responsible for the coordination and operationalization of the BCMS, and is tasked with:

- Coordinating the development and maintenance of the BCMS;

- Defining and maintaining methodologies, procedures, requirements, and specific objectives for BCMS processes;
- Coordinating the execution of the Business Impact Analysis (BIA) and business continuity risk assessment;
- Ensuring the development and updating of the Business Continuity Plans and respective Recovery Manuals;
- Planning and coordinating tests and exercises;
- Promoting training and awareness actions;
- Monitoring the performance and maturity of the BCMS, in order to ensure the achievement of defined objectives;
- Reporting results to senior management.

3.4.5 Business Continuity Management Team

Within the scope of the BCMS implementation, an internal technical team has been established, composed of, at a minimum, the Chief Operating Officer, a representative from Information Systems, and the Business Continuity Manager.

The Business Continuity Management Team is responsible for:

- Proposing to the Board of Directors, for approval, the Business Continuity Policy, Plans, Methodologies, and other supporting BCMS documentation;
- Approving operational documentation related to the BCMS (e.g., Recovery Manuals, Exercise and Test Reports, among others);
- Ensuring the operationalization of the BCMS;
- Adopting and implementing a training plan for all stakeholders involved in the BCMS;
- Adopting and implementing the review and maintenance of the BCMS to ensure that all BCMS procedures remain functional and up to date;
- Monitoring incidents and non-conformities, and identifying the necessary preventive and corrective actions;
- Analysing and preparing Test and Exercise Reports;
- Reviewing the effectiveness of the BCMS at least annually, or whenever a significant change occurs, and preparing the respective Review Report.

3.4.6 Employees

All OMIClear employees are responsible for:

- Complying with all requirements, policies, methodologies and procedures defined within the scope of the BCMS;
- Participating in training sessions and tests, where applicable;
- Reporting incidents or situations that may impact the continuity of OMIClear's functions;
- Performing their duties in accordance with the Business Continuity Plans when activated.

3.4.7 Service Providers

Service providers must:

- Comply with the Business Continuity requirements set out in the Business Continuity Policy and contractually agreed, namely ensuring the agreed service levels are maintained;
- Ensure the existence of appropriate Business Continuity mechanisms;
- Report incidents that may impact the services provided;
- Support and contribute as necessary to the preparation of incident reporting documentation.

4. Validity and Document Management

It is the responsibility of the Business Continuity Manager, as the owner of this Policy, to submit to the Board of Directors any proposals for amendments or updates to this Policy, with its review and approval being the responsibility of the Board of Directors.

This Policy is reviewed at least on an annual basis and, in particular, whenever there is a change in circumstances and whenever legislative or regulatory changes occur, to ensure that it remains current and appropriate in light of applicable standards.

The internal dissemination of this Policy is the responsibility of the Business Continuity Manager, and it shall be available for consultation at all times on the shared network drive, at: O:\53_bSecure\00_Documentos para consulta.

Additionally, the Policy is available for consultation on the OMIClear corporate website.

All OMIClear stakeholders (internal and external) must be aware of this Policy and comply with it within the scope of their specific roles and responsibilities, and contribute to the monitoring and continuous improvement of the BCMS.

In accordance with OMIClear's governance model, the Business Continuity Manager is responsible for monitoring the proper implementation and application of this Policy, compliance with applicable legislation and regulation, as well as the decisions of the Board of Directors in this regard.

During the review and improvement processes, the following must be assessed:

- Whether the objectives established under this Policy have been achieved;
- The effectiveness and adequacy of the Business Continuity Plans and the respective recovery manuals for functions considered critical, based on the results of exercises, tests, or incidents;
- Non-compliances with legislation and regulations, contractual obligations, and other internal organisational documents.