Business Continuity Management

Document Title	EMIR* Article	RTS** Article	Document Class
Business Continuity Management	Art 34	Chapter V	Policy

*EMIR = Regulation (EU) 648/2012 ; ** RTS = Comm. Del. Regulation (EU) 153/2013

Document Information

Document Owner	**Chief Technology Officer (CTO)**
Document Reviewer 1	**Chief Risk Officer (CRO)**
Document Reviewer 2	**Chief Compliance Officer (CCO)**
Document Approver	**General Management**

Document Review Cycle: yearly / on demand

Change Log[1]

Version	Effective Date	Change Description
V1.0	27.07.2016	Initial creation
V2.0	27.08.2018	Translation into English, general revision of the document

[1] The Change log is only used for final versions.

Content

1 Introduction 4

2 Objectives and Measures 4

3 Preventive Measures 5

3.1 Internal Control System 5

3.2 IT requirements 6

3.3 Information Security Policy 6

3.4 Change Management 6

3.5 IT Controls 7

4 Business Contingency and Disaster Recovery 7

4.1 Incident Management 7

4.2 Emergency and Crisis Management 8

4.3 Exceeded Risk Tolerance Procedure (ERT) 9

5 Continuous Improvement 9

1 Introduction

CCP Austria clears all transactions concluded at Wiener Börse AG in trading with CCP-eligible securities. As the central contracting party, CCP Austria stands between buyer and seller and thus assumes the risk of settlement and default for all transactions. By assuming these risks, CCP Austria represents an important part of the Austrian financial market infrastructure and has therefore implemented a comprehensive risk management framework.

To minimise the negative impact on business processes, if a risk materialises, and ensure a minimum level of critical functions a business continuity management, according to Articles 26 and 34 of EMIR and Articles 17 to 23 of RTS 153/2013, is established, implemented, maintained and tested on regular basis.

2 Objectives and Measures

The business continuity measures consist of organizational, procedural, technical and personnel measures that aim to optimally support the proper provision of clearing and risk management services. They allow the recovery of all pending transactions in the event of any disruption and ensure that CCP Austria is able to continue operating smoothly and to fulfill all settlement (delivery and payment) obligations on the scheduled date.

These measures include

- **Preventive measures** (specifications for service providers in contracts and Service Level Agreements (SLAs), Information Security Policy, change management processes, manuals, guidelines, internal control system including business continuity tests),
- **Business contingency & disaster recovery** (emergency & crisis management, distress contacts, incident management, workaround for critical business functions),
- **Continuous improvement** (review after a significant disruption or critical incident).

Consequently, the Business Continuity Management (BCM) focuses on operational and IT-related risks and is – regarding preventive measures – closely linked with or part of CCP Austria's Internal Control System (risk identification and assessment, Business Impact Analysis and Risk Controls).

3 Preventive Measures

3.1 Internal Control System

CCP Austria has designed and implemented an effective, comprehensive and efficient Internal Control System, which determines preventive and detective controls for identified risks of **business and core processes** and serves to minimize operational and other risks. It consists of the following components:

- **Risk Identification and Risk Assessment** to identify and evaluate threats due to operational risks that could lead to the disruption of business or core processes and to identify critical business functions and related systems. The identification and assessment of operational risks are performed together with other risk categories.

- **Business Impact Analysis (BIA)** examines and measures the impact a disruption may have. Its origin and subject matter are closely linked to the risk identification and assessment process.

- **Risk Controls** are preventive measures that reduce the damage from and the probability of operational or IT-related risks. They increase the resistance of the organization against such threats, as well as the robustness and reliability of its business processes and all related IT-systems. Requirements on IT-systems, external providers, the operations of clearing, IT workplaces, Information Security and Change Management are defined below.

3.2 IT requirements

When concluding contractual agreements or Service Level Agreements with external providers (IT-systems, facility management services, etc.) CCP Austria considers specific requirements, such as

- requirements on IT-systems used for clearing services
- requirements on IT-workplaces and other supporting services

3.3 Information Security Policy

CCP Austria maintains a robust Information Security Policy to protect information from unauthorized disclosure and to ensure data accuracy and integrity. The following topics are included in the "Information Security Policy":

- Responsibilities of the Chief Technology Officer as regards Information Security, General Management and employees/contractors/externals
- Physical access control
- System / application access rights management
- Computer & internet
- Mobile phones / tablets
- Outsourcing partners / service providers
- Virus attack or suspicious e-mails
- Data protection and data security
- Clean desk policy

Every internal and external member of staff must agree in writing to CCP Austria's Information Security Policy and the data protection and security provisions.

All external providers must have their own comprehensive Information Security Policies in place. CCP Austria checks carefully if the Information Security Policy complies with the own requirements.

3.4 Change Management

Changes in Business Processes and/or related IT-systems may cause an increased risk of disruptions. To minimize said risk, CCP Austria has implemented a change management

process with clear roles and responsibilities, as well as evaluation, approval and test procedures.

3.5 IT Controls

IT Controls are an integrated part of the general risk controls of CCP Austria's Risk Management Framework with emphasis on periodical testing of connectivity or security related topics/test scenarios, e.g.:

- Annual test of the emergency workplaces
- Annual data centre failover testing
- Quarterly testing of the contingency leased line connection to the Clearing System
- Annual penetration testing (3rd party testing)
- Annual data restore tests
- Quarterly physical access controls
- Annual system / application access revalidation (need-to-know)
- Annual information security refresher

4 Business Contingency and Disaster Recovery

CCP Austria has defined measures, which enable critical functions to recover within two hours, with backup systems ideally starting processing immediately after an incident.

The following procedures were implemented to ensure that business critical functions are properly working in extreme scenarios as well as when an incident occurred:

4.1 Incident Management

Incidents are categorized following the BSI Standard 100-4:

- **Malfunction (low-level incident)** is a temporary outage of processes or correlating resources with none or minimal damage. The problem can be solved within 2 hours (RTO according to BIA) without taking specific measures or no business critical functions were affected and pre-defined exception-handling procedures and manual workarounds are applied. Incidents with higher severity level require the invocation of the emergency management team.

- **Emergency** is an impending/occurring situation that poses an immediate risk with relevant potential financial loss. The incident may not be solved within the RTO without taking specific measures.

- **Crisis** is any event that leads or is expected to lead to an unstable and dangerous situation with limited controllability, uncertain and unpredictable outcome and harm. The public may perceive such an event.

- **Disaster** is a special case of a crisis, where not only CCP Austria is affected. A serious disruption of the functioning of a community (e.g. natural catastrophe). In addition, possible co-operation with aid organizations and public relations might be required.

CCP Austria's Operations and Back Office team manage incidents, supported by the CTO and the external providers according to error and exception handling procedures.

Any incident is immediately reported to the emergency manager on duty or his deputy. The CTO (or his deputy) coordinates the appropriate actions for returning to status quo of operation. The CTO also decides about the classification of an incident as malfunction, emergency, crisis or disaster by taking the defined RTO of the disrupted function into account and activating the appropriate process, e.g. emergency or crisis management.

4.2 Emergency and Crisis Management

An Emergency & Crisis Manual (also referred to as the Emergency Manual) serves the continuation of business (Business Continuity Management, BCM) and contains instructions and precautions to ensure that CCP Austria provides the critical functions of its clearing services in emergency and crisis situations as well.

In particular, the Emergency Manual was established on top of the Business Impact Analysis performed during the implementation of the Internal Control System, which identified the critical business functions of CCP Austria and its associated (business and core) processes (and their risks and controls).

The following measures are implemented in the context of the emergency management:

- **Emergency Management** („Business Contingency Planning“)
  Organization in and measures for emergencies and the related coordination

- **Emergency Exercises** („Business Contingency Testing“)
  Test of the emergency measures

- **Improving Emergency Management** („Continuous Improvement“)
  Regular review and, if necessary, extension of emergency measures and tests, especially for process amendments

4.3 Exceeded Risk Tolerance Procedure (ERT)

In the event of a disaster exceeding CCP Austria's risk tolerance threshold, a specific measure in accordance with the strategic guidelines of the Risk Management Framework of CCP Austria will become effective - the **Exceeded Risk Tolerance Procedure**.

In the course of that, the General Management will assume the supervision of the disaster management, which formerly was managed by the CTO. In coordination with the Supervisory Board and the Shareholders, no new trades will be accepted for clearing, as long as the triggering event persists and no alternative measure has been established. In such a case the General Management also informs the clearing participants, the Vienna Stock Exchange, the OeKB CSD and the financial market authority (FMA)

5 Continuous Improvement

All incidents are logged, regularly reported to the General Management, the CRO and the CCO and are part of the internal quarterly Operational Risk Management Report. Related improvement measures are also included and followed up by the General Management, the CRO and the CTO.

This Policy and the related documents e.g. BIA, Information Security Policy, Emergency & Crisis Manual or operational manuals are reviewed at least once a year or after any significant disruption or critical incident.