Emergency Playbook

Incident Management - Handling and Communication of Outages

Baden-Württembergische Wertpapierbörse

Version: 2.0 – Dezember 2023

Table of contents

1. Introduction

This document provides trading participants an overview on the handling of outages at Baden-Württembergische Wertpapierbörse (BWWB or Exchange) caused by technical incidents, especially with regards to communication with trading participants and the public in case of an outage.

The MiFID II framework, in particular Articles 47 and 48, requires trading venues to ensure their systems are resilient, have sufficient capacity and are able to ensure orderly trading under conditions of market stress. Furthermore, these systems need to be fully tested and subject to business continuity arrangements. Commission Delegated Regulation 2017/584 (RTS 7) further specifies the requirements to ensure trading venues’ systems are resilient and have adequate capacity. These requirements must be taken into account when assessing trading venues’ procedures to deal with market outages, in particular in terms of business continuity arrangements.

BWWB has stable and resilient systems and aims to minimize disruptions and uncertainties for their trading participants. BWWB continuously works on improving business continuity measures and reviews its arrangements periodically. BWWB does its utmost to ensure continuity of trading during normal trading hours.Therefore trading interruptions are rare and unlikely, but nevertheless require an appropriate preparation and response. In the event of a market outage BWWB has established clear procedures to minimize the impact on orders and trading and restore an orderly trading including decisions on trading halts or trade cancellations and communication with stakeholders.

BWWB ensures efficient incident notification to the competent authority without any delay in the event of system disruptions. The provision of the respective information to the responsible competent authority is first of all based on given guidance and templates in accordance with the legal notification obligations of Article 54(2) and Article 31(2) of MiFID II with further clarifications in Article 81 of Commission Delegated Regulation (EU) 2017/565. With this document BWWB provides publicly available information of its setting of notification and communication with further stakeholders, especially with trading participants and the public, in the event of an outage. The processes described in this playbook are reviewed, tested and updated on a regular basis.
This document takes ESMA’s Opinion on market outages into account (final report).

2. Incident Prevention

The trading systems of BWWB are based on a robust and resilient architecture and are continuously improved. Their design is guided by the requirement to ensure data integrity and high availability.

3. Handling of Incidents and (IT-)emergencies

The handling of incidents and (IT-)emergencies at BWWB is in line with the procedures and arrangements of Boerse Stuttgart Group and in particular is based on the following principles:

- Keep markets open as long as they are operating in a fair and orderly manner
- Restore the service as quickly and safely as possible, whilst fulfilling the regulatory responsibilities. This includes securing the consistency between order and trade records at all times and minimising impact on trades
- Communicate appropriately and in a timely manner to internal and external stakeholders
- Carry out a post-event review and take actions to avoid the recurrence of an outage

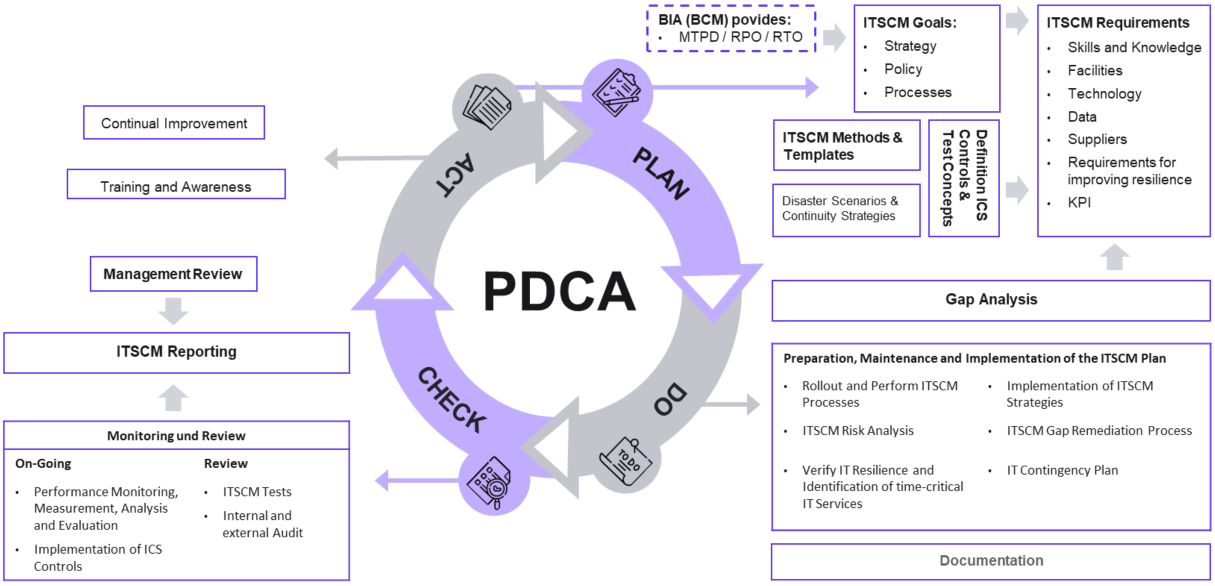
3.1. Incident Management

Boerse Stuttgart Group has pre-defined procedures concerning Incident & Service Request Management und Major Incident Management. The procedures are based on ITIL, a best-practice-framework and the de-facto-standard for an effective IT-Service-Management. The procedures are triggered by the input of an event, service request or incident. The procedures establish clear steps and departments and pre-defined committees, which are to be included, to enable decisions and solution in a timely manner. First of all the input in the incident management system is classified in dependence of its impact and severity and the relevant stakeholders are identified. Based on this analysis the required further measures can be started including internal and external communication.

3.2. ITSCM

The IT Service Continuity Management (ITSCM) of Boerse Stuttgart Group ensures the provision of IT services required to maintain time critical business processes. The risk of failure of IT services for time-critical business processes identified in Business Continuity Management (BCM) is monitored and managed by ITSCM. Furthermore ITSCM coordinates groupwide activities to address these risks and ensures that overarching cooperation between the divisions, affiliates and external IT service providers is covered and operationally effective. This includes the implementation of the required processes in the operational IT units as well as the verification of compliance with the BCM requirements.

Based on the Business Impact Analysis (BIA), the ITSCM derives specifications that IT must fulfill when providing time-critical IT services. The ITSCM is oriented to the ISO 27031 standard "Guideline for the readiness of information and communication technologies for business continuity" of the International Organization for Standardization and methodically uses the recommendation of the Federal Office for Information Security of Germany BSI 200-4.


BIA (BCM) povides:
MTPD / RPO / RTO
ITSCM Goals:
Strategy
Policy
Processes
ITSCM Requirements
Skills and Knowledge
Facilities
Technology
Data
Suppliers
Requirements for improving resilience
KPI
ITSCM Methods & Templates
Definition ICS Controls & Test Concepts
Disaster Scenarios & Continuity Strategies
Continual Improvement
Training and Awareness
Management Review
ITSCM Reporting
ACT
PLAN
DO
CHECK
PDCA
TO DO
Gap Analysis
Preparation, Maintenance and Implementation of the ITSCM Plan
Rollout and Perform ITSCM Processes
Implementation of ITSCM Strategies
ITSCM Risk Analysis
ITSCM Gap Remediation Process
Verify IT Resilience and Identification of time-critical IT Services
IT Contingency Plan
Documentation
Monitoring und Review
On-Going
Performance Monitoring, Measurement, Analysis and Evaluation
Implementation of ICS Controls
Review
ITSCM Tests
Internal and external Audit

The ITSCM process and its roles are located in the operational area of the BCM organizational structure. Preventive and reactive roles are implemented for this purpose.

ITSCM provides preventive measures that prepare for IT contingency situations and enable a rapid response in the event of occurrence. Preventive roles are implemented for this purpose, in which both areas of responsibility and authority to issue instructions are regulated.

Roles of the reactive contingency organization represent a special organizational structure that is only set up temporarily for contingency operations and is intended to ensure rapid information and decision-making paths.

3.2.1 IT Emergency plans

The IT emergency plans contain clear instructions for the restart, emergency operation and recovery of the relevant ITSCM units with time-critical IT services. The orchestration of the IT contingency plans takes place in the IT contingency manual in order to take appropriate account of the dependencies between IT services. This documents the sequence and dependencies between the IT services. The IT emergency manual is therefore the central document for managing an emergency involving IT and for the orderly restart of all IT services. In addition, the IT contingency plans contains the following information:

- The detection, alerting and reporting of incidents
- The restart of the resources required for normal operation
- The continuation of business in a defined emergency operation
- A regulated transition from emergency to normal operation

These are created by the decentralized ITSCM managers of the ITSCM-relevant unit and reviewed annually or at the request of the ITSCM officer.

Article 16 (contingency plan) of COMMISSION DELEGATED REGULATION (EU) 2017584 (supplement to Directive 201465EU) is fully considered and implemented in all IT Emergency plans.

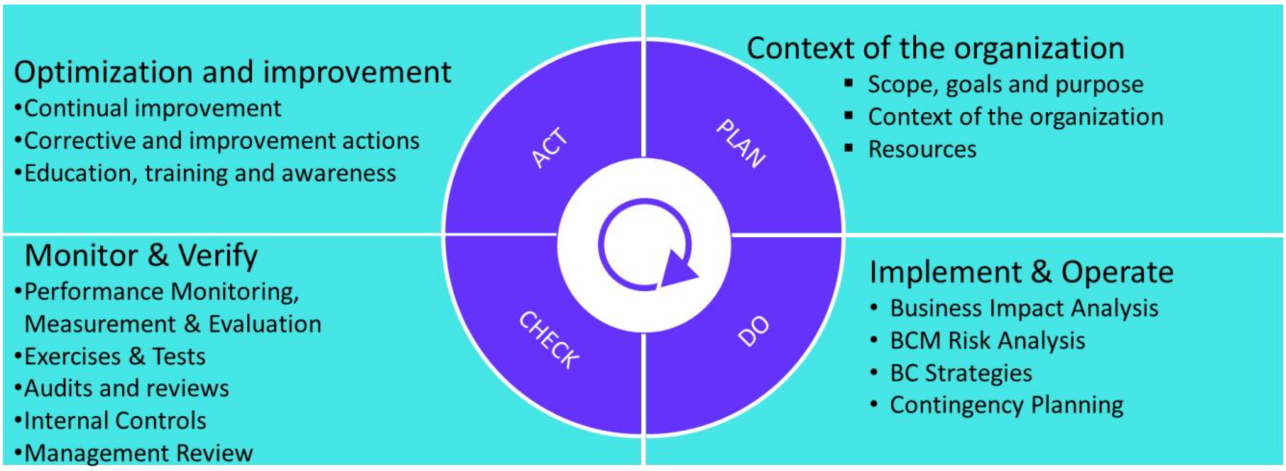
3.2.2 Practice and test

The reactive IT emergency organization, measures for IT emergency preparedness and the IT emergency plans must be regularly checked for their appropriateness, effectiveness and efficiency using IT emergency tests. IT emergency tests must take into account both the testing of individual plans as well as cross-plan scenarios and the associated restart.
The frequency and scope of IT emergency drills are determined in a risk-appropriate manner depending on the availability requirements of the higher-level business process. However, the IT emergency tests fully covers all time-critical IT services on an annual basis.
Another aim of the IT emergency tests is to confirm whether the people involved in implementing the measures have the necessary skills and abilities to implement the defined measures and are aware of their tasks and responsibilities.
The results of the IT emergency tests are documented and evaluated in logs in order to review and further develop the ITSCM process and the emergency plans.

Article 17 (Periodic review of emergency arrangements) of COMMISSION REGULATION (EU) 2017584 (supplement to Directive 201465EU) is fully taken into account and implemented when practicing and testing.

3.3. Business Continuity Management

The PDCA model of the Business Continuity Management System (BCMS) is described below in accordance with ISO 22301 and BSI 200-4. The following figure provides an overview of the BCMS, to which further processes are assigned. The individual processes of the BCMS are explained below and, if necessary, regulated in more detail in separate work instructions.


Optimization and improvement
•Continual improvement
•Corrective and improvement actions
•Education, training and awareness
Context of the organization
▪ Scope, goals and purpose
▪ Context of the organization
▪ Resources
ACT
PLAN
CHECK
DO
Monitor & Verify
•Performance Monitoring, Measurement & Evaluation
•Exercises & Tests
•Audits and reviews
•Internal Controls
•Management Review
Implement & Operate
• Business Impact Analysis
• BCM Risk Analysis
• BC Strategies
• Contingency Planning

3.3.1 Business continuity plans

The business continuity plans (BCP) contain clear instructions for the emergency management of the respective organizational units with time-critical business processes. Within the BCP, the four main BCM failure scenarios:

- (Partial) failure of a site
- Failure of a critical number of employees
- Failure of IT systems or communication infrastructure
- Failure of service providers

are considered with the aim of ensuring that they can be managed in an emergency. Business continuity plans are drawn up by the decentralized BCM managers of the organizational units and reviewed annually or at the request of the BCM nominee.

Article 16 (contingency plan) of COMMISSION DELEGATED REGULATION (EU) 2017584 (supplement to Directive 201465EU) is fully considered and implemented in all business continuity plans.

3.3.2 Practice and test

The reactive emergency response organization, emergency preparedness measures and emergency plans are regularly reviewed for their appropriateness, effectiveness and efficiency by means of exercises and tests. Exercises and tests are taking into account the testing of individual plans as well as complete business interruptions and the associated restart. This also takes into account increasing complexity and changing scenarios. All relevant failure scenarios can also be combined as part of an exercise:

- (Partial) failure of a site
- Failure of a critical number of employees
- Failure of IT systems or communication infrastructure
- Failure of service providers

Furthermore, it is checked whether the people involved in the implementation of the measures have the necessary skills and abilities to implement the defined measures and are aware of their tasks and responsibilities. The results and protocols resulting from exercises and tests are used to review and further develop the BCMS as well as to provide evidence to third parties (e.g. external auditors).

Article 17 (Periodic review of emergency arrangements) of COMMISSION REGULATION (EU) 2017584 (supplement to Directive 201465EU) is fully taken into account and implemented when practicing and testing.

3.4. Crisis Management

The central emergency manual is the basis for emergency and crisis management at Boerse Stuttgart Group.
The procedures documented in the central emergency manual support emergency and crisis response and cover the phases from the occurrence of the damaging event to the restart and continuation of business of time-critical business processes to the return to normal operations.

To this end, the central emergency manual contains instructions for action and tools for avoiding and containing damage and consequential damage through effective and targeted actions within emergency and crisis management.

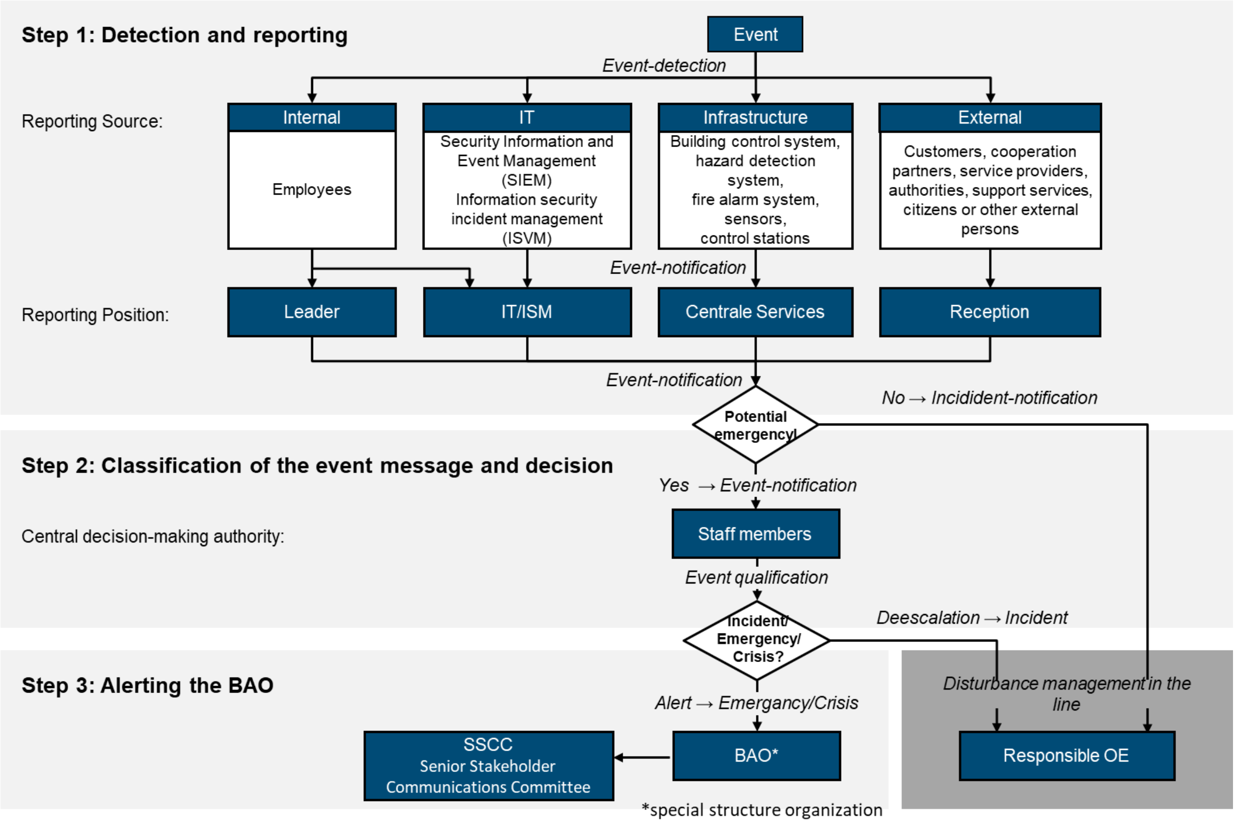
Definitions and explanations of terms relating to business continuity management as well as conceptual and organizational aspects that do not contribute to direct emergency and crisis management are described in the BCM Policy.

The BCM Managers of Boerse Stuttgart Group are responsible for defining and maintaining the specifications of the central emergency manual.
The specifications of Boerse Stuttgart Group described in the central emergency manual are to be reviewed annually and, if necessary ad hoc, by the BCM Manager with regard to their appropriateness. In particular, changes in the organizational structure and findings from exercises and tests are taken into account.

Within the Business Continuity Management of Boerse Stuttgart Group, the following failure scenarios are considered:

- (Partial) failure of a location
- Failure of IT systems or the communication infrastructure
- Failure of a critical number of employees
- Failure of service providers

Damage events can have a variety of causes and are to be handled by the crisis team according to the situation.


Step 1: Detection and reporting
Event
Event-detection
Reporting Source:
Internal
Employees
IT
Security Information and Event Management (SIEM)
Information security incident management (ISVM)
Infrastructure
Building control system, hazard detection system,
fire alarm system, sensors,
control stations
External
Customers, cooperation partners, service providers, authorities, support services, citizens or other external persons
Event-notification
Reporting Position:
Leader
IT/ISM
Centrale Services
Reception
Event-notification
Potential emergency
No → Incidident-notification
Step 2: Classification of the event message and decision
Yes → Event-notification
Central decision-making authority:
Staff members
Event qualification
Incident/ Emergency/ Crisis?
Deescalation → Incident
Step 3: Alerting the BAO
Alert → Emergancy/Crisis
Disturbance management in the line
SSCC
Senior Stakeholder Communications Committee
BAO*
Responsible OE

*special structure organization

The emergency response process follows the following procedure:

- The occurrence of the damaging event marks the point in time when the event is first noticed and becomes apparent.
- This is followed by immediate measures aimed at protecting life and limb and preventing or containing further damage as a result of the damaging event. Situationally, the occurrence of a damaging event may require action and must be initiated before the event escalates to an emergency.
- Alerting and escalation contains how a damaging event should be reported to the previously defined reporting points. The defined reporting points initially assess the event and, if the event is qualified as an emergency/crisis, report it to the central decision-making unit. If this is confirmed, the decision-making authority ensures the described alerting and reporting path.
- The constitution of the special organizational structure (BAO) includes all activities necessary to ensure the BAO's ability to work. This includes the provision of the infrastructure and the necessary equipment.
- The start of the special organization is characterized by the declaration of an emergency/crisis situation. The situation is assessed, and initial measures are defined, implemented and followed up. In parallel, the affected organizational units and defined emergency teams must start implementing business continuity plans to ensure orderly emergency operations.
- The purpose of emergency communications is to collect, verify and process information during the event and to distribute it in a way that is appropriate to the needs and

addressees. In the course of this, prepared regulations and behavioral instructions can be used.

- The restart phase is characterized by the intervention of all necessary measures in order to be able to switch to a pre-defined emergency operation in a structured manner. This includes, for example, the provision of alternative resources or the conversion of processes and activities for a reduced emergency operation.
- Business continuation describes the execution of business operations in emergency mode using, for example, alternative resources and process steps. The use of alternative systems or activities within business processes through planned deferral, modification, or prioritization is provided here.
- Recovery is used to return to normal operations. Recovery here includes all activities from the start of emergency response to de-escalation of the event and occurs in parallel with restart and business continuation. As a rule, recovery is carried out by the organizational units responsible for affected (IT-)resources.
- De-escalation of the loss event marks the transition from emergency/crisis management back to normal operations and is called out by the Exchange's crisis team as soon as the necessary conditions allow and are appropriate.
- Rework is often required between de-escalation and the achievement of full normal operations. These are summarized as part of the disruptive operations phase. Disruptive operation includes all rework that occurred during or as a result of emergency operations. Disruptive operation is no longer part of emergency response.

3.5. Re-Opening Procedures

Once the problems that have occurred have been resolved, Boerse Stuttgart will endeavor to make the trading system available to trading participants again as quickly as possible, whilst fulfilling the regulatory responsibilities. This also includes the corresponding preparations for reopening. Depending on the extent/length of the technical disruption, this will also be specified. This is communicated before the market opens.

3.6. Communication to Competent Authorities

If a significant system disruption according to provisions of MiFID II and its supplementing regulations is declared the competent highest state authority of the State of Baden-Württemberg, the Exchange Supervisory Authority, will be informed as soon as possible via E-Mail and in case of need via phone. The contents of the notifications follow the provisions of Article 54(2) and Article 31(2) of MiFID II. A first notification is made in the manner of a general initial emergency message. As a second step more detailed information are provided taking into account ESMA’s standardised template in relation to such instances.

Besides further regulatory based requirements concerning communication towards competent authorities in the event of a market outage are implemented within Boerse Stuttgart Group.

3.7. Further External Communication

If the continuity of trading is interrupted, the trading systems providers, other affected service partners, data vendors and trading participants will be informed as close to real-time as possible via E-Mail and in case of need via phone and the public on the websites of the Exchange. Updates of the information will be provided as soon as possible in case of changes.Communication to market participants will take place at regular intervals according to the disruption or outage.

Lists of contact persons of the trading systems providers, service partners, data vendors and trading participants to ensure business continuity are periodically updated. Trading participants are required to provide up-to-date contact details to ensure a complete list of persons acting on their behalf to be contacted when incidents occur.

As soon as the trading restriction can be narrowed down (e.g. to individual asset classes or interfaces (FIX connection, front end, managed file transfer service, etc.), the affected stakeholders are informed accordingly. If possible, the time for resumption is specified accordingly. Where it is not possible to communicate the status of orders directly from the messages provided, the affected trading participants will be informed directly via bilateral calls to ensure clarity on each order.

Following on from the previous communication regarding a trading restriction/interruption (including associated updates), all affected internal and external stakeholders are notified. Where possible, the same communication channels are used throughout. The communication channels may differ depending on the target group/stakeholder group. The content is tailored to the respective target group. If necessary and possible, the restart is announced to the relevant stakeholders in advance. The lead time may vary depending on the occasion.

In addition, trading participants have the option of deleting all open orders themselves using the FIX protocol or requesting order deletions from the Börse Stuttgart Group via e-mail, which are then executed manually by the Trade Reconciliation & WPBH department using the front end. If the status of submitted orders cannot be transmitted or requested via the FIX protocol, a bilateral telephone exchange can take place with the trading participant(s) concerned if necessary

The emergency messages distributed via these channels are based on pre-defined templates taking into account different emergency scenarios. All messages contain comparable information in regard to a respective scenario and are updated on a regular basis.
Questions can be addressed to the Exchange in any cases and are welcome. The account details can be found under: https://www.boerse-stuttgart.de/de-de/service/kontakt/

3.8. List of Abbreviations

Abbreviations	Explanation
BaFIN	Bundesanstalt für Finanzdienstleistungsaufsicht
BAO	Besondere Aufbauorganisation / Special Structure Organization
BCM	Business Continuity Management
BCMS	Business Continuity Management System
BIA	Business Impact Analysis
BSI	Bundesamt für Sicherheit in der Informatik
BWWB, Exchange	Baden-Württembergische Wertpapierbörse
ESMA	European Securities and Markets Authority
EU	European Union
ISO	International Standardization Organization
ISVM	Information Security Incident Management
ITIL	Information Technology Infrastructure Library
ITSCM	IT Service Continuity Management
KPI	Key Performance Indicator
MiFID II	Markets in Financial Instruments Directive (recast) – Directive 2014/65 of the European Parliament and of the Council
MTPD	Maximum tolerable period of disruption
PDCA	Plan, Do, Check, Act
RPO	Recovery Point Objective
RTO	Recovery Time Objective
RTS 7	Commission Delegated Regulation (EU) 2017/584 of 14 July 2016 supplementing Directive 2014/65/EU of the European Parliament and of the Council with regard to regulatory technical standards specifying organisational requirements of trading venue
SSCC	Senior Stakeholder Communications Committee
SIEM	Security Information and Event Management

4. Contacts

https://www.boerse-stuttgart.de/de-de/service/kontakt/

5. Publication

This playbook is published on the website of the Exchange (https://www.boerse-stuttgart.de/de-de/fuer-geschaeftspartner/reports/).