DEUTSCHE BÖRSE GROUP

Written Rules Framework applied

Incident and Crisis Management Policy

Version: 1.0

Valid From Date: 01.08.2025

Last Review Date: 01.08.2025

Notes: This written rule uses gender-neutral and inclusive language. Whenever possible, the generic masculine is avoided, and all employees of any gender identity (m/f/d) are addressed.

Content changes compared to the previous document version are highlighted in color. Due to the new creation, this has been omitted in this version.

Content

1. Purpose, Objectives and Basis

1.1. Purpose and Objectives and Basis

The purpose of the Incident and Crisis Management Policy is to provide a binding ruleset for managing incidents and crises.

This policy aims to achieve the following objectives:

- Provide a framework for managing incidents and crises, aiming to minimize their impact, ensuring a coordinated and effective response, and safeguarding assets, reputation, and stakeholders' interests.
- Provide the key principles for managing incidents and crises effectively, including:
  - **Preparation**: Develop and maintain guidelines and procedures.
  - **Responsiveness**: Ensure timely and appropriate actions during incidents and crises.
  - **Recovery**: Restore normal operations.
  - **Post Recovery**: Learn from incidents and crises to improve future responses.
- Align with ISO 22361:2022(E) guidelines.

This policy and related templates are the responsibility of Crisis Resilience Management and will be published as well as developed further by this Unit.

1.2. Basis of this Written Rule

Considering the definitions of the Written Rule Framework Guideline, this written rule is based on:

	External Requirements	• n/a
x	**High-risk activities**	• The basis of this written rule lies in high-risk activities, including vital business or risk mitigating activities which, in case not properly governed and executed, could threaten DBAG`s business model, future performance, solvency, liquidity and/or reputation.
	Strategy of DBAG	• n/a

2. Scope and Target Groups

2.1. Scope of applicability

Entity	• DBAG and adopting LE within DBG
Area	• All areas

Legal entities that have adopted the Policy grants Crisis Resilience Management the right to request and receive information necessary to fulfill its adherence oversight role. This specifically applies when minimum requirements are implemented by reflecting respective DBAG Policies within LE-specific written rules. For clarity, the LE remains responsible for compliance with the adopted rules.

2.2. Target groups

Target group	Key message
Incident Owner	Ensure that all incidents are reported immediately to their supervisor or the designated response team.
Incident Manager / Overall Coordinator	Ensure that procedures are in place to assess and contain the incident.
Crisis Management Team	Ensure that procedures are in place to assess and contain the crisis.
Crisis Resilience Management	Ensure that governance is properly established, including guidelines and procedures, call trees, and an annual review process.
Senior Management	Ensure that clear tasks and responsibilities for Incident and Crisis Management are assigned, a binding ruleset is followed for managing incidents and crises, appropriate governance structures are in place the Legal Entity, and compliance with all applicable minimum requirements is maintained.

3. Definitions

- **Incident**: An “incident” is an unexpected event or situation that can lead to a disruption, loss, emergency, or crisis. Incidents require prompt attention and resolution to prevent further complications but do not pose a significant threat to the institution's overall stability, financial standing, or reputation.

- **Crisis**: A "crisis" is an abnormal or extraordinary event or situation that threatens the organization and requires a strategic, adaptive, and timely response to preserve its viability and integrity. A “crisis” requires immediate and comprehensive management efforts to mitigate damage and restore normal operations.
- **Call Tree:** A “call tree” is a list of contact names and phone numbers used in incident and crisis management to ensure efficient communication. It is organized hierarchically, with each person responsible for contacting specific individuals. A call tree should include an escalation process for critical information and backup contacts to maintain communication should the primary contact become unavailable.

4. Minimum Requirements

The policy covers all incidents and crises, including but not limited to operational disruptions, cybersecurity threats and data breaches, workplace safety incidents, natural disasters, as well as reputational, regulatory, and legal issues.

The foundation for establishing robust incident and crisis management capabilities is based on the following minimum requirements:

a) **Organizational Structure:** The Executive Board of the Legal Entity is responsible for implementing a strong incident and crisis management structure to safeguard the organization's assets and objectives during incidents and crises. This includes establishing:

- An Incident and Crisis Management (ICM) Function or equivalent, responsible for maintaining the incident and crisis management framework at legal entity level.
- An Incident Management Team (IMT) or equivalent. Each board area must designate both a primary incident manager and a deputy to ensure coverage and continuity.
- A Crisis Management Team (CMT) or equivalent, optionally supported by a Crisis Management Support Team (CMST).

b) **Governance:** The ICM Function must implement clear governance for the incident and crisis management structure outlined in point (a). This includes:

- Defining roles and responsibilities.
- Outlining an escalation process to ensure proper incident escalation.
- Creating appropriate “call trees” covering Business Segments and/or Legal Entities.

c) **Framework**: The ICM Function and Incident and Crisis Managers must develop comprehensive documentation for effective incident and crisis response. These documents should be systematically structured across three distinct levels:

- Strategic Level (ICM Function): Incident and Crisis Management Policy.
- Tactical Level (ICM Function): Incident and Crisis Management Guideline.
- Operational Level (Incident or Crisis Managers): Incident and Crisis Management Procedures.

d) **Incident Classification:** The ICM Function must establish uniform criteria for classifying incidents, considering factors such as severity and impact.

e) **Decision Making:** The ICM Function must ensure effective decision-making by implementing a structured approach that, among other things:

- Relies on accurate and timely information management.
- Takes into account the input of business experts.
- Considers legal and insurance aspects.

f) **Communication**: The Communication Team must develop communication plans for handling incidents and crises. These plans should include clear procedures for managing internal and external crisis communications.

g) **Incident and Crisis Management Tools:** The ICM Function and Incident and Crisis Managers must establish effective communication and coordination during an incident or crisis by ensuring the right tools and resources are in place; these include:

- Notification tools
- Collaboration tools
- Physical rooms
- Backup solutions

h) **Ethics:** In line with DBG values, all parties must ensure legal compliance when dealing with incidents or crises, particularly by refraining from paying ransoms. Any exceptions must be approved by the Executive Board.

i) **Continuous Improvement:** The ICM Function must ensure continuous improvement by:

- Performing a comprehensive review of the incident and crisis management framework at least once a year.
- Conducting regular trainings for relevant personnel.
- Ensuring regular tests of the incident and crisis management capabilities are executed by the Incident Management Teams and Crisis Management Team (e.g., test program).

j) **Collaboration in a crisis across Legal Entities within Deutsche Börse Group:** The management of each legal entity is responsible for crisis management within their respective entities. If an incident or crisis affects several companies, certain aspects must be coordinated and aligned with DBAG's CMT, particularly regarding the following topics:

- Internal and external communication such as messaging consistency, stakeholder notifications, and media handling.
- IT & security measures such as incident reporting, threat containment strategies, patch management & system checks, data sharing, and decryption.
- Legal & regulatory compliance such as breach notification laws, data protection requirements, and litigation risk.
- Recovery (e.g. restoration priority and customer support).
- Post-Incident review, including root cause analysis and lessons learned.

The alignment with DBAG's CMT should be done – if legally and practically possible – before the respective measure is taken by the legal entity.

In any event, attention has to be paid to DBAG's ad-hoc notification requirements, in particular any incident which is likely to have a major reputational or financial impact has to be discussed with the chair or any other member of DBAG's ad-hoc committee prior to any communication.

k) **Performance evaluation:** The ICM Function must establish a yearly report to the legal entity's management body on the status of the ICM framework. This should include an overview of the implementation of the ICM minimum requirements, performance, adequacy, results of testing and ongoing improvements of the ICM framework as well as status of audit findings regarding the framework.

5. Roles & Responsibilities

- **Executive Board (or equivalent) of the Legal Entity:** The Executive Board is responsible for approving any decisions that diverge from this policy or exceed the authority of those managing an incident or a crisis. Moreover, the Executive Board ensures effective communication with stakeholders, including shareholders, regulators, and the public. In doing so, they help manage the organization's reputation and maintain trust during and after a significant incident or crisis.

- **Respective Incident and Crisis Management functions:** The ICM Function, or its equivalent, within each Business Segment and/or Legal Entity is responsible for reviewing and updating their respective Incident and Crisis Management Policy, as well as the subordinate Incident and Crisis Management Guideline. Additionally, the ICM Function must review and update the Crisis Management Team Procedure, strengthen crisis management capabilities (e.g., by organizing tests) and provide guidance on the Crisis Management Process during a crisis.

- **Crisis Management Team (CMT):** The CMT is the designated body that convenes in the event of a crisis. Once a crisis is declared, the CMT is responsible for coordinating and overseeing crisis management activities. If a crisis affects multiple entities within DBG, the DBAG's CMT serves as the central point of contact for sharing information across the Group and with the Executive Board of DBAG.

- **The Incident Management Team (IMT):** The IMT is the designated team responsible for coordinating and managing responses to incidents that impact the legal entity. The team consists of Incident Manager(s) and subject matter experts (e.g., the Incident Owner), who are tasked with assembling promptly when an incident occurs. Their role is to ensure that all necessary actions are taken to mitigate the impact and restore normal operations as quickly as possible. In cases where multiple areas and Incident Managers are involved, one Incident Manager will assume the role of Overall Coordinator. This role includes assessing the situation, implementing response strategies, and coordinating with other teams to ensure a cohesive and effective response to any disruptions.

- **Communications Team:** The Communications Team at the legal entity or business segment level is responsible for developing and disseminating timely and accurate information to internal and external stakeholders during an incident or crisis. This includes working closely with the IMT and CMT to ensure message alignment and to manage communication channels effectively. If a crisis impacts multiple entities within DBG, internal and external communications should be aligned with Group Communication.

6. Appendix

6.1. Contact Information

For questions regarding this policy, please contact Crisis Resilience Management (U).

6.2. Document History

Document History

Version	Date	Changes & Background
1.0	30.06.25	Initial Document

Coordination before publication

Version	Date	Task	Function
1.0	01.06.2025	**Creator**	Crisis Resilience Management (U)
	23.06.2025	**Content Review**	Head of Group Risk Resilience (S), CRO DBAG
	16.06.2025	**Content Confirmation** **Written Rule Owner**	CRO DBAG Head of Crisis Resilience Management (U),

Approvals

Version	Date	Task	Function
1.0	30.06.2025	**Approval**	Head of Group Risk Resilience (S)
1.0	25.07.2025	**Approval**	DBAG Executive Board

6.3. Related written rules

Superordinated written rules	- n/a
Subordinated written rules	- Incident and Crisis Management Guideline

6.4. Abbreviations

CMST	Crisis Management Support Team
CMT	Crisis Management Team
CRO	Chief Risk Officer
DBAG	Deutsche Börse AG
DBG	Deutsche Börse Group
ICM	Incident and Crisis Management
U	Unit