DEUTSCHE BÖRSE GROUP

DEUTSCHE BÖRSE GROUP
Written Rules
Framework applied

Incident and Crisis Management Guideline

Version: **5.0**

Valid From Date: 01.12.2025

Last Review Date: 01.12.2025

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 significant changes in all areas, this has been omitted in this version.

Content

1. Purpose, Objectives and Basis

1.1. Purpose and Objectives

This Guideline establishes guidance for the creation and maintenance of:

- Incident and Crisis Management Procedures (ICMPs)
- Crisis Management Team Documents (e.g., Terms of Reference, Crisis Management Playbook)

These, along with any other related procedures and documents, are collectively referred to as "subordinated documents". Where provisions apply exclusively to a specific document (e.g., Terms of Reference), this will be clearly indicated.

The objective of the Guideline is to:

- Minimize the impact of crises (e.g., cyberattacks).
- Meet legal, industry, and governance requirements.
- Improve cross-functional collaboration during crisis.
- Institutionalize lessons learned from past incidents.

This Guideline falls under the responsibility of Crisis Resilience Management (U) and will be published and further developed by this unit.

1.2. Basis of this Written Rule

The basis for this guideline is thematically linked to the Incident and Crisis Management Policy and considers relevant key requirements of:

- Digital Operational Resilience Act (DORA - 2022/2554)
- ISO 22361:2022(E) – Guidelines for Crisis Management

2. Functional Scope and Target Groups

2.1. Functional Scope of applicability

Entity	– DBAG
Area	– All areas

Table 1: Scope

2.2. Target groups

Target group	**Key message**
Incident Manager/ Overall Coordinator	Ensure that ICMPs established by Incident Managers are prepared in accordance with the requirements outlined in this guideline. The Incident Manager is responsible for ensuring that all minimum standards defined herein, as well as any applicable regulatory requirements, are consistently upheld.

Crisis Management Team	Ensure that all documents and procedures established by, or to be followed by, the Crisis Management Team are prepared in accordance with the requirements outlined in this guideline. The Crisis Management Team (CMT) is responsible for ensuring that all minimum standards defined herein, as well as any applicable regulatory requirements, are consistently upheld.
Crisis Resilience Management	Ensure that governance is properly established, including guidelines and procedures, call trees, and an annual review process.

Table 2: Target groups

3. Definitions

Subordinated documents shall adopt the following standardized definitions for the terms to ensure consistency across the entity.

- **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.
- **Incident & Crisis Management Procedure (ICMP):** Is a document that defines a structured set of processes and responsibilities to identify, escalate, and manage unexpected events (incidents) or severe disruptions (crises) that threaten business operations, reputation, or safety. It ensures timely response, clear communication, and coordinated actions to minimize impact and restore normal operations as quickly as possible.
- **Crisis Management Team Documents:** Are documents that outline the structure, roles, and operational guidance for the Crisis Management Team (e.g. Terms of Reference, Playbook, etc.).

4. Requirements

4.1. Incident and Crisis Management Procedure

The Incident and Crisis Management Procedure (ICMP), as a formal procedure, must be developed using the required Written Rules Framework and template

(see https://deutscheboerse.sharepoint.com/sites/WrittenRulesDatabase).

This Incident and Crisis Management Guideline provides detailed guidance on how to fill out the template from the Written Rules Framework for the ICMP, particularly for Ch. 3 (Requirements) and Ch. 4 (Roles and Responsibilities).

Although the procedure owner may adapt the structure of the ICMP to suit their specific needs, the following table recommends a structure for the ICMP (not mandatory). For each section you can find guidance in this guideline.

Chapter	Recommended Structure for the ICMP
4.	**Requirements**
4.2.	Centralized Storage of Documents
4.3.	Interface between ICMPs, BCPs, and DRPs
4.4.	Incident Classification and Escalation
4.5.	Notification and Collaboration
4.6.	Incident Handling
4.7.	Incident and Crisis Communication
4.8.	Continuous Improvement and Performance Evaluation and Review
5.	**Roles & Responsibilities**
5.1.	Incident Identifier
5.2.	Business / IT Duty Manager
5.3.	Incident Manager
5.4.	Overall Coordinator
5.5.	Crisis Management Team Facilitator (CMT Facilitator)
5.6.	Crisis Manager
5.7.	Deputies
5.8.	Incident Management Team
5.9	Crisis Management Team
5.10.	Crisis Management Support Team

4.2. Centralized Storage of Subordinated Documents

Subordinated documents have to be accessible via links from the centralized SharePoint sites maintained by Crisis Resilience Management (CRM). There are two separate SharePoint sites: one for Incident & Crisis Management Procedures (ICMPs) and another for Crisis Management Team documents. Both sites are managed by CRM.

While hosting is centralized, responsibility for the accuracy and content of documents remains with their respective owners, who are required to provide CRM with a link to the most recently approved version of their documents. This approach keeps the centralized repository current and enables CRM to maintain oversight and continuous accessibility of relevant documentation.

Moreover, it should be considered how to store key subordinated documents during disruptions (e.g., MS 365 outages); for example, on a backup platform or hard copies.

4.3. Interface between ICMPs, BCPs, and DRPs

Subordinated documents have to, where appropriate, explain the interaction between Incident and Crisis Management Procedures (ICMPs), Business Continuity Plans (BCP), and Disaster Recovery Plans (DRP), as these form the organizational response framework to disruptions to normal business.

In principle, ICMPs provide a tactical and operational structure for managing disruptions, from initial incident detection to escalation and resolution. These procedures trigger BCP activation to ensure critical business functions continue during a crisis, while DRP focuses on restoring IT infrastructure and data integrity. Together, they enable coordinated decision-making, minimize downtime, and protect operational assets.

4.4. Incident Classification and Escalation

4.4.1. Incident Classification

The first step of the incident classification is the assessment of the incident type (e.g., ICT- or non-ICT-incident).

A clear differentiation between ICT & non – ICT related incidents is mandatory for appropriate incident / crisis handling.

- Non-ICT incidents are to be handled according to the ICMP of the relevant area.
- ICT related incidents underly both the ICMP as well as the ICT Incident Management Procedure, to ensure regulatory compliance.

The second step of the incident classification considers the derivation of the Alert level based on the color-coding matrix.

Subordinate documents have to, where appropriate, reference or incorporate the color-coding matrix provided in this document for incident classification and escalation. This matrix establishes standardized thresholds for assessing incident severity and impact, ensuring consistent and uniform classification across the organization.

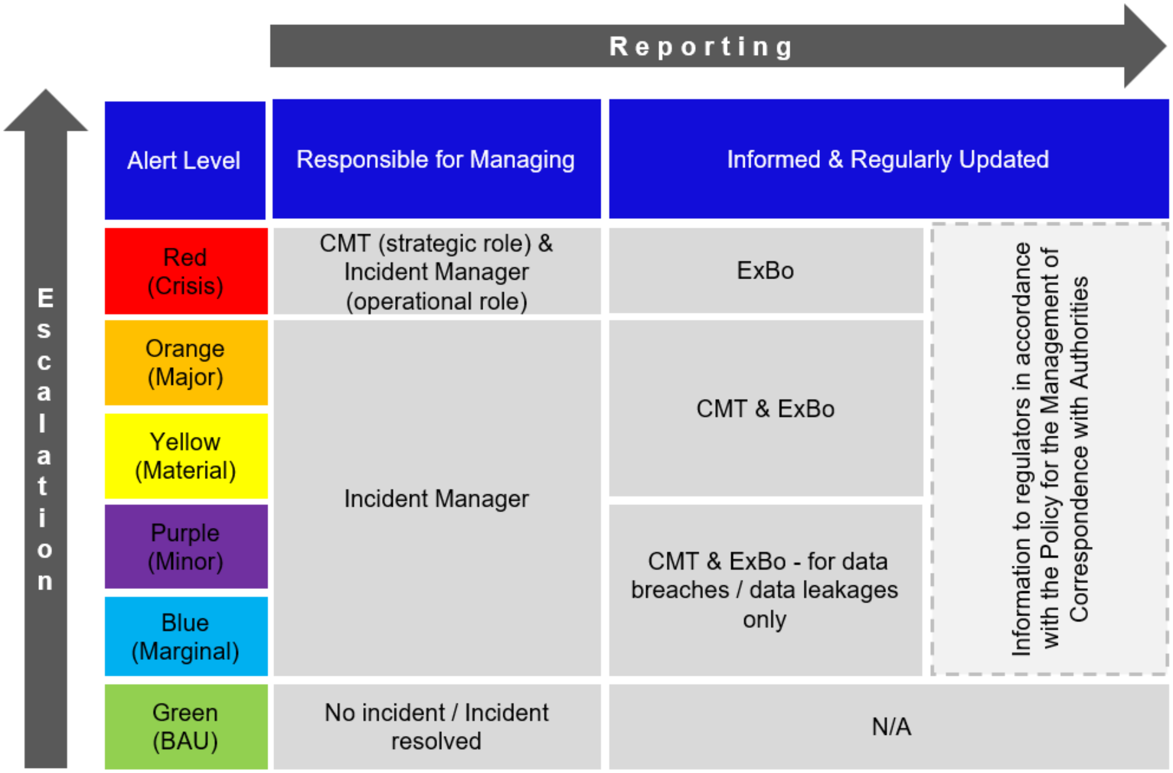
Alert Level		Severity Criteria (exemplified guidance only)			
		Business Impact	Physical Assets	IT Impact	Information Security
Red (Crisis)	High Visibility	Critical (i.e. severe) business disruption, such as widespread outages or events threatening overall business continuity (e.g., severe customer detriment, existential regulatory fines, or extreme market losses).	Critical (i.e. severe) damage to physical assets, affecting one or more entire locations, with situations that may pose a risk to life or personal safety.	IT Severity: Very High Critical prolonged unavailability of strategic location (e.g., datacenter, cloud provider) with extensive impact.	Critical (i.e. severe) information security event, such as a cyber incident (e.g. ransomware) or loss of confidentiality of information, potentially resulting in severe financial damage.
Orange (Major)		Major business disruption, such as the non-delivery of business products or processes, leading to customer detriment, substantial regulatory fines and customer claims.	Major damage to physical assets, affecting a high number of individuals, with consequences that may strain or exceed the capabilities of current contingency solutions.	IT Severity: Very High Critical application/service completely unavailable. Very high effect on other Product services/ processing or strategic locations.	Major information security event, such as a cyber incident or loss of confidentiality of information, potentially resulting in major financial damage.
Yellow (Material)	Increased Visibility	Material business disruption, such as the non-delivery of business products or processes that may spill over to business areas, potentially exceeding RTOs.	Material damage to physical assets leading to the activation of contingency plans.	IT Severity: High Critical application/service av. Impacted, significantly reduced performance. High effect on other Product services/processing or strategic locations.	Material information security event, such as a cyber incident or loss of confidentiality of information, potentially resulting in material financial, operational, or reputational damage; or multiple repeated security control breaches under the same line management within a fortnight period.
Purple (Minor)		Minor business disruption, such as controllable impacts on deliveries, products, or processes, with contingency measures in place and recovery RTOs.	Minor damage to physical assets, with a limited number of staff affected, and manageable within existing contingency plans.	IT Severity: Medium (pot. high)[1] Major/critical application/service availability impacted. Reduced performance with significant impact.	Minor information security event, such as a cyber incident or loss of confidentiality of information, potentially resulting in minor financial damage, or repeated security control breach under the same line management within in a fortnight period.
Blue (Marginal)	Minor Visibility	Marginal business impact, such as missed deadlines and disruptions affecting limited business areas for short durations.	Marginal damage to physical assets that can be managed without activating contingency plans.	IT Severity: Medium Application/service unavailability with minor/moderate impact and low/medium urgency.	Marginal information security event, such as a cyber incident or loss of confidentiality of information, potentially resulting in marginal financial damage; or one security control breach occurred, e.g., CyberArk bypass.
Green (BAU)	Status after resolution of incident, no further impact / BAU				

[1] The decision on initiating an IMM is conditioned by a time component (e.g., high urgency, hotfix not achieved within a certain timeframe)

While the matrix serves as a valuable guidance tool, it is important to note that the actual decision to classify the severity of an incident is based on the specific situation and the information available at the time. Depending on the development of the situation, the severity classification can be either increased or decreased.

4.4.2. Incident Escalation & Reporting

Subordinate documents have to, where appropriate, specify the process for incident escalation and reporting. The table below outlines the responsibilities for managing an incident or crisis, including who must be notified and reported to, based on the assigned color codes. In addition, the reporting process must align with the Policy for the Management of Correspondence with Authorities, ensuring that relevant information is shared with regulators in a timely and compliant manner.


Reporting
Escalation

Alert Level	Responsible for Managing	Informed & Regularly Updated	
Red (Crisis)	CMT (strategic role) & Incident Manager (operational role)	ExBo	Information to regulators in accordance with the Policy for the Management of Correspondence with Authorities
Orange (Major)	Incident Manager	CMT & ExBo	
Yellow (Material)			
Purple (Minor)		CMT & ExBo - for data breaches / data leakages only	
Blue (Marginal)			
Green (BAU)	No incident / Incident resolved	N/A	

4.5. Notification and Collaboration

4.5.1. Notification Tools

Subordinate documents have to outline, where appropriate, the methods for notifying stakeholders during an incident or crisis. They must also define backup solutions (i.e., secondary channels) for the primary notification methods should they become non-functional (e.g., when the network is down).

4.5.2. Call Trees

Subordinate documents have to include, where appropriate, a call tree. A “call tree” is a hierarchical list of contact names and phone numbers used in incident and crisis management to ensure efficient communication. Everyone listed is responsible for notifying specific contacts. The call tree have to also designate backup contacts to ensure continuity in case of unavailability.

There are two types of call trees, both of which must be established and maintained:

- **Entity Level Call Tree**
  Maintained by **Crisis Resilience Management**, the legal entity call tree (i.e. DBAG) serves as the central communication framework during major incidents or crises. It ensures that key stakeholders across the organization are informed and coordinated efficiently.
- **Area-specific Call Tree**
  Maintained by the respective **Incident Manager** in their ICMP, these call trees are tailored to individual departments, locations, or business units. They support localized response efforts and ensure swift communication within specific operational areas during incidents.

4.5.3. Collaboration Tools

Subordinate documents have to specify, where appropriate, the channels for collaboration during an incident or crisis. They must also define backup solutions (i.e., secondary channels) for the primary collaboration channels in case they become non-functional (e.g., when the network is down). They have to include a detailed explanation of how to use the backup solution to ensure seamless collaboration during disruptions.

4.5.4. Collaboration Rooms

Subordinated documents have to list, where appropriate, the primary incident and/or crisis management rooms and backup rooms. The crisis management rooms shall include the following resources, while incident management rooms, should they differ, may have fewer resources:

General Room Specifications

- Large table
- 6+ chairs

Communication Tools:

- Standard telephone
- Video conferencing equipment
- Internet access

Documentation Tools:

- Whiteboards and markers
- Flip charts and markers (optional)
- Notepads and pens (optional)

Access to Technology Resources:

- Clean laptops (ready for immediate use), power cables, and phone chargers should be readily accessible. Although these items must not be stored directly in the incident and crisis management rooms, they must be easy to locate and retrieve when needed.

Framework Resources:

- Contact List as hard copy
- Physical copies of subordinated documents

4.6. Incident Handling

Subordinated documents must include, where applicable, a section titled “Incident Handling” that is tailored to the specific needs of the respective area. This section has to describe the area’s unique context for managing incidents, including relevant processes, roles, and dependencies under various scenarios (if applicable).

Additionally, this section has to include sub-chapters for “Coordination across Entities,” “Decision Recording,” and “Ethics.” These topics are more generic in nature and apply uniformly across all areas and are described in the below subsequent chapters.

4.6.1. Coordination across Legal Entities within DBG

Each Legal Entity (LE) within DBG is responsible for managing its own incidents. However, when an incident impacts multiple LEs, the following coordination process applies:

- **Multiple LE Incidents:** The Overall Coordinator is responsible for coordinating the response among the affected Legal Entities (see section 5.4).
- **Multiple LE Crises:** DBAG’s Crisis Management Team (CMT) takes over responsibility for coordinating the response.

Before individual LEs take any significant measures, they must align with other affected entities whenever legally and practically possible. This principle is especially important for decisions regarding external communications, IT and security measures, legal and regulatory compliance, and recovery strategies.

4.6.2. Decision Recording

All significant decisions made during incident and crisis management must be documented to ensure transparency, accountability, and support for post-event analysis. The method of decision recording depends on the classification of the event:

- **Incidents:** For incidents all key decisions, including the rationale and agreed actions, must be recorded in the official meeting minutes. These minutes have to be distributed to relevant stakeholders and stored according to DBAG`s general safeguarding requirements.
- **Crises:** For crises, all decisions must be documented in a dedicated crisis logbook. The crisis logbook serves as the authoritative record for all decisions made by the Crisis Management Team and supporting teams. It has to include the context and reasoning for each decision, the time and date, the names and roles of participants, and the actions taken. The logbook must be maintained in real time throughout the crisis and safeguarded as a confidential document. The person(s) responsible for maintaining the Crisis logbook has to be identified in the Crisis Management Team (CMT) Terms of Reference.

Decision records, whether meeting minutes or crisis logbooks, have to be labeled “Strictly Confidential” and retained for at least 10 years in accordance with organizational and regulatory requirements.

4.6.3. Ethics

Adherence to DBG’s core values is fundamental to maintaining lawful and regulatory compliance across all stages of incident and crisis management. Ethical conduct must be upheld without exception. A critical principle in this context is the absolute prohibition of ransom payments. Any deviation from this rule may only be considered under exceptional circumstances and requires explicit approval from the Executive Board.

4.7. Incident and Crisis Communication

4.7.1. Internal Communication

Subordinate documents have to describe, when appropriate, how, when and by whom employees will be made aware of a noteworthy situation. Effective internal communication is crucial during incidents and crises to ensure that employees are informed and aligned with the organization's response efforts. For example, in the event of a crisis, it is important to notify staff to prevent employees from being caught off guard by external communications. This approach helps maintain trust and morale within the organization.

4.7.2. External Communication

4.7.2.1. Customer Notification

Subordinated documents have to, where applicable, include or reference instructions for customer communication during incidents and crises. These instructions have to cover communication channels, responsible roles, escalation protocols, and message content tailored to the nature and impact of the event. Particular attention must be paid to DBAG's ad-hoc notification requirements.

4.7.2.2. Regulatory Reporting

Subordinated documents have to, when appropriate, describe the process for reporting regulatory compliance issues to various authorities. This includes:

- Identify the types of incidents that require regulatory notification (e.g. under DORA). This could include breaches of regulatory requirements, significant operational disruptions, or other compliance issues.
- Define the timeline for reporting to regulators/oversight bodies. This could include immediate reporting for severe incidents or periodic updates for ongoing issues.
- Specify the methods for reporting, such as formal reports, emails, or online submission portals.

4.7.2.3. Media Management

Subordinated documents have to include or reference to, where appropriate, procedures for managing communication with the media during incidents and crises. This includes:

- Determine the circumstances under which the media should be informed. This could depend on the public interest, the potential impact on the company's reputation, and the need for transparency.
- Establish the timing for media notifications. This could include immediate press releases for significant incidents or scheduled briefings on ongoing issues.
- Describe the methods for communicating with the media, such as press releases, press conferences, or social media updates. It has to also include guidelines for preparing key messages, designating spokespersons, and ensuring consistent and accurate communication.

4.8. Continuous Improvement and Performance Evaluation and Review

4.8.1. Continuous Improvement

Subordinated documents have to outline, where appropriate, provisions for continuous improvement, ensuring that activities such as learning sessions and post-event reviews are conducted to capture lessons learned and identify opportunities for enhancement.

For incidents classified below “yellow,” these reviews are optional but strongly recommended. For incidents classified as “yellow” or higher, Lessons Learned sessions are mandatory.

In addition, the Incident Management Team (IMT) and Crisis Management Team (CMT) are expected to routinely perform capability tests to validate preparedness and pinpoint areas for improvement.

4.8.2. Performance Evaluation

Subordinated documents have to outline, where appropriate, that a yearly performance evaluation report on the validity of Incident & Crisis Management (ICM) framework is prepared and submitted by the Crisis and Resilience Management Unit (i.e. responsible ICM function) to the management body of the legal entity.

This report is based on the feedback received by Incident Managers and serves to ensure transparency and to validate the adequacy and performance of the ICM framework.

4.8.3. Maintenance

Subordinated documents have to include, where appropriate, the following review frequencies of documents.

Document	Responsible	Type	Frequency/date
Incident & Crisis Management Procedure	Business Areas	Ad hoc	Upon significant changes affecting the information in the ICMP.
		Post testing / Incident	Within the deadline as per test results or as part of Lessons Learnt from a real incident.
		Regular	Every 6 months
Terms of reference	Crisis Management Team (CMT)	Ad hoc	Upon significant changes affecting the information in the ToRs.
		Post testing / Incident	Within the deadline as per test results or as part of Lessons Learnt from a real incident.
		Regular	On an annual basis (every 12 months)
Performance Report	Crisis Resilience Unit	Regular	On an annual basis (every 12 months)
Entity-wide Call Tree	Crisis Resilience Unit	Ad-hoc	If contacts change.
		Regular	On an annual basis (every 12 months)
Area-specific Call Tree	Incident Manager	Ad-hoc	If contacts change.
		Regular	On an annual basis (every 12 months)

5. Roles and Responsibilities

Subordinated documents should, where appropriate, adopt the following definitions of roles and responsibilities to ensure consistent terminology across the organization.

5.1. Incident Identifier

The Incident Identifier (II) is the individual who detects and reports an incident.

5.2. Business / IT Duty Manager

The Business Duty Manager (BDM) / IT Duty Manager is a designated business / IT representative on call, responsible for receiving internally reported incidents and, if necessary, escalating them to the appropriate Incident Manager.

5.3. Incident Manager

The Incident Manager (IM) is responsible for leading, coordinating and ensuring the proper and timely response to incidents within their designated area. These include:

Framework

- Drafts and maintains the Incident and Crisis Management Procedure for their designated area of responsibility.

Incident Classification

- Classifies incidents using the color-coded matrix and if applicable, DORA-relevant criteria for ICT incidents.

Initiates Incident Management Meeting

- Initiates an Incident Management Meeting upon the occurrence of an incident and invites relevant subject matter experts (e.g., using call trees) to form an Incident Management Team tailored to nature and scope of the incident.

Incident Coordination

- Acts as the single point of contact for the impacted area.
- Facilitates cross functional collaboration to ensure a unified incident response.
- Oversee the resolution process to ensure timely restoration of BAU operations.
- Activates contingency plans and facilitates root cause analysis when necessary.

Documentation and Reporting

- Maintains detailed records of incidents, including impact scope, actions taken, and outcomes.
- Coordinates internal and external reporting with relevant stakeholders (e.g., communication, compliance).
- Supports regulatory reporting obligations as required.
- Reports status depending on color coding matrix to ExBo and CMT.

Post Incident Review

- Conducts reviews with stakeholders to evaluate the effectiveness of the incident management process and identify lessons learned.

Continuous Improvement

- Ensures a semi-annual review of incident and crisis management procedures under his/her responsibility and implements enhancements based on the review findings.

5.4. Overall Coordinator

The Overall Coordinator (OC) is an Incident Manager who takes the lead when multiple areas or legal entities are impacted simultaneously. The Overall Coordinator's responsibilities, beyond those of an Incident Manager, include:

- Acts as the single point of contact across impacted areas or legal entities, ensuring consistent coordination.
- Ensures timely dissemination of incident related information to impacted Legal Entities.
- If the incident is not declared a crisis, the OC also provides updates to the affected responsible Legal Entity Board members.

5.5. Crisis Management Team Facilitator (CMT Facilitator)

The CMT Facilitator is responsible for assessing together with the Overall Coordinator if an incident qualifies as a crisis. Upon declaring a crisis, the CMT Facilitator initiates the Crisis Management Process by convening the Crisis Management Team to meet and discuss the incident.

5.6. Crisis Manager

The Crisis Manager is responsible for the coordination of a crisis for the impacted entity. It is, when multiple areas are impacted, the person communicating on behalf of the entity to the DBAG CMT and, if necessary, the ExBo.

5.7. Deputies

To ensure continuity if any one of the defined roles in Chapter 5. is unavailable, at least one, preferably two, designated deputies must be appointed. These deputies must understand their roles within the incident and crisis management process and be capable of temporarily assuming the associated responsibilities. Designated deputies must be clearly documented in subordinate documents (e.g., call trees, ICMPs, terms of reference, etc.).

5.8. Incident Management Team

The Incident Management Team (IMT) is a temporary, purpose-built group of subject matter experts assembled by the Incident Manager in response to incidents of different types. It is not a standing or pre-defined team, but rather a dynamic formation tailored to nature, scope, and impact of the incident.

Purpose

The IMT supports the Incident Manager in addressing the response to an incident and ensuring that normal operations are restored.

Composition

The IM determines the composition of the IMT based on the incident's characteristics and may adjust it as the situation evolves. That said, the IMT is typically composed of:

- The Incident Identifier (as necessary)
- The Incident Manager
- Relevant Subject Matter Experts (SMEs) from impacted or supporting departments (e.g., IT, Legal, Compliance, Communications, etc.)
- Representatives from affected business units or legal entities, if applicable.

Activation

- The IM initiates the formation of the IMT upon detection or escalation of an incident. Meeting invitations are issued using predefined contacts (e.g., call trees).[1]

Meetings

- Incident Management Meetings (IMMs) serve as the central coordination forum for the IMT, enabling alignment among stakeholders, impact assessment, and resolution planning

Responsibilities

- Assessing the situation, defining priorities, and executing recovery actions.
- Ensuring internal and external communication across impacted stakeholders.
- Identifying of key stakeholders responsible for initiating lessons learned based on root cause analysis.

Dissolvement

- The IMT is dissolved once the incident is resolved, and the post-incident review is complete.

5.9. Crisis Management Team

The Crisis Management Team (CMT) is the crisis management body called upon to assemble in the event of a crisis at DBAG.

[1] The decision on whether to initiate an IMM is conditioned by a time component. In case of high urgency, when approaching mandatory deadlines or time to recover is unforeseeable, an IMM shall be initiated.

If a crisis affects multiple Legal Entities within Deutsche Börse Group (DBG), the DBAG Crisis Management Team (CMT) also serves as the central point of contact for coordination and information sharing across the Group.

Purpose

- The DBAG CMT ensures consistent internal and external communication across impacted entities.
- Aligns legal and regulatory compliance efforts.
- It coordinates IT and security measures, including incident reporting, containment strategies, and data sharing.
- Harmonizes recovery priorities and customer support strategies.
- Initiates post-crisis reviews and lessons learned exercises across entities.

Composition

- The composition of the Crisis Management Team (CMT), including the roles and responsibilities of its members, must be clearly defined in the CMT's Terms of Reference.

Activation

- The CMT is activated by the CMT Facilitator after aligning with the OC upon the classification of an incident being a crisis or potential crisis.
- Meeting invitations are issued using predefined contacts (e.g., call trees).

Responsibilities

- Supporting the IM in assessing the situation, defining priorities, and coordinating recovery actions, within its decision authorities.
- Ensuring timely and accurate communication between involved parties and stakeholders.

Dissolvement

- The CMT is concluded once the Crisis is resolved, and the post-incident review is completed. Lessons learned and opportunities for improvement are captured and fed into the continuous improvement cycle.

5.10. Crisis Management Support Team (CMST)

The Crisis Management Support Team is nominated by the Crisis Management Team (CMT). It assists in organizing CMT meetings, preparing the situation analysis, preparing a logbook, and ensuring that all relevant information is accurately documented. Their support helps maintain clarity and efficiency during a crisis. The composition of the CMST shall be defined within the CMT`s Terms of Reference.

6. Appendix

6.1. Contact Information

Written Rule Owner: Head of Crisis Resilience Management (U).

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

6.2. Document History

Document History

Version	Date	Reason for changes
1.7.3	30.05.18	Added Incident Manager / Overall Coordinator responsibility of Legal Entity, Regulatory and Contractual partners reporting, Made reference to CSDR requirements triggering additional notifications to the competent authority and relevant authorities (ESMA RTS 71.4b+c), Added requirement for indication of relevant Legal Entities in individual Crisis Management Procedures.
1.7.4	20.08.18	Specified the circumstances triggering an incident investigation and reporting.
1.7.5	11.10.18	Alignment with BCM Policy regarding responsibilities for the naming and update of Incident Managers in the relevant divisions, Updated Departments (after re-organisation October 2018).
1.7.6	22.11.18	Renaming of document. Amendments of role for BCM (chapter 1.5) and wording specifics. Incorporated CSDR requirements.
2.0	28.10.19	Update of Guideline: alignment of Incident and Crisis Management Process throughout DBG, update of color-coding system and escalation & notification process.
2.1	10.02.20	Update of colour-coding matrix (‘business impact’, chapter 1.2) Update of chapter 2.2 (2.2.1 - 2.2.3) New Annex 5: Remote Access activation/deactivation process for contingency situations

3.0	22.03.21	Annual Review of document Incident Logging and Reporting (2.2.4) Specification of notification towards int./ext. stakeholder (3.) Update of Annexes (supportive templates)
4.0	19.04.22	Annual Review of the Guideline Update of colour-coding matrix & escalation process Update of chapter 2 “Roles & Responsibilities”, specification on “blue” Update on chapter 2.2 “Incident Manager” responsible for ensuring communication Update of chapter 2.2.4 “Incident Logging and Reporting”, interface to PILS Incorporation of CMP Maintenance Guideline (chapter 3 – 3.4)
4.1	22.07.22	Re-naming “Corporate Security” to “Physical Security” Chapter 2, adding requirement for use of IMM agenda as of purple All Annexes reviewed (incl. added versioning and review date to each one)
4.2	31.07.23	General review and updates, including adjustments ref. organizational changes branch setup, adding template (Annex 8 CMG) and requirement for external communication to applicable Regulators (major BCM tests), review and update of all Annexes (supportive templates)
4.3	04.03.24	Review and inclusion of terms and definitions in accordance with referenced ISO Standards, inclusion of three-stage incident reporting approach
5.0	07.11.25	Major update in all areas.

Coordination before publication

Version	Date	Task	Function
5.0	05.11.2025	**Creation**	Head of Crisis Resilience Management (U)
	06.11.2025	**Review**	Head of Group Risk Resilience
	07.11.2025	**Content Confirmation**	Head of Crisis Resilience Management (U)

Approvals

Version	Date	Task	Function
5.0	25.11.2025	**Approval**	CRO DBAG

6.3. Related written rules

Superordinated written rules	• Incident and Crisis Management Policy
Subordinated written rules	• Incident and Crisis Management Procedures

6.4. Links

- n/a

6.5. Supporting Documents

- n/a

6.6. Abbreviations

BAU	Business as usual
BCM	Business Continuity Management
BCP	Business Continuity Plan
BDM	Business Duty Manager
CMT	Crisis Management Team
CMST	Crisis Management Support Team
CRM	Crisis Resilience Management
DBG	Deutsche Börse Group
DBAG	Deutsche Börse AG
DORA	Digital Operational Resilience
DRP	Disaster Recovery Plan
ExBo	Executive Board
ICM	Incident & Crisis Management
ICMP	Incident and Crisis Management Procedures
ICT	Information & Communication Technology
II	Incident Identifier

IM	Incident Manager(s)
IMM	Incident Management Meeting
IMT	Incident Management Team
ISO	International Organization for Standardization
LE	Legal Entity(ies)
MS 365	Microsoft 365
OC	Overall Coordinator
RTO	Recovery Time Objective
SME	Subject Matter Expert
ToRs	Terms of Reference