

Special Organisational Structure (BAO) for Crises Management

Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH

4 January 2016	
Approved by:	Chair of the Management Board
Author:	OE0D10, M Wagner, S Frieber
Departments/units involved:	OE0D10, Corporate Communication, Personnel Department, ELVIS, task force "delivery", Medical Services, Facility Management
CC:	GIZ Management Board, Departments 1-8
Version; version date:	V 1.8., 26 June 2016
	Field Version
Next review:	December 2016
Purpose:	Description of the procedures and structures used for crisis management at GIZ.

1. Definition	4
2. General information	4
3. The special organisational structure	5
3.1. The CMT at field level – members and roles	6
3.1.1. Manager of the field level CMT (person responsible: the country director or his/her deputy)	6
3.1.2. Crisis coordinator/ Risk Management Advisor/Security Focal Point.....	6
3.1.3. Documentation/administrative support	6
3.1.4. PR/HR and distribution of information	7
3.1.5. Status updates	7
3.1.6. Logistics and security	8
3.1.7. On-site Crisis Management Team (CMT)	8
3.3. Members and roles of the Head Office CMT	10
3.3.0. Management Board.....	10
3.3.1. Crisis officer	10
3.3.2. Cooperation with personnel in stress, conflict and crisis (COPE)	11
3.3.3. Director general of departments, director of divisions	11
3.3.4. Press Office/Corporate Communications Unit	11
3.3.5. Head Office country manager, regional division	12
3.3.6. HR Services	12
3.3.7. Facility Management – non-permanent member; where necessary.....	12
3.3.8. GIZ Medical Services – non-permanent member; where necessary.....	13
3.3.9. Commercial crisis advisory services help desk– non-permanent member; where necessary	13
3.3.10. Legal Affairs and Insurance Unit – non-permanent member; where necessary	13
3.3.11. ELVIS – Information Technology – non-permanent member; where necessary	14
4. Communications in times of crisis – Head Office.....	14
5. HR pool for crisis management at GIZ.....	17
6. Raising the alarm at the Head Office CMT.....	18
7. Psychosocial emergency assistance.....	19
8. Emergency and continuity planning, Head Office	25
8.1. Breakdown of communication systems in Germany	25
8.2. Breakdown of IT systems in Germany	26
8.3. Unavailability of the Crisis Room at GIZ Head Office.....	27
8.4. Loss of power supply.....	27
8.5. Power cut – Loss of power supply, internet, servers etc.	28
8.6. Around-the-clock operations.....	29

8.7. Absence of Head Office CMT staff31

8.8. Working outdoors, from home or at an alternative location31

Annex C – Notification – telephone cascade.....32

Annex D – Security briefing for information purposes – ‘Information Report – Current Situation’33

Annex E – Security briefing for decision-making purposes – ‘Situation Report for Decision Making’34

Annex F – Decision-making.....35

Annex J – GENESYS conference call40

Annex M – After action review42

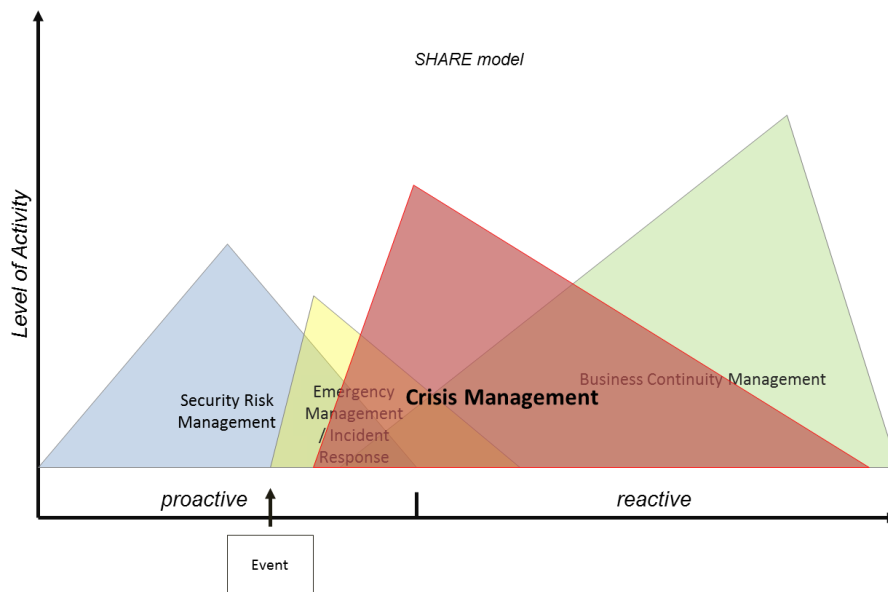
Annex N – Report on lessons learned43

1. Definition

According to the German Federal Office of Civil Protection and Disaster Assistance (BBK), a crisis is an abnormal incident or event. As defence mechanisms are vulnerable or may already have been damaged, existing procedures and structures can no longer cope and a 'special organisational structure' is required to deal with the situation (BBK glossary 2011, p. 17, currently available in German only).

2. General information

GIZ's special organisational structure for dealing with crises is an integral component of the company's Business Continuity Management strategy and constitutes part of its overall concept for a security and risk management system.



Overall responsibility for the special structure lies with the Management Board, which appoints company crisis officers to implement GIZ's crisis management policy in the event of an incident. The officers arrange for and coordinate the assignment of a Head Office Crisis Management Team. Decisions are made at the director of division level and the directors general of departments and Management Board are to be consulted where necessary. The decision-makers are assisted by an **operational and tactical** component (the *on-site Crisis Management Team*) and an **administrative and organisational** component (the *Head Office Crisis Management Team*).

The on-site Crisis Management Team (CMT) is responsible for responding to incidents at a local level. In consultation with the Head Office CMT, it communicates with local staff and with German officials (at the embassy, for example) in the country of assignment. In this context, the country director makes and bears responsibility for decisions at the

operational level. The on-site CMT is responsible for documenting crisis management procedures locally.

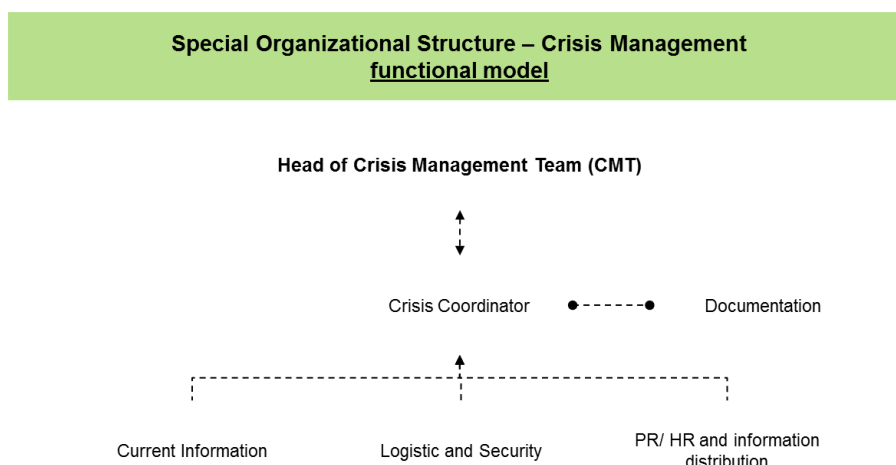
The Head Office CMT is responsible for overarching decisions and for communication within the company, with commissioning parties and clients and with the German Federal Government's crisis response units. It also assists the on-site CMT in carrying out administrative and organisational tasks. Where necessary, the Corporate Security Unit sends a crisis manager to the country of assignment to provide support for the team.

Unlike other crisis management models, in the GIZ model the crisis officer is only responsible for managing and coordinating the Head Office CMT and does not make any decisions that go above and beyond this team's organisational structures. Such decisions are made at other levels in GIZ's hierarchical structure, for example, by directors of division, directors general of departments or the Management Board.

3. The special organisational structure

Functional model:

In terms of the tasks that need to be carried out to respond to an incident, GIZ's crisis management system must cover six areas that go above and beyond the normal boundaries of crisis management to a significant degree. This functional model is geared to operational and tactical needs and can be tweaked to accommodate involvement of the Head Office CMT.



In cases where a crisis affects several countries within an entire region, an on-site CMT is set up in each of the affected countries. These teams coordinate their activities and

exchange information on the shared incident or event (e.g. tsunami, earthquake, pandemic, or cross-border, regional conflict).

3.1. The CMT at field level – members and roles

3.1.1. Manager of the field level CMT (person responsible: the country director or his/her deputy)

- Manages and coordinates incident response measures locally
- Makes and bears responsibility for operational decisions
- Develops and communicates the operational approach and strategy
- Communicates information on a crisis to local GIZ staff and media and to other actors (in consultation with the GIZ Press Office/Corporate Communications Unit and in line with the duties listed in section 3.1.4.)
- Is responsible for the work carried out by the on-site CMT

3.1.2. Crisis coordinator/ Risk Management Advisor/Security Focal Point

- Organises the CMT
- Coordinates the work carried out by the on-site CMT and contributions made by support components
- Recommends potential emergency response strategies to the on-site CMT
- Coordinates operational aspects of evacuations in response to medical emergencies and security threats
- Reports to the Corporate Security Unit at routine intervals
- Communicates with local and international security networks on site
- Gives the security briefing for advisory purposes
- Gives the security briefing for decision-making purposes
- Steers and implements after action reviews and reports on lessons learned.

3.1.3. Documentation/administrative support

- Keeps an 'incident diary'
- Writes and distributes minutes of meetings
- Operates the general phone line (on-site phone) and ensures that the Corporate Security Unit's "Crisis Desk" can be contacted at all times
- Welcomes visitors
- Updates information on the Head Office CMT (Annex K)
- Assists in compiling staff schedules and plans of operations

- Updates an overview of (ongoing and incident-specific) deadlines for the CMT

3.1.4. PR/HR and distribution of information

- Coordinates information on crises with the Head Office CMT (member: Press Office/Corporate Communications Unit)
- Deals and communicates with local media in consultation with GIZ's Press Office/Corporate Communications Unit
- Prepares briefings
- Prepares statements and presentations in consultation with the manager of the on-site CMT/country director, GIZ's Press Office and Corporate Communications Unit for communication with media representatives on site
- Prepares speaker's notes for interviews and press conferences in consultation with GIZ's Press Office/Corporate Communications Unit
- Gathers and prepares relevant information on the affected staff (personal information/personnel list etc.)
- Assists GIZ's Press Office/Corporate Communications Unit in preparing updates for the intranet
- Prepares/writes obituaries for deceased staff members
- Liaises and coordinates with HR Management at Head Office
- Sets up and runs a hotline if necessary
- Arranges staff meetings and provides information¹

3.1.5. Status updates

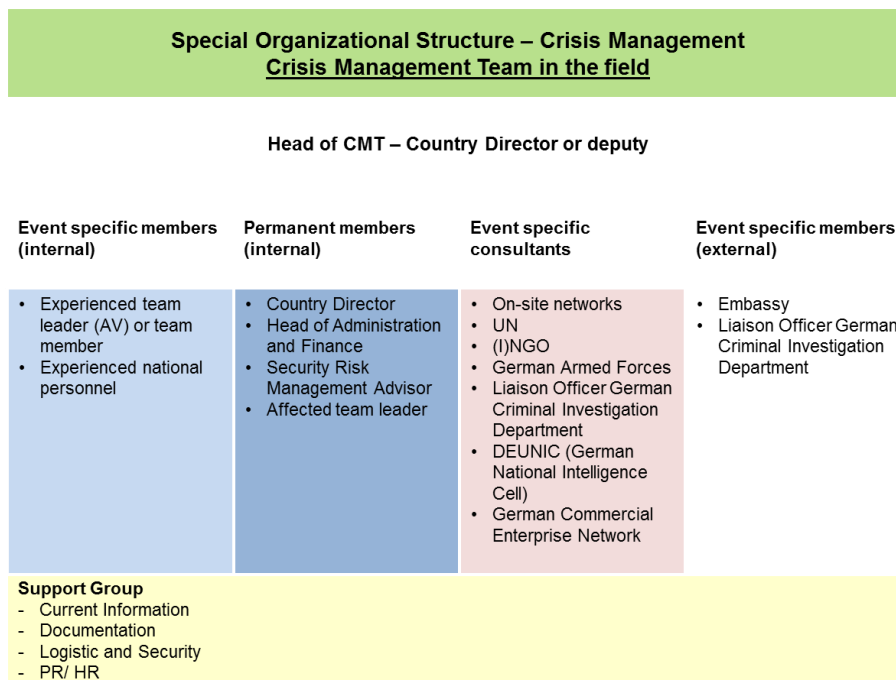
- Collects information from local networks and local/international media
- Observes the situation
- Keeps an eye on social media reports – Facebook, Twitter etc.
- Analyses security-related information
- Devises courses for action
- Drafts responses to different scenarios and to potential developments
- Communicates with and exchanges information with the security network on site

¹ In the event of a crisis, information is not usually communicated to staff in writing. Staff members still need to be kept informed about what is going on, so as a rule of thumb, GIZ's official policy during times of crisis is for management to communicate any information verbally to the workforce rather than in writing.

3.1.6. Logistics and security

- Implements any security measures required immediately
- Prepares alternative premises as meeting points/safe houses
- Prepares a vehicle pool
- Prepares and maintains communication equipment (radio devices, satellite phones and internet)
- Provides logistical and administrative support for the CMT and provides assistance in responding to events
- Implements relocations²/evacuations³
- Ensures that there are sufficient reserves of fuel, food and water

3.1.7. On-site Crisis Management Team (CMT)



The CMT in the field is appointed and coordinate by the country director. He/she also heads up the team. The team is convened when an incident occurs that attracts a lot of media attention or that could potentially damage GIZ's reputation or put the lives of GIZ staff members at risk. It is also set up

² In a security context, relocation describes the (temporary) removal of staff from a particularly dangerous area in a country. Staff may need to be relocated from any location to another area in a town or city/region/country or to Germany or a neighbouring country.

³ Evacuation, on the other hand, describes the withdrawal of staff from a dangerous or potentially dangerous location to one that is more secure. The result is the ordered withdrawal of staff and activities following instructions that are given based on a (political) decision. Evacuation involves 'third parties' (military, service providers) and the withdrawal of staff across international boundaries.

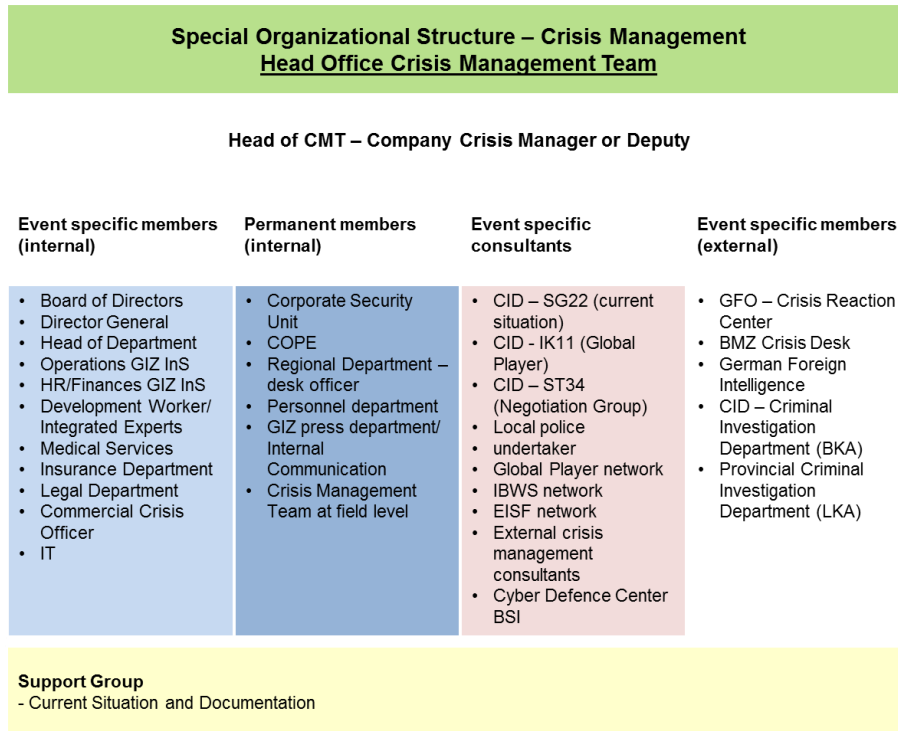
when the available resources are no longer able to cope with an incident at the project level or when the country director believes a special team is needed to deal with a particular situation.

The country director decides who needs to be appointed to the CMT in the country in question. Team members are appointed on the basis of who is best equipped to carry out the tasks in hand, not on their role in GIZ's hierarchy. A person's expertise, experience and ability to perform under pressure are key criteria. The CMT is made up of its permanent members at the very least.

The country director must decide on a deputy system so that all roles in the team are covered at all times. Arrangements must also be made for the team to work in shifts in the event of a large-scale crisis.

The main mandate of the on-site CMT is to respond to incidents and to implement emergency aid measures to deal with crises. The team also communicates with the CMT at Head Office (Corporate Security Unit) as the single point of contact.

3.2. Head Office Crisis Management Team (CMT)



Where necessary, GIZ's Head Office crisis officer appoints an official crisis management (CMT for short) to respond to a crisis.

3.3. Members and roles of the Head Office CMT

3.3.0. Management Board

- Bears responsibility for crisis management at GIZ
- Is informed about proposed key company decisions by the manager of the Head Office CMT
- Decides on corporate strategy measures

3.3.1. Crisis officer

- Heads up and coordinates the CMT at GIZ Head Office
- Provides technical advice to Head Office managers (directors of division, directors general of department) and to management
- Liaises with official and unofficial networks
- Liaises with and reports to the German Federal Government's crisis response units (BMZ's crisis management division; the AA's Crisis Response Centre)
- Provides the Management Board with status updates

- Has a right to veto decisions made in relation to the risk of imminent danger if decisions made at the operational level (by directors of division, directors general of department, the CMT or country director) poses a risk to the company or its staff
- Is responsible for the work carried out by the Head Office CMT
- Gives the security briefing for advisory/decision-making purposes and arranges for work inputs to be provided as part of the CMT's support role
- Is responsible for documenting the crisis
- Commissions the after action review and the report on lessons learned

3.3.2. *Cooperation with personnel in stress, conflict and crisis (COPE)*

- Advises the CMT on issues related to psychosocial emergency assistance
- Provides support and advice to affected staff members on how to deal with emotional and physical stress
- Liaises with and supports family members and survivors
- Liaises with official and unofficial psychosocial emergency assistance networks (the German Federal Office of Civil Protection and Disaster Assistance (BBK) and its central Coordination Office (NOAH), the interministerial specialist group for psychology, health authority/psychosocial emergency assistance), as well as therapeutic services (offered by doctor's surgeries and clinics)
- Is responsible for psychosocial emergency assistance

3.3.3. *Director general of departments, director of divisions*

- Is appointed by the CMT
- Makes decisions on matters in his/her own area and bears responsibility for these
- Can fine-tune the details of or make changes to decisions made by the on-site CMT
- Can request security briefings for advisory/decision-making purposes
- Ensures the on-site CMT compiles an after action review/report on lessons learned

3.3.4. *Press Office/Corporate Communications Unit*

- Advises the Head Office CMT on communicating information in a crisis
- Coordinates activities with the German Government's press divisions

- Compiles information on what is being reported in the media and observes social media
- Advises the country director on communicating with staff and with local media
- Compiles and distributes intranet bulletins and press releases; bears responsibility for internal communication
- Is responsible for external communication
- Prepares statements for the press and press conferences where necessary
- Acts as GIZ's spokesperson where necessary
- Provides work inputs for the Head Office CMT
- Provides work inputs for the security briefing for advisory/decision-making purposes

3.3.5. Head Office country manager, regional division

- Supports the Head Office CMT by providing relevant information on staff, projects and the situation on the ground
- Represents the regional division's point of view
- Provides work inputs for the Head Office CMT/Supports the Head office CMT
- Ensures that up-to-date GIZ office personnel lists are available
- Provides work inputs for the security briefing for advisory/decision-making purposes
- Assists the Head Office CMT in implementing measures to support victims and their relatives

3.3.6. HR Services

- Advises the Head Office CMT
- Steers regulations relating to business trips, luggage, household goods, the status of staff etc.
- Provides work inputs for the Head Office CMT
- Provides work inputs for the security briefing for advisory/decision-making purposes

3.3.7. Facility Management – non-permanent member; where necessary

- Advises the Head Office CMT
- Organises procedures in its area of responsibility (Germany)
- Liaises with local German authorities at GIZ locations in Germany

- Supports the Head Office CMT by providing suitable infrastructure, premises and aids (e.g. organising for flags to be flown at half-mast as a mark of respect)
- Organises for representatives of the press to obtain access to GIZ's premises
- Provides work inputs for the Head Office CMT
- Provides work inputs for the security briefing for advisory/decision-making purposes

3.3.8. GIZ Medical Services – non-permanent member; where necessary

- Advises the Head Office CMT in cases where staff are injured or need to be evacuated for medical reasons
- Is responsible for advising injured staff
- Is in charge of coordinating and communicating with MedEvac's framework agreement partners/service providers involved in medical evacuations for which it is responsible
- Provides work inputs for the Head Office CMT
- Provides work inputs for the security briefing for advisory/decision-making purposes

3.3.9. Commercial crisis advisory services help desk– non-permanent member; where necessary

- Advises the regional departments and the field structure on commercial risk management
- Is the first point of contact for coordinating the clarification of commercial issues among the responsible departments/units that support the field structure
- Supports the field structure in the event of a crisis
- Advises the Head Office CMT
- Provides work inputs for the Head Office CMT
- Provides work inputs for the security briefing for advisory/decision-making purposes (where necessary)

3.3.10. Legal Affairs and Insurance Unit – non-permanent member; where necessary

- Advises the Head Office CMT on legal and liability issues
- Advises the Head Office CMT on insurance issues
- Provides work inputs for the Head Office CMT
- Provides work inputs for the security briefing for advisory/decision-making purposes (where necessary)

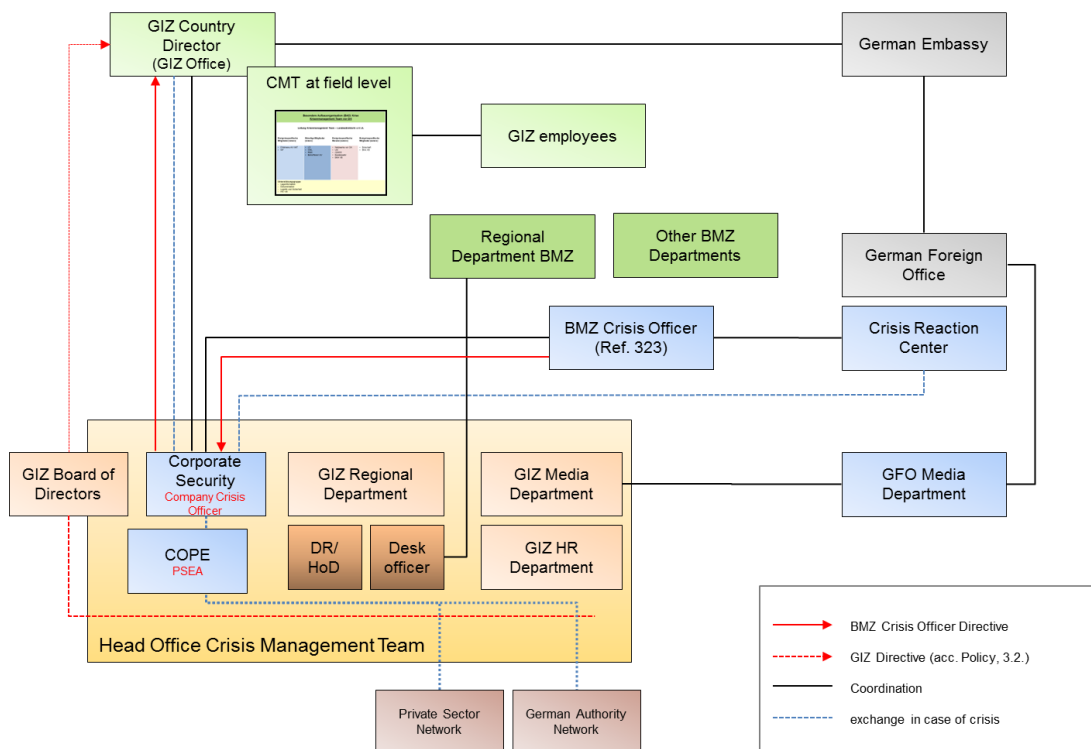
3.3.11. ELVIS – Information Technology – non-permanent member; where necessary

- Advises the Head Office CMT on cyber-attacks (DD4BC/DDos attacks)
- Acts as single point of contact to the cyber defence centre of the German Federal Office for Information Security (BSI) and as the key contact for the police
- Provides work inputs for the Head Office CMT
- Provides work inputs for the security briefing for advisory/decision-making purposes (where necessary)

4. Communications in times of crisis – Head Office

In the event of a crisis, GIZ's Head Office crisis officer is the single point of contact for distributing information within the company and for liaising with the Federal Government's crisis response units.

GIZ's Crisis Management Teams (CMTs) and the Federal Government units have agreed the following procedure for communicating information in crisis scenarios.



On behalf of the Head Office CMT, the Head Office crisis officer provides the Management Board with regular status updates.

Independently of this, GIZ country directors communicate with the German embassies in the relevant partner countries in their role as manager of the on-site CMTs. The embassies in turn use their reporting system to update the Crisis Response Centre at the German Federal Foreign Office (GFO).

The press offices of GFO/AA and GIZ have agreed to cooperate closely and to coordinate communication strategies in the event of a crisis⁴.

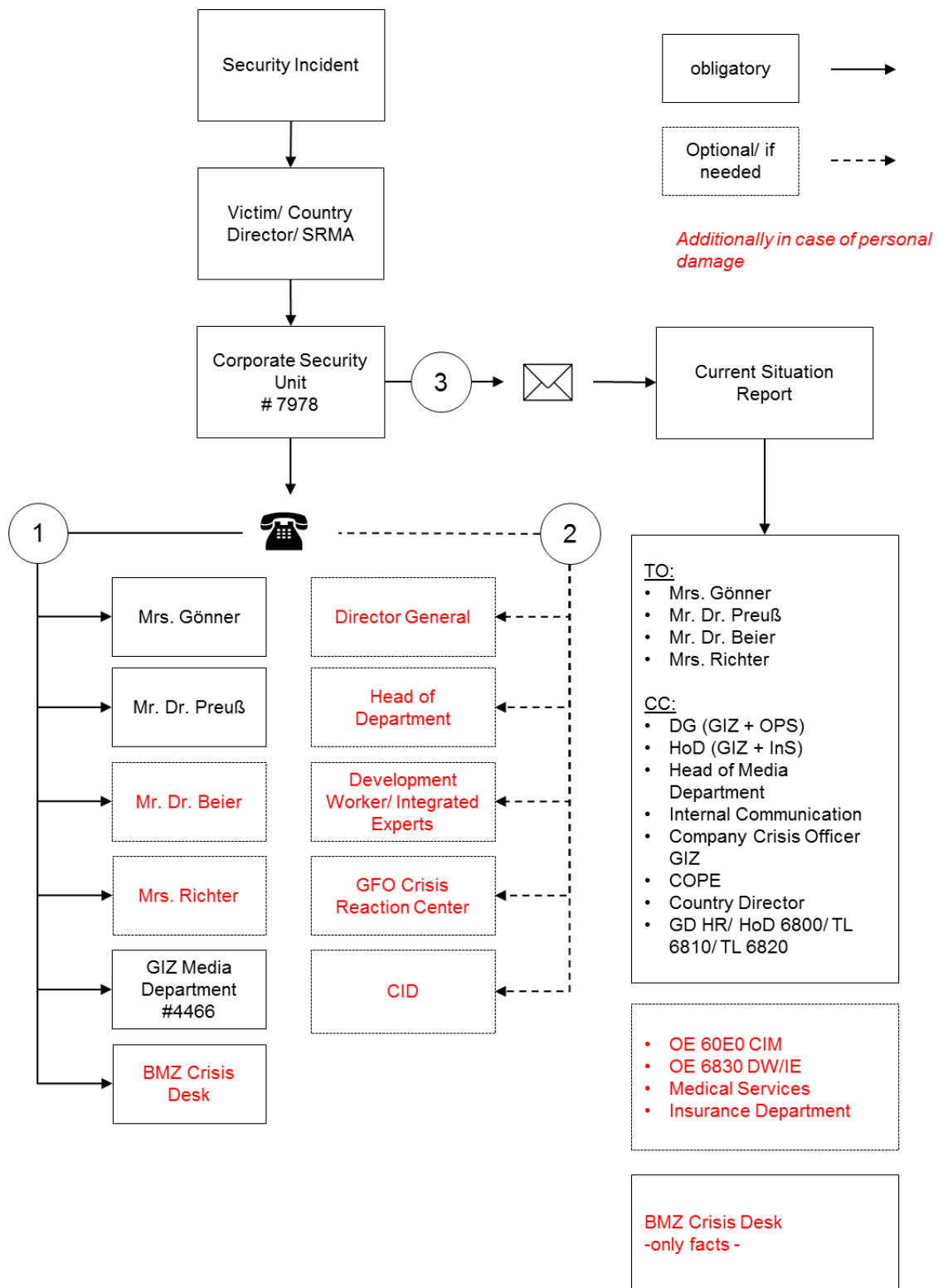
Status updates to GIZ's Management Board

GIZ's Management Board has put in place procedures that must be followed throughout GIZ in the aftermath of security-related incidents.

If there is heightened media interest or if staff or property have been injured or damaged in the incident, the Corporate Security Unit informs the Chair of the Management Board, the Labour Relations Director and the Press Spokesperson directly by phone. A status update is then sent to all of the members of the Management Board and to all of the names on the crisis distribution list.

In cases where staff have been injured or kidnapped, all of the actors highlighted in black and red in the diagram are informed by phone (priorities 1 and 2) and in writing (priority).

⁴ https://intranet.giz.de/cps/rde/xchg/giz_intranet/XSL/hs.xsl/-/HTML/39257.htm



⁵ The steps to be followed in the event of an incident that is not security or crisis-related (e.g. a medical emergency) are laid down in the procedures for the responsible organisational units.

5. *HR pool* for crisis management at GIZ

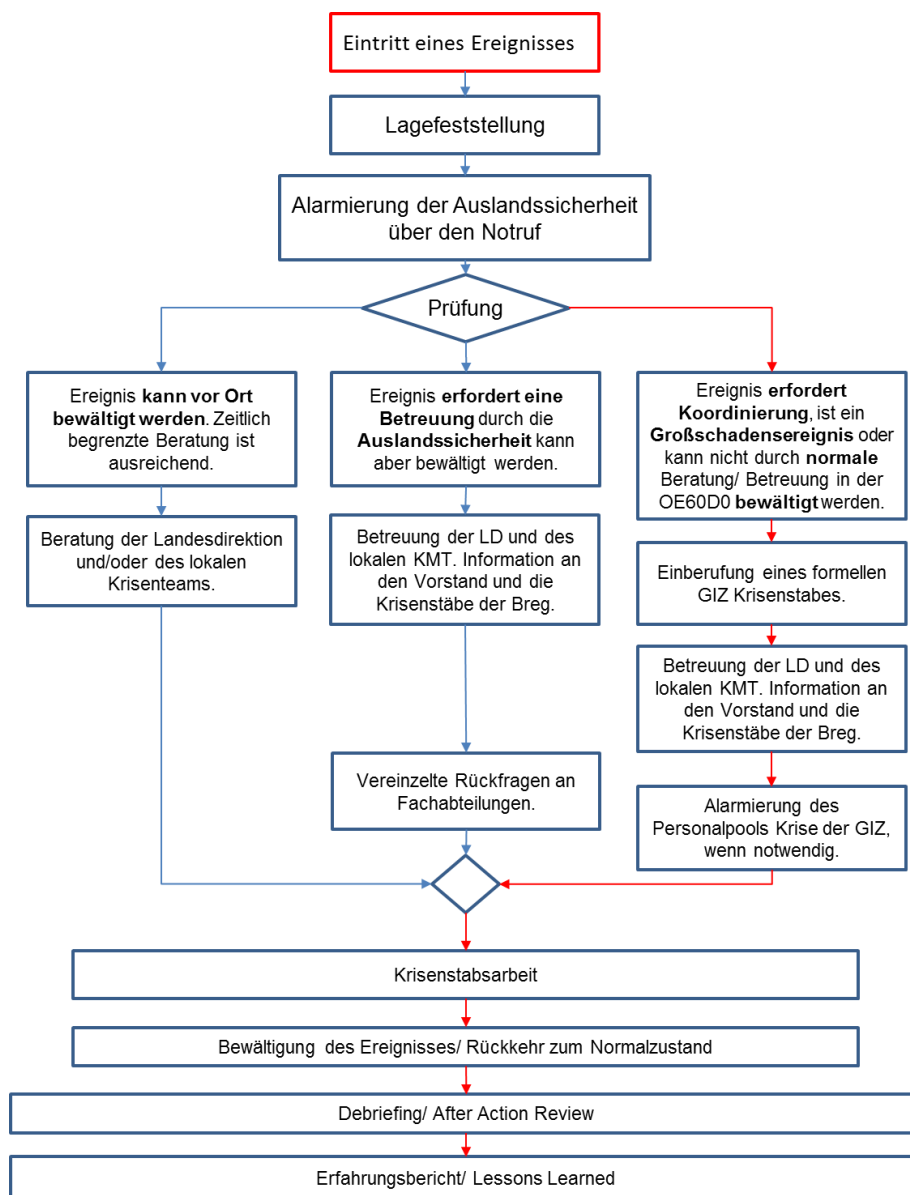
The Corporate Security Unit has a pool of staff at GIZ Head Office in Eschborn who can be released from their internal roles at short notice and assigned to crisis management duties.

Should the need arise, the head of the HQ CMT is authorised to release staff from their day-to-day roles at GIZ and assign them to their team. The relevant directors of division must be informed of the temporary transfer.

6. Raising the alarm at the Head Office CMT

If an incident occurs, the company crisis officer or the head of HQ CMT use the information provided in the emergency phone directory/Germany (yellow list) to notify the permanent members of the team.

The HR Services division routinely distributes the 'yellow list' to the Corporate Security Unit, the directors of division/directors general of departments and to the Management **Board**.



Depending on the nature of the incident that has taken place, event specific members of the CMT are notified directly by email or by phone and are assigned to the team. GIZ Medical

Services calls on its COPE psychologists – who are permanent members of the team – if the victims of a crisis need specialist support.

If it is evident from the outset that shift work will be required or that team members need to be replaced, reinforcements from the HR pool receive direct notification of their assignment.

The manager of the Head Office CMT decides whether the team members need to be based at GIZ Head Office in Eschborn or whether they can work from home or from another location.

Participation in the HR pool is an additional, voluntary duty and members are not paid to be on call. GIZ grants time off in lieu of overtime.

7. Psychosocial emergency assistance

7.1. Basic principles and objectives

The current version of the quality standards and guidelines of the German Federal Office of Civil Protection and Disaster Assistance (BBK) provide the baseline for psychosocial emergency assistance in Germany. For GIZ, implementation of the minimum standards for occupational health and safety during field assignments (08/2008), which are laid down by the German Federal Ministry of the Interior for statutory accident insurance offered by the statutory insurance company UVB (formerly known as the Federal Government Accident Insurance Scheme – UK Bund) is strongly recommended.

Typical scenarios in which psychosocial emergency assistance is provided at GIZ include:

- Initial care for the victims of violence or an accident (e.g. following a car accident, robbery, break-in, sexual assault or attack)
- Frontline counselling for relatives and colleagues (e.g. following a kidnapping or missing person incident, death or serious injury)
- Medium and long-term support for staff members affected by violence (e.g. following an attack or kidnapping) and assistance in the reintegration process
- Support for organisational units affected by a particular incident

The overarching objectives of psychosocial emergency assistance are to:

- Prevent post-traumatic stress
- Detect post-traumatic stress at an early stage following an accident or incident during an assignment
- Provide appropriate support and assistance to help individuals and groups process trauma and deal appropriately with any post-traumatic stress and excessive psychological strain experienced during an assignment

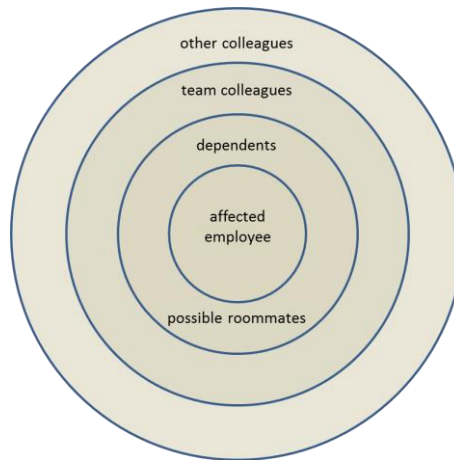
Counsellors in GIZ's Corporate Security Unit are responsible for providing psychosocial emergency assistance at GIZ. They also advise the Head Office CMT on psychosocial elements of crisis management and help liaise with family members and survivors.

During a crisis, COPE liaises with existing contacts in official and unofficial psychosocial emergency assistance networks (the German Federal Office of Civil Protection and Disaster Assistance (BBK) and its central Coordination Office (NOAH), the interministerial specialist group for psychology, health authority/psychosocial emergency assistance) and with experts in therapeutic services (at doctor's surgeries and clinics)

7.2. Target groups

GIZ's psychosocial emergency assistance measures target staff members directly affected by an emergency or stressful event during a foreign assignment. They also cater for their family members or housemates (who are usually colleagues at locations that are not suitable for families), managers of the relevant unit and any colleagues who may be indirectly affected.

Circles of Impact



Support for victims and their family members is provided directly in counselling sessions (sometimes by phone) or in the form of guidelines, information leaflets, measures to diagnose post-traumatic stress at an early stage, support services or referral to appropriate therapy offered by third parties. Advice is also provided to managers and organisational units on how to deal with survivors and their team members.

In addition to counselling and supporting victims, COPE also assists the affected security and risk management advisors and the on-site CMT in preventing and dealing effectively with post-traumatic stress (follow-up discussion).

In the event of a crisis, the COPE emergency hotline can also be used to liaise with victims and their family members, managers and colleagues. Additional services can be offered where necessary.

7.3. Structure of psychosocial emergency assistance services; roles

In the event of a large-scale incident or complex, high-risk situations, individuals must be appointed to the following psychosocial emergency assistance service roles. The exact nature of the tasks assigned to each role will depend on the specific context:

7.3.1. Psychosocial emergency assistance coordinator

The psychosocial expert assigned to the Head Office CMT is responsible for coordinating emergency assistance measures at GIZ. Duties include:

- Advising the CMT on setting up emergency assistance structures for the particular incident and implementing them in an efficient (and cost effective) manner
- Identifying and monitoring needs, compiling an overview of the available resources (including regulations on replacement/deputies and shift work, inter/supervision, maintaining a good work-life balance, coordinating leave, the assumption of costs)
- Liaising with the assigned experts and coordinating the emergency assistance measures implemented
- Communicating with other actors involved in crisis management
- Acting as a contact for external organisations (the central Coordination Office of the German Federal Office of Civil Protection and Disaster Assistance (NOAH), the German Federal Foreign Office (AA), etc.)
- Documenting the assignment and evaluating the lessons learned

Depending on the severity of the crisis, additional roles may be required in this context. These include:

7.3.2. Deputy coordinator

- Represents the psychosocial emergency assistance coordinator
- Is responsible for quality assurance
- Carries out support tasks
- Notifies the coordinator of the outcome of counselling sessions

7.3.3. On-site psychosocial emergency assistance expert

In certain situations, a psychosocial emergency assistance expert may need to be seconded to provide on-site counselling for victims and teams in the short term

7.3.4. Corporate Security Unit hotline operator (1188 – 'First point of contact')

Is responsible for dealing with initial contact – which is usually an emotional experience – and for identifying information and counselling requirements, verifying authenticity (ensuring individuals are not 'undercover' reporters and that they belong to appropriate target group), screening, and forwarding individuals to the right contact within GIZ

7.3.5. Counsellor/case manager:

Conducts counselling/support sessions with victims and/or family members, documents proceedings, networks with other actors within/outside of GIZ, forwards case to support network. Where possible, at least one counsellor should be assigned to each case/victim/family. If more than one family is affected, a family is considered as one 'case'.

7.3.6. Support expert for managers and teams:

Advises the relevant managers on what action they need to take in order to fulfil their duty of care; runs team workshops and similar measures to advise teams that are indirectly affected.

7.3.7. Crisis support team members (psychosocial emergency assistance):

As staffing resources can quickly become overstretched due to the scale of demand for psychosocial services following complex incident or high-risk situations or the occurrence of several traumatic incidents at once, it is advisable to set up a crisis support team at GIZ. Ideally, this team should be made up of between five and ten individuals from other organisational units who have the expertise required to deal with the situation in hand. It should support and reduce the workload of the psychosocial emergency assistance team where appropriate. Duties could include (depending on an individual's qualifications) intermittent operation of the hotline or carrying out support tasks. Once the crisis support team is in place, the team members should be assigned on temporary placements and receive relevant training to enable them to carry out their tasks effectively.

7.4. Quality assurance of psychosocial emergency assistance services at GIZ

7.4.1. Training standards

All actors involved in psychosocial emergency assistance services at GIZ are to be trained in accordance with the guidelines laid down by the German Federal Office of Civil Protection and Disaster Assistance (BBK). Psychosocial experts must be qualified in the field of emergency psychology, in line with the standards set by the Association of German Professional Psychologists (BDP) or they must receive equivalent further training in psycho-trauma therapy. Support staff must also receive the training they require to carry out their tasks effectively.

7.4.2. Intervision

The discussion of individual cases and peer-to-peer exchange on specific issues that arise are an important component of ongoing quality assurance. It goes

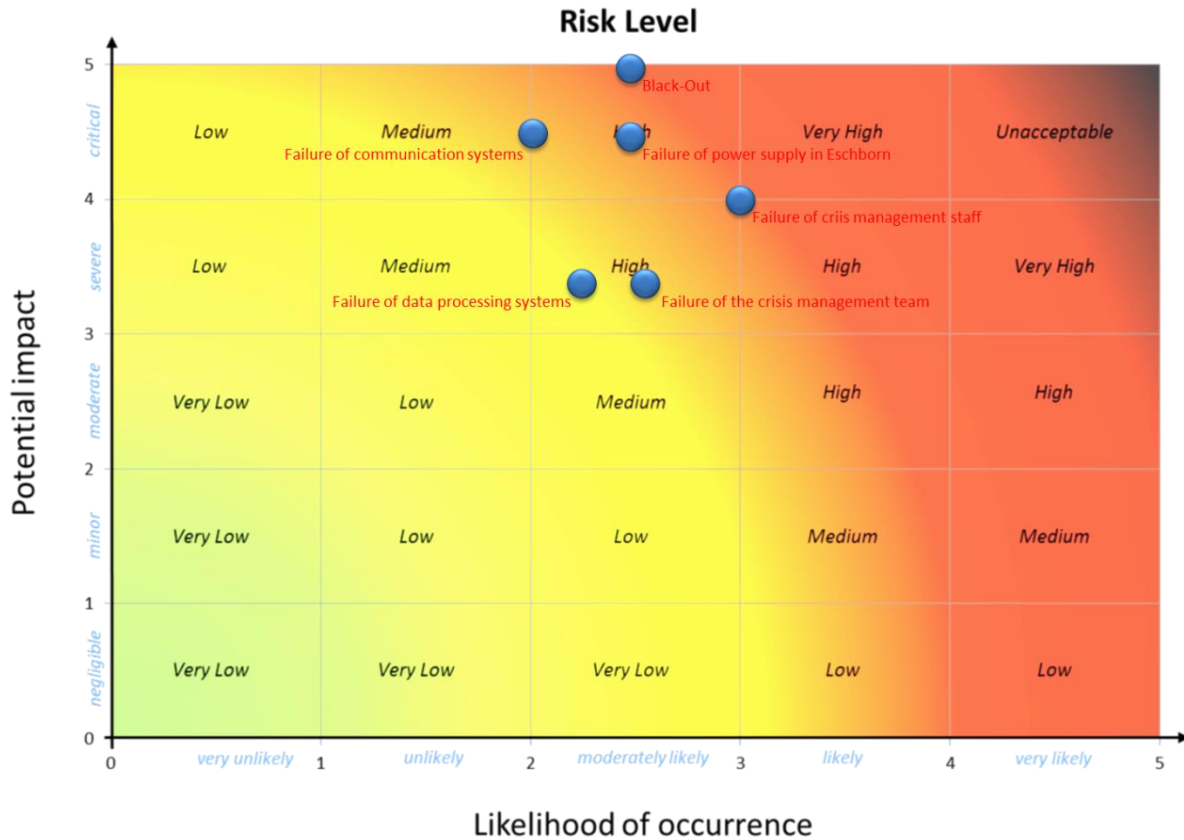
without saying that all staff involved in providing psychosocial services are obliged to observe strict confidentiality at all times. In cases where the individual concerned is an endangerment to him/herself or to others, the 'four-eye' principle must be observed in order to minimise risks. In other words, the case manager gets a second opinion by keeping a second expert updated on the case and discussing key steps with him/her.

7.4.3. Supervision

A suitably qualified, external supervisor carries out routine supervision sessions in order to safeguard quality assurance, ensure that services are provided in a professional manner and make any improvements that are required. These sessions also provide a platform for boosting cooperation within the team and with other organisational units where necessary and for psychosocial counsellors to work through any job-related stress that they experience themselves.

8. Emergency and continuity planning, Head Office

When the special organisational structure for crises was being drafted, a risk assessment was carried out for different scenarios.



The following sections outline the risks identified in the relevant context. The red triangle icons (△) represent residual risks and identify issues that require further clarification.

8.1. Breakdown of communication systems in Germany

Assumption: All mobile phone and landline networks throughout Germany do not operate due to a fault, a terror attack, an overloaded network or hacking.

Assessment: Under the current circumstances, there is a realistic possibility that such a situation could occur and affect GIZ. The potential damage is regarded as serious as a lack of alternative systems would result in the complete failure of the crisis management system.

Contingency plan:

- a) The Corporate Security Unit has a BGAN 300 portable phone and internet satellite terminal, which currently operates on a prepaid basis.

- △ Communication by phone/internet is no longer possible once the remaining credit is used.
- b) The Corporate Security Unit also has an IRIDUM satellite phone, which can be used when the mobile or fixed network is inaccessible. The device currently operates on a prepaid basis.
 - △ Communication by phone is no longer possible once the remaining credit is used.
- c) The core team members of the Corporate Security Unit have laptops that can be powered by solar chargers.

8.2. Breakdown of IT systems in Germany

Assumption: IT systems (laptops, printers, photocopiers, email servers etc.) do not function.

Assessment: Under the current circumstances, there is a realistic possibility that GIZ's IT systems could fail as a result of age or a technical defect. The potential damage is regarded as serious as a lack of alternative systems would result in significant restrictions to and even the complete failure of the crisis management system.

Contingency plan:

- a) The Corporate Security Unit has a BGAN 300 portable phone and internet satellite terminal, which currently operates on a prepaid basis.
 - △ Communication by phone is no longer possible once the remaining credit is used.
- b) The use of standalone devices in the offices of the Corporate Security Unit could compensate for the breakdown of multifunctional network devices (such as copiers, scanners and printers).

Device	Room	CODE no.	Function
RICOH 4100NL	ED34075/Wagner	DE1BXE	Printer b/w
RICOH MP 161 SPF	ED34074/Crisis	DE2DCC	Printer, scanner, copier

c) Breakdown of email servers:

Continued operation of the crisis management team by phone (where available) and detailed manual documentation.

NYXEOS.net server: This operates independently of a connection to power, a server or the internet. It connects all crisis response units in German authorities as well as participating companies. The system is based on an independent server that runs an intranet system within Germany that is not internet-based and can be used in the event of a crisis. Each participant is assigned a static, fixed IP address via a satellite connection established using a fixed internet satellite terminal (such as BGAN). NYXEOS.net can be used in the event of an emergency or crisis to communicate with German authorities and companies. Use could also be extended to outside Germany.

8.3. Unavailability of the Crisis Room at GIZ Head Office

Assumption: The Crisis Room at GIZ Head Office is not available due to an incident (such as a fire or terror attack).

Assessment: Under the current circumstances, there is a slight possibility that GIZ's Crisis Room could be completely inaccessible. The potential damage is regarded as significant.

Contingency plan:

- a) The Corporate Security Unit is able, either independently or together with other units, to set up a CMT and operate it for a limited period of time.
 - △ This contingency plan relies on the availability of a) electricity and b) credit for the emergency communication systems.

8.4. Loss of power supply

Assumption: There is a loss of power supply in Eschborn and the surrounding area.

Assessment: Under the current circumstances, there is a realistic possibility that the power supply at Head Office Eschborn could be restricted or break down completely. The potential damage is regarded as serious as there is currently no emergency plan that prioritises work areas and emergency power can only be provided for ten working hours.

Contingency plan:

- a) Facility Management provides an emergency power supply to GIZ Head Office in Eschborn that would safeguard operations for a limited period. After a

downtime of about 60 – 90 seconds, power is fed to the brown sockets in offices. GIZ Eschborn's emergency power units can provide about **10 hours'** emergency power to offices.

△ The Corporate Security Unit currently has no battery backup system that would safeguard the continued operation of vital technology in the event of a crisis.

△ If emergency power were to be turned off or run out at GIZ Head Office in Eschborn, there would be a complete blackout.

8.5. Power cut – Loss of power supply, internet, servers etc.

Assumption: There is a complete power outage for several hours or even days due to a fault, a terror attack, overloaded network or hacking. This also results in the breakdown of all communication and IT systems.

Assessment: Under the current circumstances, there is a realistic possibility that such a situation could occur and affect GIZ. The field structure would not be able to keep in contact with the Head Office CMT. The exchange of information with other German embassies would also not be possible. The potential damage is regarded as serious as a lack of alternative systems would result in the complete failure of the crisis management system.

Contingency plan:

- a) Power supply – Facility Management provides an emergency power supply to GIZ Head Office in Eschborn that would safeguard operations for a limited period. After a downtime of about 60 – 90 seconds, power is fed to the brown sockets in offices. GIZ Eschborn's emergency power units can provide about **10 hours'** emergency power to offices.
- b) Communication – The Corporate Security Unit has an IRIDUM satellite telephone and a BGAN 300 portable phone and internet satellite terminal which can be used in emergencies.
△ CAUTION: The systems currently only operate on a prepaid basis.
- c) NYXEOS.net server: This operates independently of a connection to power, a server or the internet. It connects all crisis response units in German authorities as well as participating companies. The system is based on an independent server that runs an intranet system within Germany that is not internet-based and can be used in the event of a crisis. It can be used in the event of an emergency or crisis to communicate with German authorities and companies. Use could also be extended to outside Germany. At the moment, no GIZ location is connected to the NYXEOS server. A power cut, followed by the loss

of emergency power supply (which can run for about T+10 hours), would result in a complete communication blackout with the field structure. This would mean that the field structure would no longer be able to communicate with the CMT in Germany.

If this were to happen, GIZ Head Office's only option if it wished to continue communicating with the field structure would be to move its CMT work to the Academy for Crisis Management, Emergency Planning and Civil Protection (AKNZ) of the German Federal Office of Civil Protection and Disaster Assistance (BBK).

8.6. Around-the-clock operations

Assumption: GIZ is affected by a large-scale event (in Germany or abroad). Its Head Office CMT needs to operate around the clock, in shifts, as a result.

GIZ will reimburse any costs that CMT staff incur because they have to cancel ongoing leave or approved, impending leave, based on the principle of cost-effectiveness.

GIZ can only request staff to return from leave if this is required for urgent work reasons or if the company's operations are at risk and no viable alternatives are available. These are the only circumstances under which GIZ can call on its staff to honour its duty of allegiance and cancel leave. The request to return from leave must be reviewed and approved by the manager of the Head Office CMT/the crisis officer, in consultation with the Labour Relations Director and the staff council. Approval must be documented.⁶

Contingency plan: Run GIZ's crisis management system in 12-hour shifts.

⁶ GIZ is obliged to assume costs incurred by staff members if they need to cancel leave to respond to an emergency. This includes cancellation fees or the cost of the return journey.

Members of the Head Office CMT:

Member	Individual(s) responsible*	Deputy*
Manager of the Head Office CMT	Cornelia Schomaker Matthias Wagner	Matthias Wagner Cornelia Schomaker
COPE	Kai Leonhardt Benjamin Mueller Elvira Draschner Miriam Kapinus	Benjamin Mueller Kai Leonhardt Miriam Kapinus Elvira Draschner
Director general of department/director of division	Relevant director of division/director general of department	Deputy for director of division/director general of department
Press Office	Anja Tomic	Julia Jakob
Corporate Communications Unit	Sabine Tonscheidt	Anja Tomic
HR Services	Ulrich Heise/ Jutta Hein (or responsible HR officer)	Kordula Oberklus / Claudia Debusmann/ Jutta Hein (or responsible HR officer)
Facility Management	Detlef Kroell	Jürgen Seelbach
Commercial crisis advisory services	Harald Edling	Bettina Gruber
Medical Services	Stefanie Wagner	Sven Wegener/ Christina Neckermann
Information Technology	Eric Heinen-Konschak	to be confirmed
Corporate Security		
Documentation	to be confirmed	Oliver Sudbrink
Status update	Daniel Lay	Nora Lietzmann
Logistics and security	Nora Lietzmann	to be confirmed

*Person on duty when emergency declared at GIZ

The Corporate Security Unit manages the overview of staff at Head Office CMT. It requests an update every three months.

A CMT representative may be seconded to the Federal Government's crisis response units provided that the individual in question a) agrees to a security clearance check and b) has experience in working in a crisis management team at the central level⁷.

Currently, three head-office staff members have 'secret' security clearance (level SÜ2).

⁷ e.g. in a federal authority

In the event that a large-scale incident continues after normal working hours (9.00 – 17.00) at the same time as a crisis situation in Germany (as outlined in sections 8.1. – 8.5), **the staff members of the Head Office CMT** are to present themselves at GIZ's Crisis Room in Eschborn **at their own volition** within the first **three hours** of the incident. The CMT meets to decide on tactical and strategic measures to ensure the team's ability to operate, review the assignment of personnel and safeguard internal and external communication, for example.

8.7. Absence of Head Office CMT staff

Assumption: CMT staff is not available as planned (for example, due to illness, absence, leave, business trips, lack of public transport, injury or death).

Contingency plan:

- a) The deputy takes on the role, where necessary, and notifies the HR pool, which appoints a replacement.
- b) Support is requested from affiliated companies or from the Academy for Crisis Management, Emergency Planning and Civil Protection (AKNZ) of the German Federal Office of Civil Protection and Disaster Assistance (BBK).

8.8. Working outdoors, from home or at an alternative location

Assumption: The Crisis Room in Eschborn is out of action due to an incident that prevents it from being used. Requirements: Power and communications networks are operational.

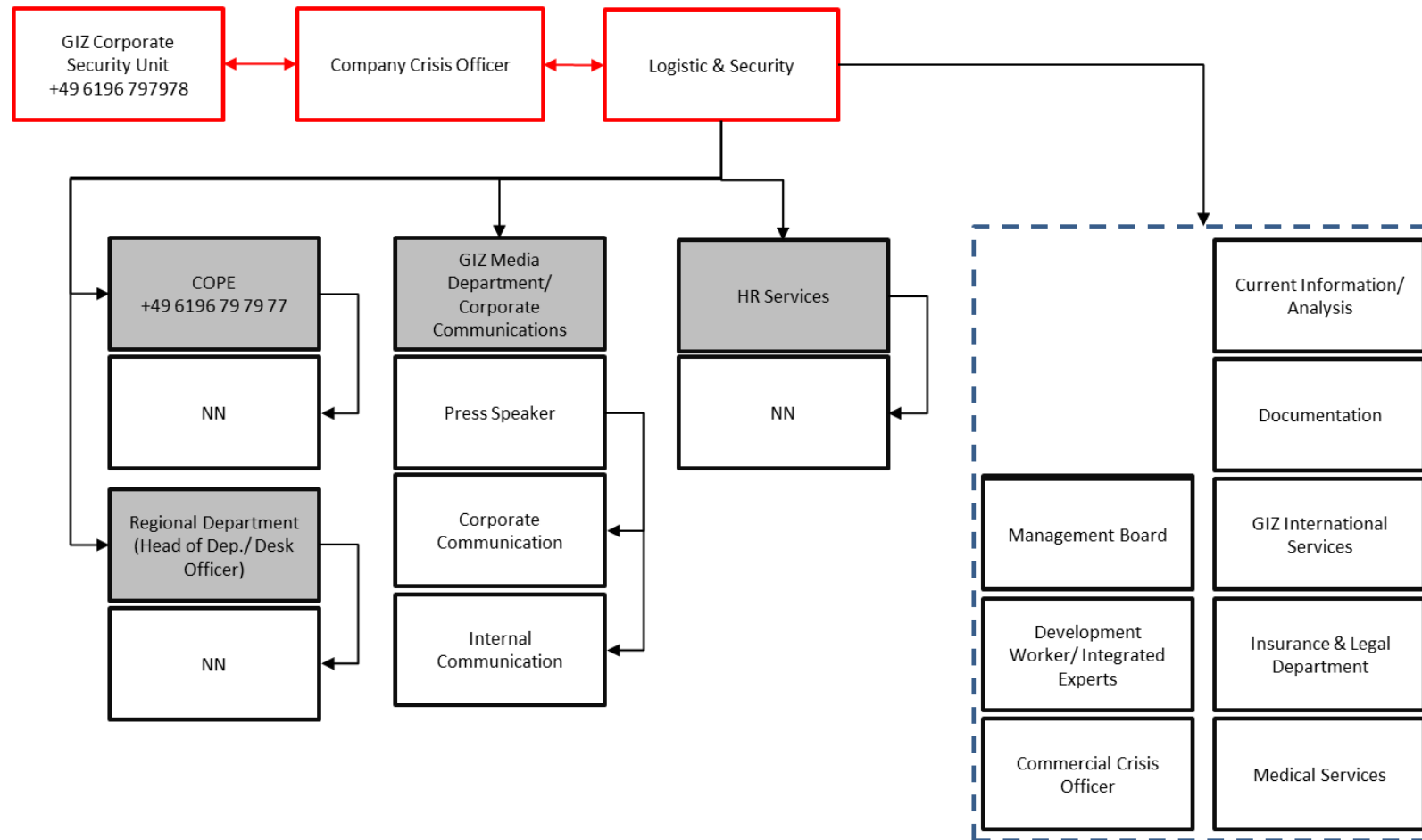
Contingency plan:

- a) The Corporate Security Unit is able, either independently or together with other units, to set up a CMT and operate it for a limited period of time. Satellite communication technology is splash-proof and can also be used outdoors.
- b) The Corporate Security Unit has a call conference system that can be used from any location using the local phone connections.
 - △ The local phone networks (landline or mobile) must be operational.
- c) If necessary, the Corporate Security Unit can be relocated to GIZ Bonn or GIZ Berlin or to the AKNZ in Bad Neuenahr-Ahrweiler, which has the infrastructural requirements for to continue business operations.

Annex C – Notification – telephone cascade

Instruction: **RED** informs **GREY**


GREY informs **WHITE** and reports back to **RED**



Annex D – Security briefing for information purposes – ‘Information Report – Current Situation’

The following format for security briefings for information purposes can also be used as an agenda and as minutes for Head Office CMT meetings. The briefing aims to present a uniform overview of the current situation for all of the members of the Head Office and CMTs at field level.

1. Brief description of the situation
2. CMT situation on-site
3. Corporate Security Unit
4. COPE
5. Regional division
6. HR Services
7. Media Department
8. Measures taken/decisions made to date
9. Miscellaneous

LVU – Information Report – Current Situation


Uto-Zentrale/Inre-Mechanik
 Unser Zentrale
 E-Mail: matthias.vagner@giz.de

Telefon: +49 6100 120-2142
Telefax: +49 6100 1200-2142
Datum: 25. November 2015

1. Current information
 Klicken Sie hier, um Text einzugeben.

2. CMT – situation in the field
 Klicken Sie hier, um Text einzugeben.

3. Corporate Security Unit
 Klicken Sie hier, um Text einzugeben.

4. COPE
 Klicken Sie hier, um Text einzugeben.

5. Regional Department
 Klicken Sie hier, um Text einzugeben.

6. HR Services
 Klicken Sie hier, um Text einzugeben.

7. Press/Media
 Klicken Sie hier, um Text einzugeben.

8. Measures/Decisions
 Klicken Sie hier, um Text einzugeben.

9. Miscellaneous
 Klicken Sie hier, um Text einzugeben.

Annex E – Security briefing for decision-making purposes – ‘Situation Report for Decision Making’

1. Brief description of the situation

1.1. *State the nature of the incident. Include the relevant facts and describe the CURRENT situation. What action has been taken so far to manage the crisis?*

2. Assessment of the situation

2.1. *Consideration of the framework in which GIZ is operating*

2.2. *Appraisal of the external factors influencing the situation*

2.3. *Appraisal of the crisis/incident*

2.4. *Appraisal of GIZ's capacities to manage the crisis*

3. Decisions made to date

3.1. *So far, what measures have been taken? How far has implementation progressed?*

4. Further need for support


4.1. *Do other actors/divisions need to be involved?*

5. Assessment of GIZ's scope for action

5.1. *Outline the different options available as well as their pros and cons. What is the timeframe? What is the likelihood of success?*

6. Proposal for action

6.1. *What do you believe is the best course of action for GIZ? Why?*

LVE – Situation Report for Decision Making


Zur Kenntnis an

Ihr Zeichen/Ihre Nachricht		Telefon	+49 6196 79-3149
Unser Zeichen	MW	Telefax	+49 6196 7980-3149
E-Mail	matthias.wagner1@giz.de	Datum	25. November 2015

1. **Brief description of the situation**
State the nature of the incident. Include the relevant facts and describe the CURRENT situation. What action has been taken so far to manage the crisis?
 Klicken Sie hier, um Text einzugeben.

2. **Assessment of the situation**
 - 2.1. *Consideration of the framework in which GIZ is operating*
Klicken Sie hier, um Text einzugeben.
 - 2.2. *Appraisal of the external factors influencing the situation*
Klicken Sie hier, um Text einzugeben.
 - 2.3. *Appraisal of the crisis/incident*
Klicken Sie hier, um Text einzugeben.
 - 2.4. *Appraisal of GIZ's capacities to manage the crisis*
Klicken Sie hier, um Text einzugeben.

3. **Decisions made to date**
 3.1. *So far, what measures have been taken? How far has implementation progressed?*
 Klicken Sie hier, um Text einzugeben.

4. **Further need for support**
 4.1. *Do other actors/divisions need to be involved?*
 Klicken Sie hier, um Text einzugeben.

5. **Assessment of GIZ's scope for action**
 5.1. *Outline the different options available as well as their pros and cons. What is the timeframe? What is the likelihood of success?*
 Klicken Sie hier, um Text einzugeben.

6. **Proposal for action**
 6.1. *What do you believe is the best course of action for GIZ? Why?*
 Klicken Sie hier, um Text einzugeben.

Annex F – Decision-making

The following sections describe the crisis management decision-making process. The situation is reassessed once the decision has been made and the corresponding measures implemented.

The security briefings for advisory and for decision-making purposes both need to be included in the documentation of the corresponding incident (incident log book).



Decision-making in the crisis management team is based on a process referred to as FORDEC.

Facts	What is the situation?
Options	What options are there for dealing with the situation?
Risks and Benefits	What risks and benefits are associated with each option?
Decision	What option has been chosen?
Execution	Implementation of the chosen option.
Check	Has the option selected produced the desired results?

Brief description of the situation:

This section provides a current overview of the situation as it stands. What has happened? What has been done so far? The information outlined here provides the baseline for managing the crisis. The following questions will help you describe the relevant facts. They are intended as a guideline only – use your discretion and decide what information is needed to move thing forward. The CMT must be able to weigh up the facts – based on confirmed and unconfirmed reports – so that each member has a good overview of the situation.

- *What happened? When? And where? (Time, type of incident, location, extent)?*
- *Who is affected? (How many people? And in what way?)*
- *What will happen now? (Impact?)*
- *Who provided the information?*
- *Who/what authorities have been informed?*
- *What additional information is needed?*
- *What immediate action needs to be taken?*

Assessment of the situation and status update:

Once it has been established what has happened, the severity of the situation is assessed. This section describes the direct or potential consequences of the incident. Describe the 'big picture' based on a timeline of the short, medium and long-term impact.

Assess the situation against the following backdrops:

- Best-case scenario
- Most likely scenario
- Worst-case scenario

	Short-term	Medium-term	Long-term
Best-case scenario			
Most likely scenario			
Worst-case scenario			

The assessment of the situation as a whole is influenced by four key factors:

- I. Consideration of the framework in which GIZ operates
 - a. Intention of the commissioning party/client, Management Board, regional division, country director, etc.
 - b. The project context and framework conditions
 - c. Other conditions such as international law, project commission etc.
Time limits, legal restrictions, other regulations
 - d. Issues to be appraised
What needs to be decided and when? What information is required?

- II. Appraisal of the external factors influencing the situation
 - a. Location
 - b. Time
 - c. Environmental factors
 - d. Other actors

- III. Appraisal of the crisis/incident
 - a. Possible impact and the scope
How can the extent of the crisis be determined? Could it escalate even further? How will this affect GIZ's ability to deliver?
 - b. Possible scenarios
What scenarios are likely to develop in the short, medium and long term? What impact could this have on us in the future?
 - c. Assumed intentions of others
Can we second-guess what others intend to do? (local security authorities, media, etc.)

- IV. Appraisal of GIZ's capacities to manage the crisis
 - a. Capacities
What staffing resources are available? When? And for how long? Mobility (vehicles, risks involved)? Who knows their way around? Who can be contacted and how? Who can provide support? What appropriate measures can be taken for staff?
 - b. Expertise and skills
Who has what expertise? How are the relevant skills used?
 - c. Need for support
Do other actors need to be involved (such as BMZ, the Federal Criminal Investigation Department (BKA), and the German Foreign Office (AA))?

Status update

The situation is assessed using the following rule of thumb:

- Identify
- Appraise
- Draw conclusions/draft recommendations/make decisions

- **Executive Summary**
What is the key message of the status update? (Everyone involved is doing well. Everything is under control. There are a number of challenges to be addressed. We are facing certain difficulties. Decisions need to be made at Management Board level. And so on...).
- **Backdrop for the incident/anticipated consequences**
What happened? What will happen now? Assessment of the situation at the GIZ location, situation of the commissioning party/client, the staff (e.g. seconded experts, CIM integrated experts, development workers etc.), the media (both inside and outside of the country/countries in question), and of the victims' family.
- **Appraisal of the situation ...**
What does the incident and any consequences it may have mean for GIZ in the country/countries in question and for the company as a whole? Are positive or negative developments expected? What weak points could pose a further risk for GIZ?

- **GIZ's situation and intentions/measures so far**
What resources are available? What is the objective? What measures have already been implemented?

Scope for action by GIZ:

Here, the aim is to outline the different options available (action items A, B, C ...) for managing the crisis. Describe the pros and cons for each option. You can also outline the likelihood of success and the time required, which will help in decision-making. The following information can be included too:

- *Personnel costs*
- *Resources/inputs required*
- *Potential risks*
- *Potential consequences/fallout*

The bottom line is usually the same: Act now or wait?

Remember that the more you discuss the different options available the less likely you are to make the wrong decision.

Decision-making and security briefing for decision-making purposes:

Once you have completed the first three steps in the crisis management process, you need to make a number of different decisions to deal with the incident or event. In this step, you weigh up the pros and cons of each option for action, the effort involved and the likelihood of success and make a decision on how to proceed.

Security briefing for decision-making

- **Brief description of the situation**
State the nature of the incident. Include the relevant facts and describe the CURRENT situation. What action has been taken so far to manage the crisis?
- **Assessment of the situation**
 - I. *Consideration of the framework in which GIZ operates*
 - II. *Appraisal of the external factors influencing the situation*
 - III. *Appraisal of the crisis/incident*
 - IV. *Appraisal of GIZ's capacities to manage the crisis*
- **Decisions made to date**
So far, what measures have been taken? How far has implementation progressed?
- **Further need for support**
Do other actors/divisions need to be involved?
- **Assessment of GIZ's scope for action**
Outline the different options available as well as their pros and cons. What is the timeframe? What is the likelihood of success?
- **Proposal for action**
What do you believe is the best course of action for GIZ? Why?

Planning:

Plans are drawn up to implement the action items decided in the previous step. They clarify what further steps will be taken and the resources to be used.

Time plays a key role in this context. The plans drawn up must differentiate between emergency measures and measures or actions that are required in the medium and long-term.

Ask yourself: How will the decision be implemented?

Order design:

Job orders are to be distributed to the relevant individuals and sections to implement plans for the action items decided in the previous step. To help you allocate the job orders appropriately, ask yourself the following question:

Who does what? When? (Define a time frame). Where? Why? And with whom?

The individuals and sections commissioned/the on-site CMT must notify the manager of the Head Office CMT on completion of the activities assigned in the job order.

Monitoring:

The final step in crisis management is monitoring. Here, a check is carried out to ensure that the job orders assigned by the Head Office CMT are being or have already been implemented. Was the job order implemented correctly? Did the individuals and sections commissioned/the on-site CMT notify the Head Office CMT when the job orders were completed? Is the Head Office CMT always aware of the latest status? It takes time for the CMT to proactively follow up on and keep up to date with crisis management activities.

Implementing measures will change the situation, so the process now starts again from the top.

Ask yourself: Was the job order implemented correctly?

Annex J – GENESYS conference call

The moderator (a staff member from the Corporate Security Unit), invites individuals to participate in the conference call and gives them the access code and the conference number (see example below). The moderator starts, moderates and end the call.

Access data:

Dial-in number **+ 49 69 710 445 638** (alternative **+ 49 211 540 739 05**)

Conference no. ***271945*** (include the asterisks)

Email template for conference call participants:

Dear colleagues,

We would like to invite you to participate in the Head Office CMT conference call on XX.XX.2016 at XX.XX German time.

Five minutes before the start of the call, please dial **+49 69 710 445 638** OR **+ 49 211 540 739 05** and enter the conference number ***271945*** (including asterisks) to confirm.

The following agenda has been set for the call:

- Brief description of the situation
- CMT situation on-site
- Corporate Security Unit
- COPE
- Regional division
- HR Services
- Media Department
- Measures taken/decisions made to date
- Miscellaneous

We look forward speaking to you soon.

Corporate Security Unit

Annex L – Crisis Management Information Board

Date: Crisis Management							
CMT	Information			Decisions		Communication	
Head of CMT	What	When	Where	reported by	When	What	HQ CMT
COPE							Staff on-site
DG/ HoD							Staff in GIZ
RegDep. Desk Offr							Security Forces
Press/Media							German Embassy/CID/GSS/GAF
HR							BMZ
Documentation							GFO
Current Situation							Press
							GP network
							UNDSS/ EISF
							Family

Annex M – After action review

AFTER ACTION REVIEW (AAR)

1. What should have happened? What was the planned procedure in terms of crisis management? What did actually happen? What are the reasons for the differences between plan and reality?
2. What did work out well? What did not work well? Why? What would be worth to be repeated in a future occasion?
3. What would you do differently in the future? Where do you identify needs for improvement? What was missing? Were there any disturbing factors as well?
4. How would you rate the crisis management overall? What would be required for scoring 10 out of 10?
5. Further remarks:

Annex N – Report on lessons learned

Report on lessons learned

Organisational unit:

Document owner:

Priority area:

Project or role within the organisation:

Product or process: Crisis management

Version	Date	Author(s)	Changes

Report on lessons learned – Purpose and objectives

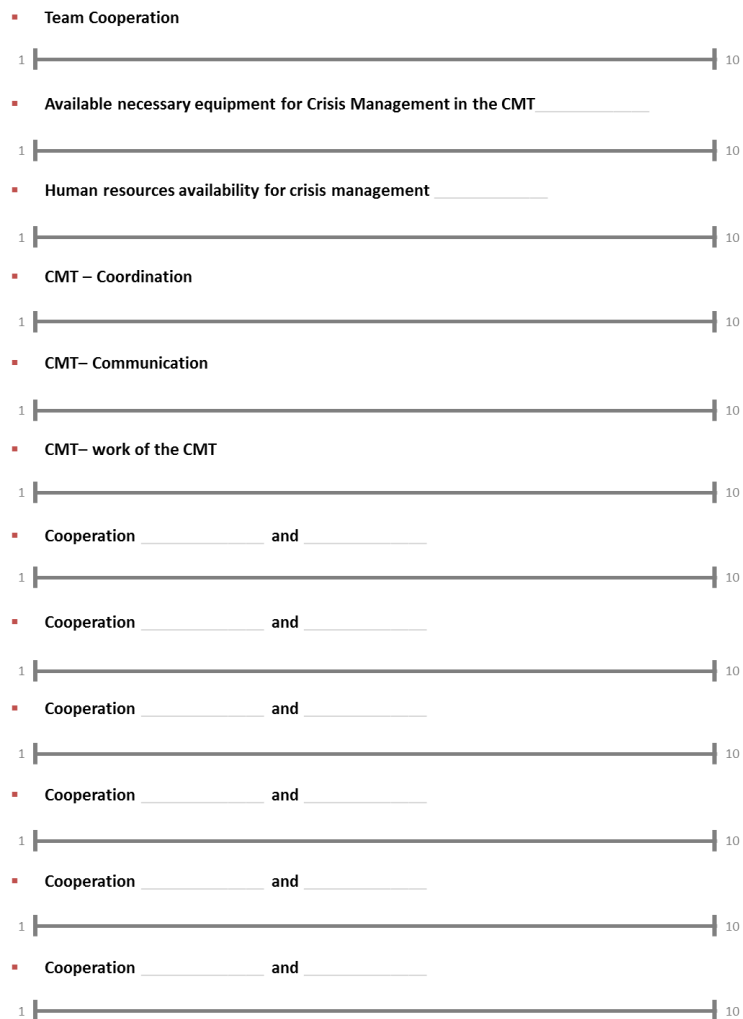
During each project life cycle, lessons are learned and potential improvements identified. As part of a process of continuous improvement, documenting these lessons learned helps promote institutional learning, as does identifying any gaps, shortfalls in resources and reasons why errors occurred. Pinpointing lessons learned can help avoid problems during subsequent project phases or in new projects or processes. The information in this report was gathered using after action review data collection sheets and in feedback meetings. A summary of the key items is provided in a table at the end.

This report aims to present all of the relevant information that will facilitate better planning and allow adjustments to be made in subsequent project phases and in new projects and processes. Improving processes and making sure that the required resources are available will prevent the same mistakes being made again, will help ensure that sufficient resources are in place and that any gaps are addressed. This in turn will help minimise potential risks.

Lessons learned – Questions

- What worked well during implementation and within the team? What needs to be improved?
- What should be modified, changed or done differently in the future?
Was the team faced with any unexpected difficulties or developments?
- Were there any aspects that took the team by surprise?
- Were all of the objectives achieved without any great difficulty? If not, what changes need to be made in order to meet future objectives or expectations?

Barometer



Sequence of events

Top three significant achievements

Success	Success factors

Other significant achievements

Success	Success factors

--	--

Scope for improvement; recommendations

Scope for improvement	Recommendations

Specific action required; options for action – after action review

Specific action required; options for action	<i>Comments from feedback received</i>	<i>Person responsible</i>