CBM International | Global Health, Safety & Security Unit

CBM Safety and Security Policy

and Guiding Framework Tools and Standards

Applicability:	CBM Federation
Author:	Philipp Burtzlaff, Global Safety and Security Advisor
ILT approved:	November 2018

Contents

Acknowledgements
The CBM Safety and Security Policy was developed by Philipp Burtzlaff.

The author would like to thank the following people who contributed their time and expertise to the development of this policy:

Chiara Anselmo, David Bainbridge, Benjamin Dard, Stefan Dofel, Mark Fonseca, Dietmar Haberzettl, Martin Hahn, Tom van Herwijnen, Dominique Schlupkothen, Martin Seiffert, Margarida Silva, Anita Smeets and Nadine Trudel.

Additional contributions to the development on this document was received from

- Josef Frei, Senior Advisor Safety and Security, Deutsche Welthungerhilfe
- Lisa Reilly, Executive Director, European Interagency Security Forum

For further reading:
Bickley, S. (2017) Security Risk Management: a basic guide for smaller NGOs. European Interagency Security Forum (EISF)

Appendices with Guiding Framework Tools and Standards

1 Introduction

1.1 Preamble

This document[1] seeks to lay down a foundation for CBM as it establishes and builds upon its existing approaches to health, safety and security[2].

The health, safety and security (HS&S) of staff are key responsibilities of CBM. CBM accepts a duty of care for all staff, whatever their personal profile.

CBM is committed to clear, applicable and proportionate security policy, protocols and plans[3]. The purpose of this policy is to increase the health, safety and security awareness of all staff, to ensure procedures are clear to staff, create a culture of well-being, safety, security, and ultimately, to enable project continuity.

1.2 Scope of this Document

The scope of this policy is all staff of CBM and all its related offices. It also governs the health, safety and security principles that apply to CBM visitors including CBM Board members and third parties (e.g. Member Association staff, personal assistants, donors, celebrities, free-lancers, volunteers, consultants and media teams) to CBM field offices or programme countries on CBM related business.

1.3 Compliance and Responsibilities

While CBM recognizes that no working environment can be made risk free, much can be done to mitigate risk when all parties recognize their roles and responsibilities within an organization's health, safety and security framework.

The International Leadership Team (ILT) is ultimately responsible for health, safety and security risk management for the CBM Federation. The ILT defines the level of the acceptable risk threshold and ensures resourcing of security risk management and advises the Supervisory Assembly on security matters.

The Regional Hub Director is accountable for security risk management within their respective regions.

The Country Director is responsible for security risk management at country level: e.g. monitoring country-level risks and establishing and maintaining appropriate security plans/arrangements for country-based staff and visitors.

---

[1] This policy replaces the December 2013 Security Policy which governed the implementation of a formal Security Management Framework across CBM International.

[2] **Health** can be defined as the condition of being sound in body, mind or spirit. **Safety** can be described as the freedom from risk or harm resulting from unintentional or accidental acts, events or hazards. **Security** can be described as freedom from risk or harm resulting from intentional acts of violence, aggression and /or criminal acts against staff, assets or property.

[3] The CBM Safety and Security Policy is in line with the guiding principles and standards of behaviour that are described in the Code of Conduct, CBM's Core Values and Mission Statement. Knowledge on all forms of unacceptable conduct, which includes sexual abuse, exploitation and sexual harassment are a critical element of CBM's HS&S risk management. The CBM Code of Conduct is available on the intranet of CBM International.

Non-compliance is a disciplinary issue and will be enforced for all staff, whatever their position in the organisation; it is compulsory and concurrent with the start of any kind of work with CBM.

The key to effective HS&S risk management is the creation of a culture of health, safety and security. CBM will work to create such an environment.

Each staff member bears a significant responsibility for their own health, safety and security and needs to be aware that their personal and professional conduct can have an impact on others health, safety and security as well.

In addition to adherence to organizational policies and procedures, individuals must be sensitive to their environments and willing to adapt to changing threats. For this reason, health, safety and security is necessarily a cooperative effort between the organization and all its employees.

2 Safety and Security Policy Principles

2.1 Primacy of Life

For CBM, life is of greater value than material and therefore no staff should endanger their own life, or the lives of others, whilst attempting to protect CBM property, equipment, financial resources, documents or infrastructure. This also means that CBM will consider primacy of life the priority when dealing with any crisis.

2.2 Right to withdraw

CBM upholds the right to withdraw an employee or a group of employees from an area or country at all times. Non-compliance is a disciplinary issue.

2.3 Principle of non-Partiality and Neutrality

CBM adopts the principles of non-partiality and neutrality. These principles are the foundation of a strategy based upon acceptance by the host community. This is the security strategy that CBM considers most appropriate.

2.4 Acceptance as the primary Security Strategy

The primary strategy to mitigate risk is acceptance. A security strategy based on acceptance means building a safe operating environment through consent, approval and cooperation from individuals, communities and local authorities. Acceptance cannot be assumed or taken for granted. It has to be pursued.

A secondary component of the security strategy is protection by reducing the vulnerability of CBM to a possible threat, for example, by building walls or hiring guards. Improving practice through standard operating procedures (SOPs) is also a protective measure.

Under certain circumstances, generally as a last resort, deterrence measures can further reduce the risk by containing the threat with a counter threat, for example: Armed protection, diplomatic/political leverage, temporary suspension.

The acceptance strategy will, dependent on the risk level in a country, be combined with protective measures. **CBM avoids deterrence measures as much as possible**. **The centre of gravity rests with an acceptance approach**[4].

CBM and its representing staff will avoid the use of armed protection. Exceptional situations, where recognized, armed protection may be non-negotiable for operational access, requires escalating to the Health, Safety and Security Manager for a decision[5].

[4] This approach rests on two elements: The organisational acceptance of CBM as an institution, and the individual acceptance, which is defined by staff behaviour.

[5] Examples: Armed guard in vehicles in Pakistan tribal areas or using vehicle convoys in DRC.

2.5 Do No Harm

One of the most influential factors for the success of CBM's acceptance approach is the 'Do No Harm Principle'[6]. **CBM will not undertake any missions, field visits or project activities that jeopardize the safety of staff, partner organisations, the beneficiaries or the local community**. In line with the "Do No Harm" principle, CBM aims to be inclusive, to respect and promote human rights within its organisational structure and to ensure that the programming is not doing any harm, be it directly or indirectly, intentionally or unintentionally. CBM has developed tools and standards to ensure that the "Do No Harm" approach is applied to integrate conflict-sensitivity wherever it is relevant[7]. From a health, safety and security standpoint, this means that CBM avoids putting people in a situation that increases their exposure.

2.6 Duty of Care

CBM has both a **legal and a moral obligation** to take all possible and reasonable measures to reduce the risk of harm to those working for CBM. In programme countries where the legal minimum standards of occupational health and safety regulations are lower than the standards upheld by CBM, the higher health and safety standards[8] should be applied to those working for, or on behalf of, CBM[9].

CBM's duty of care also encompasses **support mechanisms** following an incident or crisis, such as access to confidential care support services for psychosocial issues such as stress, anxiety and depression, and a crisis hotline for security related support as well as medical emergencies.[10]

2.7 Security Risk Threshold

The impact of CBM's activities that can be achieved should always outweigh the risks taken. In consequence, CBM will suspend its operations where the security risks are disproportionate to the potential program benefits. Therefore, CBM commits itself to continuously analyse and understand the context and the risks that result from working in that context.

CBM partners are encouraged and supported to develop their own security risk management plans, as well as to participate in the security trainings that are implemented through CBM. CBM staff who are travelling with or staying at partner organisations follow the security plan of the partner. In case the directives outlined in the security management system of CBM are more stringent, CBM staff must follow CBM's security plan. Whenever there is any doubt the line manager should be contacted for advice.

---

[6] For more detailed information on the „Do No Harm" Principle: http://cdacollaborative.org/what-we-do/conflict-sensitivity/

[7] Examples: CBM Partner Assessment Tool, Project Cycle Management Handbook, Risk Assessment Tool, Safeguarding Policy, Code of Conduct and the CBM International Safety and Security Management Plan.

[8] Example: Fire alarm or fire safety regulations; ensuring that evacuation routes are accessible also for staff with disability.

[9] Duty of Care must take into consideration the support of personal assistants, that may be required by persons with disability.

[10] More details how to access the services, and what they offer, can be found on the Intranet of CBM International. Alternatively, the information can be requested by sending an email to: hssunit@cbm.org

2.8 Security Risk Management

The Security Risk Assessment (SRA) is the primary mechanism for managing and mitigating security risks to CBM personnel, property and assets[11]. SRA's encompass a range of measures designed to reduce the level of risk to an acceptable level. The level of acceptable risk is identified in the SRA's of the country specific security plans.

CBM's security risk management has four important principles that relate to dealing with questions of acceptable risk:

1. Do not accept unnecessary risk.
2. Accept risk when benefits outweigh risks.
3. Make risk management decisions at the right level.
4. Everything reasonable should be done to reduce risk.

Acceptance by the local community and other stakeholders is one of the preconditions to operate.

When there are known and specific threats towards CBM staff in certain areas and this threat is considered as credible, CBM will not allow staff to work in or travel to this area. This also applies to circumstances where the level of generalised violence suggests a high probability of an incident harming CBM staff. CBM commits itself to minimising the risk to staff and therefore will always explore possible alternatives to attain the aims of the operations.

2.9 No Ransoms Principle

CBM will do everything ethically possible to secure the release of detained or kidnapped staff. However, CBM will not pay ransom for the release of staff.

2.10 Inclusion of Diverse Profiles

CBM strives for equality in its security approach. Individuals should not be subject to any discriminatory restrictions. However, CBM recognises that individuals may face different risks or be more vulnerable to certain threats because of their nationality, ethnicity, religion, gender identity, sexual orientation, or disability. Under certain circumstances, the prevailing security context or specific risks to an individual, because of their profile, may require CBM to take additional security measures. For this reason, individuals shall be informed of specific risks they may face and be advised how to minimise risks.

[11] At country level, the Country Director is responsible for the SRA.

Appendices with Guiding Framework Tools and Standards

Appendix 1

Health, Safety and Security Management Tools and Standards

A.1.1 Security Levels

Within CBM a system of security levels is used. This system indicates a certain level of threats towards staff in a country or area through indicators. It automatically connects this level to a set of measures, which is indicated in CBM's Global Security Management Plan, Annex R.

The system of security levels is generic by nature and the measures are merely a guidance to what needs to be put in place. The risk indicators describe what the situation is like and gives direction on actions to be taken. The CBM system of security levels is one that is defined by the Health, Safety and Security Unit and that the field offices develop and maintain.

For raising or lowering of country security levels, the principle of precaution comes into play. The Country Director has the authority to raise the security level for his or her country. Defining of security levels for countries with CBM involvement, but without an office, fall under the remit of the respective Regional Hub Director. Lowering of the security level is only possible when the Country Director as well the Director of the Regional Hub, agree in consultation with the Health, Safety and Security Unit. In case of disagreement, the matter is referred by the Regional Hub Director to the Director of Programmes.

Each CBM country (or security risk area) applies and utilizes the standard security risk level system (see Annex R of the Global Security Management Plan). The security risk levels should be contextualised and complemented with specific indicators, triggers and actions appropriate for the country (or security risk area). The Country Directors of countries with high or extreme risk classification, must ensure that their office staff and visitors are aware and adequately briefed, trained and prepared for the corresponding security context.

All CBM country offices require a staff member, who has the function of a dedicated country Security Focal Point (SFP) as a part-time duty. By default, the role of the SFP sits with the most senior person, i.e. the Country Director.

A.1.2 Incident Reporting & Analysis

Incident reporting & analysis is crucial for follow up as well as organisational learning when it comes to security management. **Every member of staff has the obligation to report any situation that jeopardized or almost**

jeopardized the safety and security of staff.[12] This includes near-misses or developments in the context that in the future might affect the security situation. Every situation that qualifies as above must be reported through the agreed incident reporting channels.

A.1.3 Health, Safety and Security Training

All CBM personnel, both national and international, who travel for CBM to programme countries, must complete a face-to-face Health, Safety and Security Course before their first business trip. In case the trip is due before the next training, an online Staff Safety and Security Training must be completed as an interim solution prior to the business trip. It is compulsory for adult dependants of expatriates to participate in a S&S training. The cost for the participation in a security training is carried by CBM.

Staff travelling to countries with a high or extreme risk rating, are required to complete a Hostile Environment Awareness Training (HEAT). This requirement also applies to staff who have a higher risk exposure due to the nature of their work such as auditors, investigators, compliance staff and members of the emergency response team. CBM will cover the cost of security trainings for accompanying personal assistants of travellers with disability[13].

A.1.4 Travel Security Clearance and Security Briefings

A.1.4.1 Travel clearance and approval

As part of CBM's travel security clearance procedures, travellers need written approval from their line manager prior to a trip. In addition, the **Country Director** or **Regional Hub Director** are to be informed about and give their **written approval for the planned trip** to their country or region[14].

A.1.4.2 Travel tracking

Prior to travelling, a travel tracking form needs to be filled in and sent to the dedicated travel tracking recipient[15]. A copy of the flight ticket, accommodation booking confirmation and the Terms of Reference (or detailed itinerary) for the

---

[12] An initial incident crisis notification report template, as well as an incident analysis and learning report format are available on the intranet of CBM International or as an annex of the CBM International Health, Safety and Security Management Plan. Alternatively, the reporting templates can be requested by sending an email to: hssunit@cbm.org
Other reporting channels, both for external stakeholders and CBM-affiliated persons to report on any breaches can be found in CBM's Code of Conduct (see also chapter 1.2 Code of Conduct).

[13] The Health, Safety and Security trainings must be refreshed every two years.

[14] If the Country Director is unavailable to respond to the travel clearance request, the Regional Hub Director will act in response. In case of travel in a country without a Country Director, obtain written approval from the individual with responsibility for the country (often a Regional hub Director or Country Director in a neighbouring country).

[15] The use of the Travel Tracking Form is mandatory for all CBM International staff for international trips to programme countries. It is highly recommended for all international trips, including those to non-programme countries. The form must be sent by email or MS Outlook via invite to: traveltracking@cbm.org two weeks in advance to the planned trip.

trip should be attached to the travel tracking form. Alternatively, the relevant information should be mentioned on the form. For local travel within the programme country, a contextualised travel tracking system must be put in place by the country office[16].

A.1.4.3 Security briefing

As part of the travel preparation, travellers must request a pre-departure safety and security briefing from their respective security unit or security focal person. Upon arriving in the destined programme country, the Country Director will ensure that visitors receive a local security briefing, which includes cultural sensitivities and local customs. This briefing should take place immediately upon arrival, before programme activities or in-country travel are initiated. In countries with a high or extreme risk level classification, additional equipment will be provided to the traveller[17].

A.1.4.4 Informed consent

Following the pre-departure health, safety and security briefing[18], travellers are asked to sign an informed consent paragraph before travel to CBM programme countries.

A.1.5 Mid- and Long-term Deployments

New CBM staff with expatriate contracts, including recognized dependents as well as new staff with travel duties, are to be briefed on and/or provided with an induction briefing on CBM's global security risk management, standard operating procedures (SOP's) and contingency plans. This will include information on possible heightened risks for individual profiles. The induction briefing includes a country specific security orientation (for mid- and long-term deployments), as well as a briefing on medical arrangements available in the country of deployment, and how to access these or call for emergency assistance.

A.1.6 Health

A.1.6.1 Medical examination and advice on prophylaxis measures

CBM requires employees to undertake a standardised medical examination and receive advice on prophylaxis prior to any work-related stay or travel abroad. This examination must be done by a specially accredited doctor. It focusses on climate-related and health related strains on the body, as well as information on

[16] Example for travel tracking from a "high risk" setting: A vehicle passenger (not the driver) sends a text message every hour to a colleague in the country office with the distance from the place of departure (in kilometres). The colleague confirms receiving the message with "OK". In case an expected message is pending for over 15 minutes, the colleague in the country office calls the vehicle passenger to inquire about the cause for the delay. The frequency of messages will depend on the security context.

[17] Travel equipment will include a charged mobile phone & SIM card, personal first aid kit, and further items, depending on the security context.

[18] The pre-departure safety and security briefing includes details of the threats and risks in the areas the staff will be travelling to, including residual risk, the mitigation measures that are in place and the responsibilities of the individual as well as the organisation for effective security risk management.

medical support at the place of work, specific information on malaria prophylaxis and on vaccinations.

A.1.6.2 Psychological Support

Staff health, safety and security includes protecting mental health. Stress has a direct impact on the ability to make effective and appropriate decisions and thus a direct impact on security for all. CBM offers access to an employee assistance programme service (EAP). The EAP consists of a confidential care support service which is available to all staff. The service is also available for family members of staff. The programme is designed to alleviate work-related issues, for example due to mental health, substance abuse, personal & workplace problems. The objective is to have a positive effect on employees' health.

Appendix 2 Communications

CBM will ensure that staff travelling for CBM have access to adequate communication means during their travel. This is to safeguard that they can be contacted in case of a security incident or a crisis.

In addition, it allows the traveller to request assistance or report an emergency and other unexpected changes or situations that require to be communicated. CBM provides communication means to travellers either before departure, or upon arrival at their country of destination.

Country Offices in countries classified as high or extreme risk must have at least one alternative communication system in place, e.g. a satellite phone. Staff based in these locations must know how to operate such systems and the Country Director must ensure the system is regularly tested and maintained.

CBM staff must be aware of the **Social Media Regulations** put in place by CBM International.

Appendix 3 Vehicles

A.3.1 CBM and CBM partner owned vehicles

All vehicles must be appropriately registered, insured, well maintained and suitable for the country, trip specific and seasonal road conditions. The vehicles can only be operated by persons with a valid driver's licence, and under conditions that comply with the local legislation and CBM's code of conduct[19].

A.3.2 Rental vehicles

Rental vehicles are to correspond to the same legal, safety and security standards that apply to CBM owned vehicles. The country and/or regional hub office are responsible to ensure that the rental vehicles and operator have adequate insurance coverage.

A.3.3 Safe driving

Vehicles must be driven safely. The person operating a vehicle for CBM must recognise the limits of the vehicle, the risks the environment poses, and adjust the driving accordingly. Vehicles must be able to stop quickly and safely in an emergency, and therefore must be driven at a speed at which the vehicle is stable, which may be lower than the allowed speeding limit. Passengers in the vehicle are also responsible for their own safety and **must** express and highlight their concern, when the vehicle operator is not driving safely. The wearing of seatbelts is compulsory.

[19] The minimum standards for vehicles and their operation are stated in the Minimum Operating Security Standards (MOSS) and the Global Safety and Security Management Plan.

Appendix 4 Offices, Premises and Facilities Protection

CBM facilities should be selected and managed to reduce the risk of injury to personnel and/or loss or damage of material.

Site security is maintained through a series of physical and procedural boundaries. Site safety is maintained through reducing vulnerability to fire, accidents and natural hazards (e.g. earthquakes or cyclones).

All buildings occupied by CBM are required to be compliant, where feasible, with international building, safety and fire regulations or the applicable laws of the host country, as appropriate.

This includes construction for resistance to earthquakes, such as choosing low-rise buildings that have earthquake resistant structures, or other natural hazards, according to local conditions[20].

The installed emergency alarm systems in CBM premises which employ staff with disabilities, must be designed and adapted, when required, to allow an emergency to be recognized as such[21].

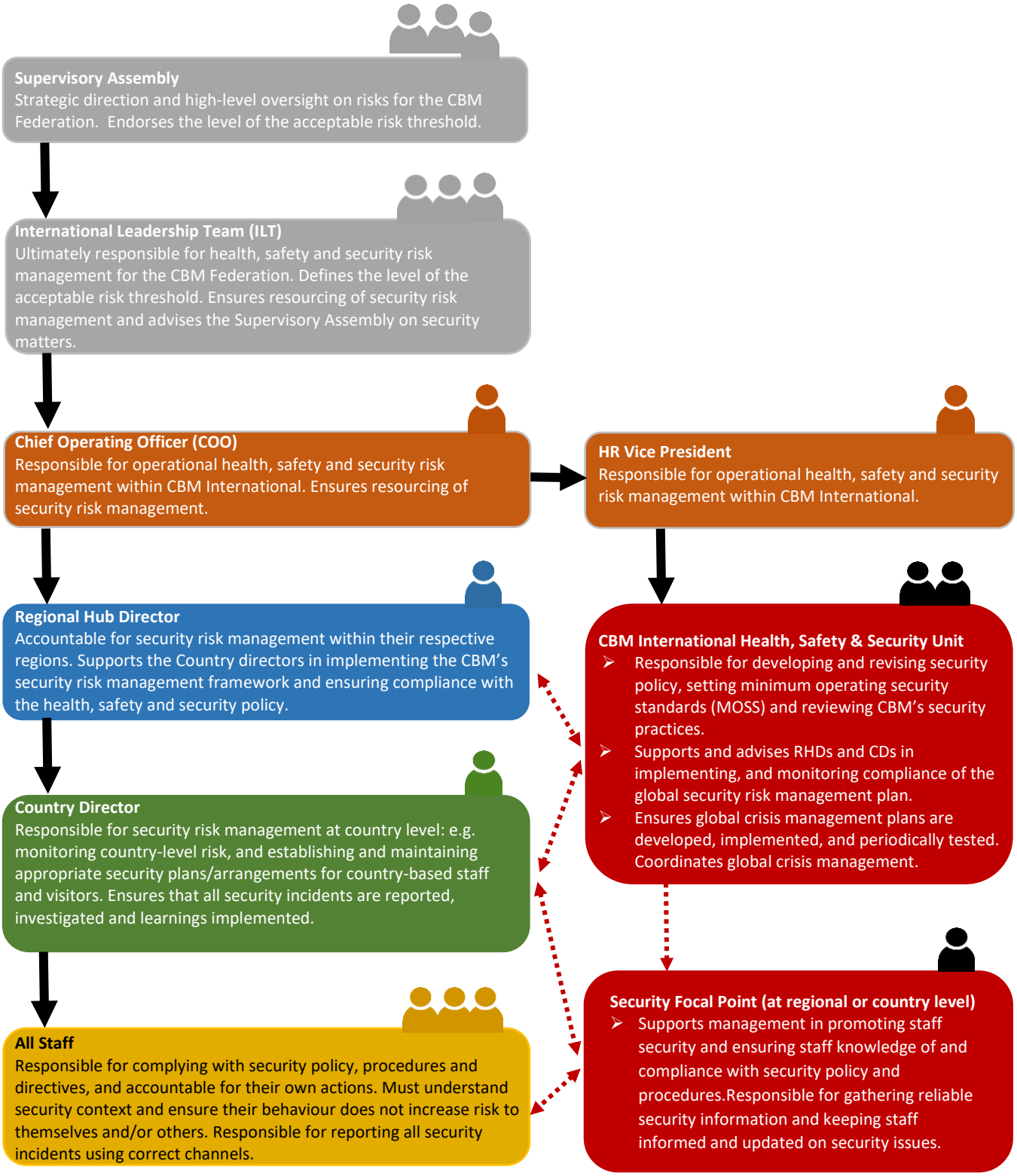
Likewise, evacuation and emergency plans should allow for barrier-free emergency exit routes and saferooms. All CBM buildings must have smoke detectors installed.

In buildings that have fossil fuel burning heaters or appliances, a fireplace, and attached garage, or other feature, fixture or element that emits carbon monoxide as a by-product of combustion, carbon monoxide detectors must be installed within three meters of each sleeping room.

[20] The detailed standard operating procedures for building and site management can be found in the Global Security Management Plan, Annex C.

[21] Examples: Installing visual and audio emergency alarm signals and regular emergency drills that include the use of an evacuation chair.

Appendix 5 Health, Safety and Security Management Roles, Structure and Responsibilities



A.5.1 Regional and Country Level

The regional hub director (RHD) is accountable for health, safety and security (HS&S) risk management within his/her respective programmes/regions. The RHD reports to the Director of Programms.

The Country Director (CD) is accountable for HS&S risk management within his/her respective programmes/country.

The responsibility for implementing contextualised minimum operating security standards (MOSS) rests with the RHD and the CD respectively.

Where CBM does not have a permanent presence in the country, the RHD must take measures to ensure that staff visiting the country are briefed in advance and safeguarded throughout their journey.

Each regional hub must appoint a (regional) security focal point (SFP). The SFP and the RHD/CD provide assistance to enable staff to comply with HS&S regulations, including the loan of equipment from a pool maintained for visits, where appropriate (communications equipment, grab bags, personal first aid kits etc).

The advice of the HS&S Unit should be sought, if necessary where the security risk assessment indicates a need for mitigation measures outside the normal competency of the CBM Security Focal Points.

Any visitor to a CBM country office is required to understand, accept and adhere to the country security plan, rules and regulations.

A.5.2 Security Focal Point (or Security Management Team)

The Security Focal Point (SFP) or the Security Management Team (SMT) is tasked to make recommendations and (delegated) decisions on the prevention of incidents during normal operations.

Where feasible, a SMT is always preferable to a SFP, particularly in countries with high or extreme risk classification. A SMT can share responsibilities and tasks, that otherwise rest on the shoulders of one person. A recommended size for a SMT is a group of four persons.

The SFP or the SMT is located in the regional hub or country office and supports management in promoting staff security. Furthermore, roles and responsibilities include ensuring that staff are aware of and comply with HS&S policies and procedures.

The SMT will meet on a regular recurring basis. The frequency of meetings depends on the identified security risk level of the country or security risk area

(to be defined by the MOSS, according to country risk level). In addition, meetings should take place whenever changes in the security risk assessment or level of escalation potential occur. The SFP (SMT) is an **advisory function** only and risk ownership remains in the management line.

A.5.3 Health, Safety and Security Unit

The CBM Health, Safety and Security Unit (HS&S Unit) is dedicated to keep operational risks at a minimum, ensuring project continuity and keeping staff safe. The Unit reports to the HR Vice President. The HS&S Unit has no direct line responsibilities for regional or country specific security matters but is tasked to uphold CBM's global MOSS. The HS&S Unit plays an important role in embedding the Health, Safety and Security Policy, the Global Security Management Plan and related documents as broadly as possible throughout the CBM federation.

The HS&S Unit also keeps track of global HS&S incidents and analyses these on a continuous basis to seek further improvement of CBM's security management systems. The HS&S Unit sets and upholds standards for global staff training in the field of health, safety and security.

Appendix 6 Crisis Management Team

The Crisis Management Team (CMT) manages a crisis at headquarter, regional hub and country level and provides a central crisis coordination platform for the CBM Federation. The CMT is activated when a critical incident or any other situation is determined to be a crisis by senior management[22]. The composition and role of the CMT differs according to the type of crisis.

The role of the CMT is to mitigate the impact of an incident. The quality of crisis response has potentially significant influence over an incident's outcome, and therefor CBM regards this role as fundamental to the organisational risk management system. The **primary objective** of the CMT is to:

- Prevent (further) harm to affected persons and ensure the health and/or safety of victim(s) and other staff affected by the crisis.

Other objectives include:

- Assure families of victims and CBM staff of a responsible and effective response.
- Ensure continued organisational management and output during the crisis.
- Ensure programme continuity.
- Fulfil organisational duty of care[23] responsibilities and reduce the risk of litigation/liability claims.
- Provide support to and advise for managers of other CBM units (Safeguarding, Internal Audit).
- Facilitates relevant interventions with global insurances and international medical evacuation procedures.
- Mitigate possible reputational damage.

The HS&S Unit provides support to RHDs and CDs to set up and train local CMTs, who take on the regional or local aspects of crisis coordination.

[22] A critical situation, or critical incident, is an event or series of events that seriously threatens the welfare of staff, potentially resulting in death, life-threatening or life-changing injury or illness and triggers CBM's crisis management response. A critical incident may also be an event that has a serious impact on programmes, organisational assets or reputation.

[23] CBM's duty of care covers the legal and moral obligation to take all possible and reasonable measures to reduce the risk of harm to those working for, or on behalf of CBM.