Leading in disability inclusive development

cbm christian blind mission

Guidance sheet: key security considerations when designing projects in crisis-prone settings.

Introduction

Incrementally, CBM is implementing projects in high and extreme risk countries or areas. These indeed are the locations where our clients are most in need of urgent CBM support. Such locations are often also the areas where donors are keen to invest funding. What is vital to acknowledge is that NGO and partner's work in such areas is prone to substantial security risks.

To be able to work effectively in risk and crisis-prone areas, these risks must be studied and appropriate mitigation measures developed. It needs to be assessed openly – and early – whether CBM and/or its partner organisations have the right means to mitigate present risks or whether, from a risk management point of view, it should be deemed wiser for CBM not to get engaged at all.

Crisis-prone areas are volatile and insecurity is constantly shifting. Therefore, projects must remain flexible and be designed in such a way that CBM and its partner staff can work in certain areas without being exposed to unacceptable levels of risk. This is an intrinsic part of our Duty of Care where the respective CBM CO and/or partner organisations constantly study the applicable risks in an area and decide whether access at a certain point in time is safe or not. To accomplish this, solid security management and mitigation measures must be embedded within project proposals from the onset. This requires that the project budget includes ample funding to implement the developed mitigation measures. This in turn will ensure that there is a greater likelihood that project objectives can ultimately be achieved and risks for CBM and partner staff is reduced.

Turning this around, it is also likely that, when risks in a target area are not appropriately identified, studied and managed, the probability of a security incident increases. This not only directly endangers CBM and our partner staff but it jeopardises the planned outcome of a project. Taking time to study risks and including security measures in a proposal should not be seen as a mere burden or a cost factor.

Taking security management seriously, actually determines greatly whether access to a target community remains possible in risk-prone areas and thus whether the project can deliver its objectives on time and without (serious) incidents. Our choice of implementing partner, and our ability and willingness to share (managed) risks with them, can help determine whether access to a difficult area remains possible for CBM, even if an area is classified as high-risk.

In our choice of projects that we get involved with, we must realize that CBM itself is not set up as a frontline agency and certain project activities will be beyond our own capabilities. Even if a partner organisation might still be capable (or willing to) implement activities in very risky areas, CBM should still carefully consider whether it is transferring risks at an acceptable level. This is the delicate and constant choice of sharing or transferring risks.

Even if CBM is profoundly implementing a project through a partner organisation (willing to take certain risks), it still remains a duty of care for CBM to ensure that risks have been studied and mitigated. Project proposals should strive for solid management of risks and thus avoid undue risks to CBM and implementing partner staff.

Process for risk mitigation during project development

Make use of the available resources and advisory support available. As part of CBM's three-way-collaboration:

1. As a 1st step, CBM's Global Security & Safeguarding (S&SG) Unit must be contacted when CBM considers responding to a call for proposals in a high or extreme risk area[1]. This first contact should be established by the CO and the Fundraising Team that seeks to develop a new programmatic proposal. Key consideration here is a principle 'go/no-go' decision (before any commitment is made) on whether the project is feasible under the current security challenges.
2. Where the Global S&SG Unit has serious doubts about the feasibility of staff security and project implementation in a high or extreme risk area (even with mitigation measures implemented), it will state so.
3. Share the basic concept of the planned intervention with the Global S&SG Unit. State the exact location, planned intervention, project duration, partner structure, CO and Fundraising Team contact person as well as the deadline.
4. As a 2nd step, if a principle 'go' decision is made, the Global S&SG Unit will liaise with the respective CO, Regional Security Staff and other involved entities to provide a first security risk assessment with suggested mitigation measures.
5. Embed the risk assessment and mitigation measures in the concept note showing clearly that active management of these risks will contribute to securing staff and delivering project results.
6. When full proposals are being developed, share the relevant yellow marked sections of proposal documents with the Global S&SG Unit in a timely manner while stating the deadline.
7. The Global S&SG Unit will comment on security risks, recommend activities / investments and will provide an estimate of what these investments could cost.
8. As a 3rd step, where required, the Global S&SG Unit will provide support to the CO in implementing approved and funded security interventions (e.g. security training, consultancy, acceptance enhancing activities).
9. In case the security situation in a project area significantly changes during the project implementation phase, the Global S&SG Unit should be contacted directly. The situation will be studied, new risks analysed, and advice will be given accordingly to seek to manage the new challenges within the scope and limitations of the project.

Budgeting

It is imperative to ensure that investments in security management are projected into the costs of a project early and for the duration of a project. When planning, it should be considered which structural security measures have already been implemented and which security resources and management capabilities are available at either CO, RHO or Global level. Or where our implementing partners already have strong systems and long years of experience to mitigate risks.

Some project proposal concepts simply do not allow for structural investments in security management capacity. It is expected by the donor that overarching security management systems and capabilities are already in place in CBM or the partner organisation. If this is the case, CBM must

[1] Which areas are considered high or extreme risk, can be found on: https://www.travelsecurity.com/Alerts.aspx?MembershipNo=31ACAM672277 and click on 'risk ratings and 'location ratings'

not assume but carefully scrutinize applicable systems and infrastructure before it submits a proposal.

To win such proposals, CBM might have to be willing to structurally invest (with its own funding) in these missing, overarching CBM or partner security management capabilities. This to tackle the identified deficiencies in a high/extreme risk CBM program field and in view of the complexity and work load of large, upcoming proposals.

It is worthwhile to take into account, for CBM and partner staff, to have possibilities to invest in community acceptance that enables access to (fragile) communities and help avoid security incidents. It is common knowledge in the NGO security sector that preventative investments in security measures are far more effective than having to respond with costly interventions when incidents occur.

Apart from the loss of staff's life and wellbeing, incidents are immensely costly and time-consuming, can ruin NGO's reputations and delay or terminate project activities. Cutting or omitting security management budgets to win a proposal is risky and a possible breach of our duty of care or risk sharing philosophy.

It is therefore recommended to invest adequate resources in preventative and preparatory security management at CBM and partner level. As a rule of thumb, we recommend:

- 2.5% of total project budget in **medium** risk countries
- 3.5% of total project budget in **high** risk countries
- 5% of total project budget in **extreme** risk countries

Actual amounts included in project budgets always require a contextualised discussion to ensure the investment is realistic – in view of what already exists – and helps mitigating the security risks identified.

Where (on site) security risk assessment or staff / partner trainings are planned, it is important to plan these early in the project cycle so that benefits can be achieved in a timely fashion.

Potential items and activities to be picked from when considering and developing proposals in risk prone environments[2]

Investment item[3]	Remark	Consider
Grab bags	Standard CBM recommended kit for travellers in high risk areas. Consider also that staff may suddenly be deployed in Humanitarian Aid work.	
Firefighting equipment	On each floor	
Smoke / carbon monoxide detectors	In each room/hallway/floor	
First aid kit for buildings	On each floor	

[2] These items or activities could be needed at CBM level or at partner level.

[3] If a country already has a well-equipped CO or sub-office in the field, very few infrastructural investment items will be needed. However, when a field or programme sub-office is set up specifically for a project, minimum operational security standards apply. The same applies where a (new) partner is selected who does not yet fulfil minimum operational security standards to keep its staff safe.

First aid kit for vehicles	In each CBM and project partner vehicle	
First aid training	First aid can be a life-saving skill for CBM staff and partners, especially for those traveling or based in a remote location.	
Communication equipment	Ensure traveling or remote deployed staff can always call for support, report an incident etc. In some areas, a satellite telephone or remote internet access may be needed.	
Safe vehicles	Ensure vehicles / motorcycles are in an excellent condition and are suitable for the areas.	
Emergency vehicle tool kits	When stuck in a remote area, can a vehicle be towed, repaired?	
Emergency energy supply	To power, computers and emergency communication equipment, a (small) generator may be vital.	
Improve security at fuel storage	Consider generator fuel as well as gas bottles (always outside).	
Strengthen wall/fence security	Contextualize; safe and strong, not easy to scale. Not standing out among other buildings.	
Lighting	Enhance (movement detecting) lighting in dark areas so staff can safely move around and burglars are deterred	
Outside/inside perimeter	Are there easy places to hide that should be cleaned, bushes/trees/branches cut?	
Strengthen gate security and entry points	Can guards safely determine and screen (also at night) who is at the gate. Consider first and secondary barriers in between where guests are screened.	
Guards equipment	Torches, rechargeable batteries, whistle/panic button, communication equipment, rain clothing.	
Guard dog	A dog is an always awake, alarm system; enhancing guards' effectiveness! A good deterrent.	
Guards wellbeing	Guards that feels cared for will watch out for you. Consider good (rain) clothing, boots, a proper guard house, etc	
Guards training	A well-trained guard knows what is expected of him/her as a routine and in an emergency.	
Drivers training	Defensive driving skills can prevent many serious incidents	
Staff training	A two-day staff training is a minimum requirement for staff deployed to high risk areas.	
HEAT training	Hostile Environment Awareness Training for staff (CBM or partner) working and traveling in a high / extreme risk area	
Security management training	A one-day security management training is a minimum requirement for managers in charge of projects in high risk areas.	
Crisis management training	A one-day crisis management training is a minimum requirement for managers in charge of projects in high risk areas.	
(On site) security consultancy	In complex areas it is a worthwhile investment to implement a security visit to the location where the	

	project will be implemented incl a participatory Security Risk Assessment.	
Strengthen locks and entry points	Good bolt or pad locks, window & door grills massively enhance building security and can build a second layer of safety once an (armed) burglar is in your compound.	
Lighting	Movement detecting lighting with battery back up in dark areas strongly enhance S&S.	
CCTV	In some locations CCTV cameras can be a deterrent.	
Safe exit points / emergency evacuation chairs	Can staff (with a disability) swiftly leave a building when an emergency (e.g. fire occurs).	
Alarm system (sound/light)	In case of fire or an incident, can your guards swiftly alert all staff?	
Sub-office	In some (remote) field locations a CBM sub-office may need to be established and made safe.	
Safe	Can you store valuable items in a fireproof safe bolted to floor/wall?	
Safe room / hibernation supplies	In higher risk areas an office / project building may need a safe room	
Blast film	In areas at risk of explosions, glass windows may require blast film to protect staff from flying glass.	
Community acceptance workshops	Enhance (partner) organization's acceptance by explaining to community stakeholders what the project entails and seeks to deliver. Vital in areas with armed groups and (irregular) checkpoints.	
Project security officer	In high risk areas with complex project activities and lots of staff movements, it can be recommendable to appoint a dedicated security officer for the duration of the project.	
Security Focal Person	Select, train and empower a Security Focal Person at (lead) partner level to coordinate local/project level security management.	
Local priorities	…….	

For more information, please contact CBM's Senior Global Security & Safeguarding Manager – Tom van Herwijnen at tom.vanherwijnen@cbm.org