Tool 5: Practical tips for including programme security in Global Fund grants

Basic security measures

Although the security challenges faced by every organisation and programme are different, and these challenges change over time, experience shows that there are some basic activities and practices that are relevant for most programmes. Considering the relevance of these to your programme can be a good way to think about how to improve your security.

1. Make programme security a routine part of your programme – review all planned activities for potential security challenges, putting mitigating and response measures in place as needed. Ideas to mitigate or respond could include:
    - Provide all staff and volunteers with ID cards indicating their name, organisation, title and contact details for their organisation or supervisor
    - Develop an agreement with a lawyer (e.g., keep a lawyer on retainer) who can provide support when incidents occur.
    - Identify, on a properly stored map (that does not include information that could be identified by others), the locations covered by the programme, including those that are safer/riskier, and information on how to access them. Also note for each location the availability of allies/colleagues (e.g. police, health workers, community leaders) who can help in case of emergency.
    - Invest in security infrastructure, such as locks and bars on windows, in offices and at drop-in-centers
    - Have outreach teams work in pairs at least. Have check-out/check-in procedures for outreach workers and other field teams, as well as providing for safe transport to and from outreach sites.
    - Use visitor logs to record who exits and enters a facility or drop-in-centre.

2. Discuss security incidents and concerns at regular team meetings (at least once per month) and encourage all staff and volunteers to share concerns and fears related to security. Record all incidents and threats and actions taken in a log, and examine these periodically to identify trends and make changes to activity plans (e.g., if you identify specific hotspots that are increasingly dangerous, shift staffing patterns or increase security measures at the hotspots).
3. Provide training for all workers (including staff and volunteers) on how to approach security when implementing the program. This should include identifying and assessing threats and then the expectations of each worker if a threat occurs (e.g., What should they do to avoid harm? To whom should they reach out for help if harm occurs? What actions, such as immediately ceasing outreach, are they empowered to take on their own? What protections are in place for them if they are injured on the job or are victims of theft or other crimes?). You do not need to do a special security training – you can do this by integrating security into all trainings related to the programme including for peers and for health care providers.
4. Have a rapid response plan for dealing with emergencies and crises, including clear communications channels, clear decision-making processes, and flexible funding that can be easily accessed.
5. Designate a focal person for security in the organisation – this can be someone with existing management or coordination responsibilities. Their role is to explain to and remind colleagues on policies and procedures. This person should be trained and supervised.

6. Identify allies for support in case of incidents and keep them briefed on any changes in the security situation (with clear lines of communication established before incidents occur).
7. Develop a phone tree / emergency communication group for all staff and volunteers so that everyone knows who to contact in a given situation and how to share urgent updates if an emergency occurs.
8. Staff and volunteers should thoughtfully decide what information to make public (e.g., location of a facility or their own personal information in the case of online peer educators) by weighing the pros and cons of such sharing

Including security in Global Fund Funding Requests

Deciding how to integrate security activities

Not all security activities require funding or a specific budget line. For instance, ensuring security is on the agenda at all team or planning meetings, is not likely to incur any costs since these meetings already take place. Other activities such as including security procedures in team trainings, and implementing a visitor log and security incident log, may require some increases in existing budgets (for instance, the cost of extending a training by half a day). In these cases the approach should be to ensure that budgets for those existing activities are sufficient to cover any additional processes related to security.

In some cases, improved security will require specific investments for additional activities or equipment. Examples include advice and equipment for better storage of digital information, physical security measures (e.g. locks, alarms, cameras), or new staffing (security guards). Costs may also be associated with additional meetings with stakeholders aimed at improving security. Another example is emergency or rapid response funds which can be used to support staff or volunteers affected by a security incident.

Eligibility of costs related to security

All of these costs are eligible for funding in Global Fund grants, as outlined in the relevant application materials (e.g. Information Notes, Technical Briefs and the Modular Framework). As is the case with any funding requested from the Global Fund, it is important that they be well justified and based on well-evidenced needs. (This is where using the self-assessment of security strategies, incident log and planning tools will be very helpful). The Funding Request form should be used to explain the security issues the project is facing or is likely to face and how these issues are addressed by the requested item/activity and line item in the budget.

Where the costs of security can be included in a Global Fund budget

In terms of where to include security costs in a Global Fund budget, the optimal approach is to integrate them within the programme module that they are directly related to rather than approaching security as a separate programme or area of work. For instance, if they are related to MSM programme implementation they should be included as interventions under the HIV/MSM module. If they are related to protections for people involved in Human Rights programmes, they should appear in the Human Rights module. Many implementing organisations work with different key populations and conduct human rights activities simultaneously. In these cases, rather than splitting up the costs of security interventions that are relevant for all of these programme areas, it makes more sense to include them in one place, for instance under Community Systems Strengthening – Institutional Capacity Building.

Ensuring funding for costs related to security is provided to front line implementers

Many HIV key population programmes receive funding from the Global Fund to fight AIDS, Tuberculosis and Malaria. For the most part this funding is not received directly, but comes through the Principal Recipient (PR) that has a grant agreement with the Global Fund, and sometimes via Sub-recipients (SR) which are contracted by the PR.

In each country the Country Coordination Mechanism (CCM) has lead responsibility for developing funding requests, with the PRs playing the lead role in developing detailed workplans and budgets and implementing grants. It is therefore important that the CCM and implementers understand the security challenges that key population programmes are facing and that they make provision for any costs associated with improving programme security when they develop Funding Requests and detailed budgets. Once they are included, it is also vital that these items be included in sub-grants or sub-contracts from PRs and SRs to key population programmes.

CCMs should ensure that security needs of HIV key population programmes are properly understood at the time of Funding Request development – for instance by ensuring that current implementers use the tools in this package to log incidents, assess capacities, identify risks and make security plans. This information should inform programme design and ensure that programme costings reflect any costs associated with security.