CIVIL SOCIETY INSTITUTE FOR HIV AND HEALTH
CSO WCA

fhi360
THE SCIENCE OF IMPROVING LIVES

THE GLOBAL FUND

SECURITY TOOLKIT: Protecting implementers and improving programme outcomes

Guidance and tools to strengthen security in Global Fund supported key population programmes

ACKNOWLEDGEMENTS

This package was developed by the CSIH-WCA and FHI 360. It builds on and adapts security tools and guidance developed by FHI 360 and collaborators under the USAID- and PEPFAR-funded LINKAGES and EpiC projects, revising them to respond specifically to the needs and realities of Global Fund-supported programming in West and Central Africa. Adaptation took place in 2022 with input from key population programmes and organisations in the West and Central Africa region. Support for this adaptation was provided by the Community, Rights and Gender department of the Global Fund to fight AIDS, tuberculosis and malaria. We thank and acknowledge the following organisations for their contribution to the process:

Burkina Faso

AIDSETI

AVP

AWEYA

SPCNLS

Cameroon

Affirmative Action

CHP

Empower-Cameroun

ESPOIR+

Ndop

Reach Out

Senegal

AJDPASTEEF

ANCS

APCSID

ENDA Santé

ONG AWA

ONG 3D

RENAPOC

RNP+

Sierra Leone

Dignity

IHPAU

RODA

SLYDCL

SWAASL

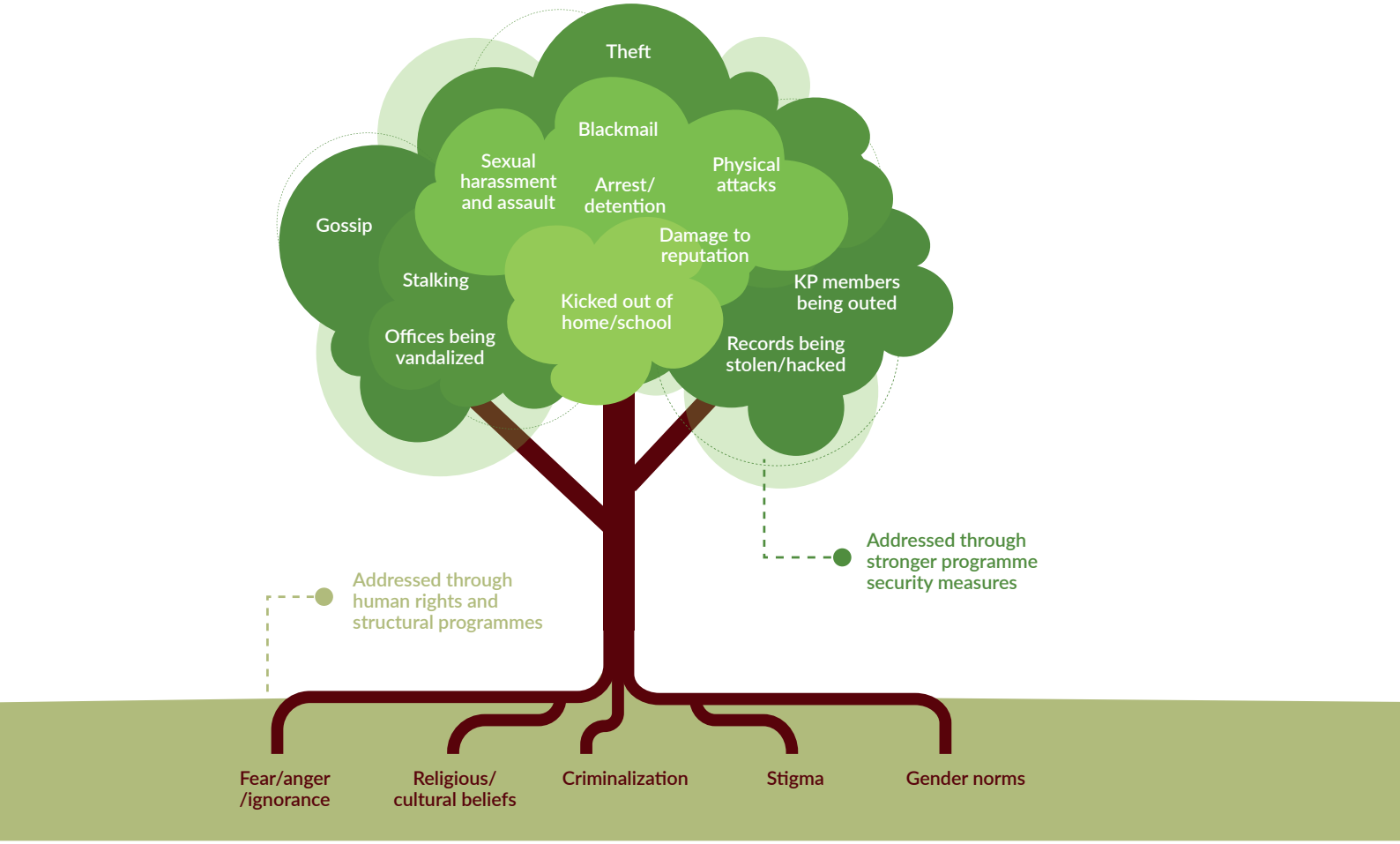
Women in crisis

TABLE OF CONTENTS

PART 1: TOOL GUIDANCE

Background

The human rights related risks and barriers faced by key populations are well-recognised, and addressing these is understood to be an essential component of a comprehensive HIV key population programme. A related, but less well understood challenge is the security of those involved in implementing HIV key population programmes and delivering services to these groups. Implementing organisations – which are often themselves key population-led – are often on the receiving end of threats and violent attacks which are directly related to their work. This insecurity has a heavy toll on the physical and mental health of those working in programmes. It reduces the effectiveness of those programmes as they deal with staff arrests, damage to organisational reputation, limited mobility, and hacked data, along with other issues that direct attention away from programming, that limit programme reach, and that can cause programme beneficiaries to decide to avoid these services.



While human rights programmes take a long-term approach to address the root causes of violence, stigma, discrimination and human rights abuses, including working at a policy and legislative level, it is also vital to implement day-to-day actions to reduce the risk of security threats and incidents faced by programmes, and to respond to those when they occur. Systematically tracking and assessing risks and putting in place resources and measures to reduce those risks and to respond to incidents is integral to any HIV key population programme, is essential to achieving and sustaining results in HIV and human rights programming. It is also part of the duty of care towards front line organisations, workers, and volunteers, and is essential to make community-led programming a safe and sustainable option.

The Global Fund to fight AIDS, Tuberculosis and Malaria is collaborating with FHI 360, and with the Civil Society Institute for Health in West and Central Africa (CSIH-WCA), to adapt tools that programmes can use to anticipate security risks, to plan ahead to reduce these risks, and to respond to incidents and threats. This document introduces the tools available to Global Fund programme implementers. They can be used to systematically build security measures into existing programmes, and as a basis for allocating resources to security as part of reprogramming or country dialogue processes.

Examples of programme security challenges

Key population organisations involved in the development of these tools have described a wide range of different security threats or incidents, whereby the perpetrators *intentionally* threaten or attack the programme because of its association with HIV and key populations. Examples of the threats and incidents that key population organisations and programmes often face include:

- Media campaigns against a CSO—characterizing CSO leadership and staff as promoting homosexuality and prostitution—resulted in mental health harm and social ostracization of CSO workers. The organisation was forced to shut down for weeks until waves of popular anger died down, limiting access to HIV services.
- An individual posing as a beneficiary came into a CSO serving KP members and filmed condom distribution. The individual then posted the video online and claimed the CSO engaged in illegal and immoral activity. The CSO was attacked by angry neighbours and had to cease operations for a time.
- An outreach worker was imprisoned for several days for carrying condoms. Upon release, the worker was rejected by family members and became homeless. This affected both the individual's ability to work and the morale of other outreach staff.
- Beneficiaries became angry with and verbally abused CSO workers when the CSO could not meet their holistic needs, such as nutritional support. The CSO workers experienced mental distress and fear for their physical safety. In some cases, workers left the organisation due to the stress.
- Outreach workers have been arrested based on a false accusation of soliciting sex when they distribute condoms, limiting their ability to effectively delivery commodities.
- A mobile testing bus was nearly run over when extremist university students formed a crowd to protest against messages, such as the importance of using condoms, which they considered immoral. This limited future outreach efforts in the district.

- A CSO's website was hacked and online trolling campaigns were organised against it after the CSO sought to decrease stigma against KP members through public messaging. Money had to be diverted from other programming or obtained through fundraising to increase cybersecurity.
- Verbal abuse, theft, and sometimes physical attacks against programme implementer staff, including clinicians, were reported at drop-in centres. This led to stress, economic loss, and turnover among workers.
- The family of a beneficiary learned their child was receiving services from a CSO that sought to reduce the risk of HIV infection among KP members. The family accused the CSO of trafficking the beneficiary and sought to bring criminal charges. The CSO's reputation suffered, and staff time had to be diverted to address the false charge.

Key recommendations for programme security

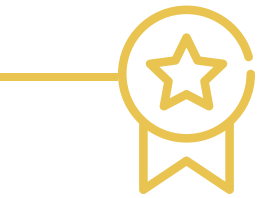
These recommendations have been developed by consensus during work on programme security with key population programmes across the world. They are relevant not just for programmes on the frontline, but also for Principal Recipients, Sub Recipients and the Global Fund. They are provided here to support your overall thinking on security.

- ✓ Make HIV programme principles and approaches the foundation of security efforts. These include "nothing about us without us" and "first, do no harm."
- ✓ Make security a priority and resource it explicitly.
- ✓ Make a safe workplace, including one that protects and promotes mental health, the organisation's responsibility.
- ✓ Plan ahead and make sure that everyone knows the plan (while maintaining flexibility).
- ✓ Explicitly discuss the level of risk that is acceptable organisationally and individually.
- ✓ Operate with a knowledge of both the actual risks and their underlying causes (including legal frameworks).
- ✓ Acknowledge the different vulnerabilities and capacities of each worker in security planning.
- ✓ Get to know all stakeholders, not just obvious allies.
- ✓ Identify both threats (physical, digital, psychological) and security strategies holistically.
- ✓ Be together with other programmes, work in coalition, and learn from one another.

Overview of the tools

What do we mean by programme security?

Programme security is about reducing and responding to *intentional* violence and threats towards the programme and anyone involved in the programme. For HIV key population programmes this normally refers to the programmes being threatened or attacked precisely because they are working on HIV with key populations. There are different causes and different perpetrators but the origin of these threats and attacks is often stigmatisation and non-acceptance of key populations.



What are the tools for?

The tools are designed to help organisations involved in delivering HIV key population programmes to:

- systematically identify their capacities, strengths and weaknesses in relation to security;
- identify priority risks that need to be addressed and track threats to their organisations and workers;
- make plans that will enable them to reduce those risks and threats or their vulnerability to them;
- and, ensure they respond effectively whenever incidents occur.

Many strategies to improve programme security involve changing the organisation's ways of working, or putting in place measures to reduce risks. In some cases it may also be necessary to include new activities in the programme – for instance greater advocacy with local authorities and security forces – or to buy equipment or pay for services and expertise that will help improve security. These costs are eligible for funding by the Global Fund, so it is important to make sure they are included in funding requests to the Global Fund and in sub-grants or sub-contracts to front-line implementing organisations. Results from using these tools can therefore inform planning and budgeting for Global Fund grants.

Who should use the tools?

The security problems faced by HIV key population programmes are very specific to each organisation and location where programmes are delivered. The actions needed to reduce security challenges are also specific to each organisation and location. Even where different key population programmes face similar threats and incidents, it is important that they identify the solutions that work for them.

For this reason, these tools are designed primarily to be used by front line organisations working on programme delivery – for instance in HIV treatment support, peer education, or human rights work for key populations.

In Global Fund supported programmes, these front-line organisations are often receiving funds not directly from the Global Fund, but from principal recipients (PRs) or sub-recipients (SRs). PRs and SRs have a role in supporting and strengthening the capacity of front-line organisations, particularly when they are community-led organisations. PRs and SRs can therefore also use these programme security tools to facilitate security planning with the front-line organisations they are supporting. Also, many PRs and SRs themselves face security risks, and they can therefore also use these tools to ensure they are working as safely as possible.

Summary of the security planning tools and process

Each of the tools in this pack is useful in its own right for organisations involved in HIV key population programming. Using just one of the tools is likely to be beneficial in terms of improving how the programme thinks about and acts on security concerns.

At the same time the tools can also be seen as different steps of a planning process that will lead toward effectively embedding security into Global Fund Funding Requests and Grants. This process and the corresponding tools are summarised in the diagramme below.

Useful resources

https://www.fhi360.org/resource/aman-mena-toolkit

https://www.fhi360.org/resource/implementer-and-data-security

https://www.fhi360.org/resource/when-situations-go-bad-worse-guidance-international-and-regional-actors-responding-acute

https://www.fhi360.org/sites/default/files/media/documents/resource-secure-mobile-devices-apps.pdf

https://www.fhi360.org/sites/default/files/media/documents/resource-linkages-safety-security-toolkit.pdf

PART 2: THE TOOLS

01

Tool 1: Security Incident Log

Description

This tool provides a template for systematically recording security incidents, including threats, that the organisation or individuals working in the programme face. Users can describe the incident, when it occurred, why, and who perpetrated it, along with a number of other details. It can record patterns in terms of types of incident or perpetrator, or even the times (of the year, of the week or of the day) when incidents most often occur. This is useful because it allows the organisation over time to understand what types of incidents occur, and how better to prevent and respond to them. The log can also be used to share information with other similar organisations so as to warn them of possible threats, and to share information with funders in order to encourage them to cover the costs of improved security. It can help identify:

- Riskier locations or activities
- Common perpetrators
- Whether a given incident or threat is also an indirect threat to others
- Whether violence is intensifying
- Who is most at risk

How to use it

The log can be used in many different ways, and it is up to each organisation to identify what works for them. The tool provided in this pack is in the form of a table in MS Word format. Users can make a new copy of the file (electronically or in hard copy) for every incident. If electronic versions are being used, the users should decide whether to copy and paste the table in the same document or to save a new file for each incident – what is most important is to keep records of all incidents in one place (e.g. in a dedicated electronic folder). Another alternative is to transfer the tool into a database format or Excel to help store the information in one place. If hard copies are being used, again each new form should be kept in the same place. In both cases the information should be kept secure, for instance as a password protected or encrypted file (electronic) or in a locked cabinet (hard copy).

Users should also decide who will complete logs and who will analyse them. The individual(s) directly affected by the incident should always be involved in completing the log, however the organisation can decide whether the individual does this alone or is supported by another person. Do not collect identifying information on the forms without the permission of the person sharing the incident. It is useful to have a focal point in the organisation who is responsible for storing and analysing the information. One way of using the information is to review all incidents periodically (e.g., during team meetings or retreats, or activity planning sessions) and to identify patterns and actions that should be taken to address these.

Finally, as with all of the tools, this tool can be adapted. Some users may feel that not all of the questions are relevant or that additional questions are needed. The main principle should be to only collect information that is likely to be useful, and to avoid making the process too burdensome, especially for individuals who have recently been through a traumatic experience.

NB note that this log is likely to contain confidential and sensitive information. Consider developing a coding system to avoid including personal information, in particular under “6. Target” and “7. Where incident occurred”.

A fictional example of a completed log for a security incident is shown below:

Security Incident log – fictional example			
	Question	How to Answer	Response
1	Incident #	Begin with number 1 and continue; the numbering allows security incidents to be linked to one another (see question #14)	10
2	Date of incident	Type as YEAR-MONTH-DAY (e.g., 2019-02-17 for February 17, 2019) to organise this security event log by date	2022-11-4
3	Time of incident	Specific time of day (if known), or more general (morning, afternoon, evening, night)	11h34AM
4	Perpetrator	If known and safe to list, or use a more general term such as "law enforcement officer"	Unknown attacker – possibly local gang member
5	Affected organisation	Name of HIV programme implementing partner (i.e., community-based organisation's name)	Fictional Organisation
6	Target	Specific person or type of staff, physical space (e.g., name of a specific hot spot), website, database, etc. Do not name individuals here unless you have their permission to do so.	Drop-in centre for key populations
7	Where incident occurred	Physical address, online, by phone, etc.	40 Independence Lane, Newtown
8	Believed motivation of aggressor (if known)	For example: intimidation, to stop programming, to deflect attention from other local issues	To intimidate the programme and damage the premises in order to stop the service as it was believed to encourage immoral behaviour
9	Description of security incident	For example: Facebook posts on project page said "[paste specific message here"]; or peer educators were arrested without charge when distributing condoms to a group of MSM during a mobile HIV testing event	The perpetrator violently attacked some of the centre users and volunteers
10	Programmatic consequences of security incident	For example: Implementing partner will conduct only online outreach until physical outreach is considered safe to conduct	The centre had to be temporarily closed, and subsequent outreach activities in this area were cancelled
11	Description of actions taken to respond to security incident	For example: On YEAR-MONTH-DAY, implementing partner targeted in Facebook post decided that it is not safe to conduct outreach activities for a two-week period and implementing partner filed a complaint with the police. Please include dates of actions taken (and continue to update this row as actions are taken).	The organisation filed a complaint with the police and local mayor but they took no action
12	Which other security incidents is this related to? (if any)	Note whether this incident was related to other security incidents by listing other security incident numbers here.	Related to incidents 2, 7 and 8
13	Incident resolution (if any)	For example: On YEAR-MONTH-DAY, peer educators were released from state custody and provided with mental health support.	As yet unresolved

For a downloadable version of this tool, please click on the links below:

- Word: https://www.civilsocietyhealth.org/website/wp-content/uploads/2022/12/1.-Security-Incident-Log-Word.docx
- Excel: https://www.civilsocietyhealth.org/website/wp-content/uploads/2022/12/1.-Security-Incident-Log-Excel.xlsx

02

Tool 2: Checklist of Security Strategies

Description

This checklist is designed to help implementers better understand where their organisation already has strong security measures and where there are opportunities to strengthen them further. Organisations complete a self-assessment of what they are currently doing, against a number of categories. The tool then provides a graph that is a visual representation of the strengths and weaknesses of the organisation.

As well as using this tool to identify the organisation's own needs, it is possible to use the results to facilitate peer-to-peer skills building with other similar organisations.

Using the checklist periodically can help an organisation to assess if it is making progress in any areas or if new challenges are emerging that need to be addressed.

How to use it

The tool comes in Excel format and includes detailed instructions for use, including who should complete which components of the assessment. While it is designed for use by individual organisations, it can also be used in the context of a meeting or workshop with multiple organisations to facilitate peer-to-peer learning. For example, representatives of each organisation can conduct the self-assessment for their own organisation, and following this each organisation can share its results, and provide more information to the other participants on the areas where they feel they are strongest.

For a downloadable version of this tool, please click on the link below:

- https://www.civilsocietyhealth.org/website/wp-content/uploads/2022/12/2.-Checklist-of-Security-Strategies.xlsx

03 Tool 3: Assessing threats, risks, and vulnerability

Description

It is important for any organisation experiencing security incidents to better understand why these are occurring. The Security Incident Log is a good starting point for this as it gathers detailed information on either threats or incidents that the organisation and its workers and volunteers have faced. By looking more closely at the Incident Log the organisation can identify what makes it or its workers vulnerable, and how serious the threats and risks are in terms of the likelihood of them materialising and their consequences. This in turn helps in thinking through what measures to put in place to prevent and respond to incidents. This tool provides some questions that can be used to assess threats, risks and vulnerability.

How to use it

There is no fixed format or approach to using this tool. The questions can be used by managers or team members when analysing incidents that have happened or as part of programme planning so as to ensure that security considerations are taken into account in activity plans.

A systematic approach to **assessing threats** includes working as a group with other programme workers to ask the following questions:

A. What are the facts surrounding the threat? (What do we actually know, not what we are assuming, about this threat?).

- This is helpful because it reminds us to move away from gossip or conjecture. Sometimes a threat can be overblown or underestimated because of the way others perceive it. Try to only think about the facts.

B. Is there a series of threats that become more systematic or frequent over time? (Does a person make threats each day or do they just harass opportunistically? Are they escalating in terms of how close they are, such as finding individuals at their home or workplace?).

- If something occurs multiple times, this increases the seriousness. It shows that making this threat is something the person/people feel a commitment too. Escalation of the threat—for example, someone was yelling at you when you were conducting outreach and now they have also found you online—is another sign that it is more serious.

C. Who is the person who is making the threats? (Is this someone known? Someone who has the ability to influence others? Someone who has information that could harm you or your colleagues?)

- This question tries to understand how much power the person threatening has. For example, a police officer making threats is likely to be more dangerous than a stranger.

D. What is the objective of the threat? (Is it to change your behaviour? Is it to scare? Is it a political tool to get votes?)

- Thinking about this can help you decide whether the person may be willing to escalate. For example, if this is just to scare me then maybe the person isn't going to ever physically harm me, even if they say they will. Knowing this can also help you decide how to act.

E. How serious do you think the threat is? (Your own personal views on the topic)

- Here is where you let your intuition and your understanding of the broader context inform your

thinking on the threat's seriousness. This analysis can be conducted based on the threats or incidents recorded in the organisation's security log.

Practically speaking the organisation or programme can examine each threat or incident that is recorded in the Security Log (see Tool 1) and complete a table addressing each of the questions above, as shown in the fictional example below, which covers the same incident described above.

Question	Answer (fictional)
What are the facts surrounding the threat?	A single perpetrator entered the drop-in centre and threatened and attacked service users and volunteers.
Are the threats part of a series that has become more systematic or frequent over time?	Yes, similar attempts have been made by other perpetrators although with less severity. They were all recorded in the incident log
Who is the person/people making the threats?	They appear to be members of the local community who live near the drop in centre, and may be local gang members. Several of them are known to be members of a church that consistently preaches against homosexuality.
What is the objective of the threat?	To prevent activities and shut down the centre.
How serious do you think the threat is?	Very serious. The physical and mental health of both service users and those working in the drop-in centre, which is a big concern. Because of the lack of action from the police we think it will happen again.

A more detailed analysis of a threat can be done by looking more closely at the perpetrator or attacker. A perpetrator or attacker needs the following to be able to carry out a threat or an act of violence:

- **Access**: to the potential victim or organisation, either physically or virtually. This could mean that they know where the programme is located and that they are able to enter unhindered; or that they can identify online workers through their online identities and use this to attack them or steal information.
- **Resources**: anything that can be used to carry out the attack – for instance, information about the victim's location or weaknesses; having a weapon or transport or money that enables them to carry out an attack.
- **Impunity**: this means that there are no consequences carrying out an attack: for instance no legal consequences or no social opposition to them doing so.
- **Motive**: a reason for carrying out an attack or making a threat. This may be to do with their attitudes towards the programme or population, or their assumptions about the same. In some cases, we may wish to limit what others know about the type of work we do. In other cases, we may want them to better understand what we do because it benefits the broader society. In some other cases, we may decide that changing what others think is not our goal and we prefer to limit the other three domains.

The reason to look at these four factors is that it can also help to identify how each of them can be reduced or mitigated. There are no "right" answers, and often limiting something like access for an attacker could also limit it for your programme beneficiaries (e.g., if you don't share your clinic's address online, neither an attacker nor person seeking HIV testing will find you easily). Making these decisions involves trade-offs. Once again, a table can be used to do this analysis in a systematic way, as shown below, using the same fictional example as used above.

	What does the attacker currently have?	How can your programme reduce these?	What are the trade-offs if you decide to act in this way?
Access	The attacker is able to enter the key population drop-in centre unimpeded.	Ensure there is a log for all visitors and that they are screened/ there is a security guard.	Need for resources to implement some security measures.
Resources	The attacker has specific information about the location of the centre and has a weapon.	The organisation can make the fact that the centre serves key populations less obvious or less public.	Genuine service users may not be able to locate the clinic as easily; some may favour visibility in order to assert their rights.
Impunity	Local community leaders and media do not vocally oppose the attacker and police do not investigate.	Advocacy to ensure stakeholders understand that all people have rights; engage legal assistance to ensure investigations take place and charges are brought.	Requires long term effort and commitment, and close monitoring of the situation.
Motive	Stigma and negative attitudes towards key populations; jealousy of key population specific services.	Provide services to the broader/ general population. Work with local leaders and community to improve attitudes.	Some key population service users may be deterred from using services if they are accessible to broader population.

For a downloadable version of this tool, please click on the link below:

- https://www.civilsocietyhealth.org/website/wp-content/uploads/2022/12/3.-Assessing-Threats.docx

04 Tool 4: Security planning

Description

This tool provides a basic framework that brings together the information from the other tools (on capacity, threats, risks, vulnerabilities and incidents) into a plan that is likely to help prevent incidents happening and that help the programme to respond effectively when threats or incidents happen.

Within a key population programme, there are different risks or vulnerabilities associated with different activities – for instance, in-person outreach and online outreach have different risks associated with them; as do different venues. If the programme includes a premises such as a clinic or a drop-in centre then they may also have specific vulnerabilities that need to be addressed through security measures.

Many security measures involve simple changes in the ways an organisation or programme works and may not necessarily involve costs. However, strengthening security can also require new equipment, advice or staffing that need to be costed and included as part of programme budgets.

How to use it

The planning approach recommended in this tool is aimed at assessing risks and making a plan for *each* type of activity that is conducted within the programme. The outcome of the security planning exercise is not one security plan for the entire programme or organisation, but rather a set of specific security plans, each related to each activity the programme undertakes or risk that it faces.

Because security planning should be an integral part of activity planning or work planning, rather than a separate process, it is recommended that this security planning tool be used each time activity plans are designed or reviewed. Insights from the incident log, the checklist of security strategies and the threat analysis should be used to inform this process.

By the end of the process people involved in implementing each activity should have participated in identifying security risks and in agreeing appropriate security measures. Because security risks can change over time, the security plans for each activity should also be updated periodically, particularly when situations are known to have changed.

Security planning involves making a plan to reduce the risks of harm to implementers associated with any given activity. At the same time this is also likely to benefit beneficiaries and the broader community. This tool should therefore be used to plan for security in relation to each of the organisation or programme's activities and each of the most important security concerns related to that activity.

A separate plan would be needed for each drop-in centre, each outreach location or activity, (with different plans for in-person and online outreach), etc.

These plans should also be reviewed over time. It is suggested that this be done during routine programme team/planning meetings so that it becomes a core part of planning, rather than a separate activity.

Security plans should be informed by the information and analyses collected through tools 1, 2 and 3. Plans can take the form of a simple table – here is an example of a completed table for risks faced during outreach to key populations in bars:

Security plan for:	Outreach to bars by sex worker peer educators
Date security plan developed/last reviewed:	1/1/2020
Person responsible:	A Manager
Risk to be addressed:	Risk of workers being physically assaulted during outreach to bars

Threats	Vulnerabilities	Existing capacity	Required capacity
Verbal abuse, including threats of physical violence, have occurred since the project began and have recently increased: the perpetrators are often the bar owners who do not want outreach to occur in their business	Outreach is done by sex workers who are unlikely to report abuse: outreach occurs at night on a regular basis: transport is on foot: bar owners do not want the outreach workers to encourage sex workers to use condoms because they believe clients will pay less	Peer outreach workers wear ID cards that show they are connected to the Ministry of Health and include a phone number to reach a local trained police officer: peers work in pairs: peers have pre-paid airtime in case of emergency: peers are trained in how to describe their work in non-controversial way: their locations are tracked using a log book: they have safe havens in each neighbourhood they work in as they are known and respected by the sex workers.	In addition to the existing capacity, begin sensitizing bar owners to decrease their abusive behaviours. If risks to the outreach workers remain high relocate activities to other places where sex workers gather.

Although each activity requires its own security plan, it is very likely that different plans will include similar measures. Programme managers should therefore review all the plans and identify whether some measures can be taken jointly, for instance in relation to training staff or allies; or purchasing equipment that can be used to make all activities safer.

Consider also prioritising developing security plans for the most significant threats that your programme faces.

For a downloadable version of this tool, please click on the link below:

- https://www.civilsocietyhealth.org/website/wp-content/uploads/2022/12/4.-Security-Planning.docx

05

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

Description

Although security measures are very contextual and one size does not fit all, experience shows that it is useful to provide some suggestions as to the types of actions that can be planned and how they can be included in Global Fund grants, in particular if they have cost implications. This tool provides some basic ideas and some hints on how to include them in grant plans.

How to use it

Unlike the other tools this is not a checklist or a specific activity, rather it is a set of suggestions that users can consider. It is not recommended that all of the activities be included automatically in a programme plan; rather, implementers should consider whether any of these activities would be useful in helping them make their programmes more secure.

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.

A. 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-centres
- 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.

B. 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).

C. Provide training for all workers (including staff and volunteers) on how to approach security when implementing the programme. 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.

D. 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.

E. 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.

F. 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).

G. 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.

H. 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

A. 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.

B. 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)[1]. 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.

An important element of programme security is the ability to respond when an incident occurs, in order to provide immediate assistance to affected programme workers - this could include emergency accommodation, evacuation, health care, or legal assistance. As with any activity being proposed for Global Fund support, including a budget line for such a fund in a funding request needs to be demonstrated to be necessary, reasonable, and contributing directly or indirectly to the programme objectives. Including within funding requests evidence of prior incidents and threats and of their impact on the programme will therefore be important. The use of emergency funds will need to follow applicable laws and regulations, and transparent and equitable criteria and conditions for their allocation to beneficiaries will be required.

C. 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.

D. 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.

1 https://www.theglobalfund.org/en/applying-for-funding/design-and-submit-funding-requests/applicant-guidance-materials/


CIVIL SOCIETY INSTITUTE
FOR HIV AND HEALTH
CSO
WCA


fhi360
THE SCIENCE OF IMPROVING LIVES


THE
GLOBAL
FUND