vialibre | Regional Platform Latin America and the Caribbean

TOOLKIT

Safety and Security for organizations working with key and vulnerable populatons to strenghthen HIV programs in Latin America and the Caribbean

February 2022

TOOL KIT: Safety and Security for organizations working with key and vulnerable populatons to strenghthen HIV programs in Latin America and the Caribbean, It is a document prepared jointly by Latin America and the Caribbean Regional Platform Community, Rights and Gender Strategic Initiative, (Plataforma LAC) Community, Rights and Gender Strategic Initiative Global Fund to Fight AIDS, Tuberculosis and Malaria

First edition
Lima, Peru. February 2022

Jr. Paraguay 490, Cercado de Lima, Lima 1, Perú
vialibre@vialibre.org.pe | www.vialibre.org.pe | www.plataformalac.org/
Telephone: (+511) 203-9900

Executive Director
Dr. Robinson Cabello

Adaptation to the context of Latin America and the Caribbean
Rosa González
Alfredo Mejía Duarte

Technical & Editorial Oversight
Anuar Luna

LAC Platform Technical Coordinator
Anuar I. Luna Cadena

Translation
Carmen Luisa Franco Hip
Alejandro M. García

Layout & Design
Juan Carlos Rodríguez Espinosa

The Latin America and the Caribbean Regional Platform for Support, Coordination and Communication of Civil Society and Communities (LAC Platform), is an initiative implemented by Vía Libre, with financial support of the Global Fund to Fight AIDS, Tuberculosis and Malaria (Global Fund).

It is part of several interventions of the Global Fund to support and strengthen community and civil society participation at all levels within their processes. It is a component of the Strategic Initiative on Community, Rights and Gender (SI CRG).

This document is an adaptation of the original version prepared within the Linkages Project with the Continuum of HIV Services for Key Populations Affected by HIV (LINKAGES). LOVE MENA. Protection and Security for organizations working with key populations to strengthen HIV programs in the Middle East and North Africa. Durham, North Carolina: FHI 360; 2020. “Aman” is an Arabic word that means safe or secure. The organizations that contributed to the development of this toolkit entitled it AMAN MENA because, in a region with so many differences, Arabic is the language spoken in all territories.

Funding disclaimer: This toolkit is made possible by the generous support of the American people through the U.S. Agency for International Development (USAID) through the terms of cooperative agreement #AID-OAA-A-14-00045. The contents are the responsibility of the LINKAGES project and do not necessarily reflect the views of USAID, or the United States Government.

Acknowledgments

This document has been adapted from two Toolkits: Continuum of HIV Services for Key Populations Affected by HIV (LINKAGES) Project Safety Toolkit and Strengthening HIV Program Implementation for Key Populations in the Middle East and North Africa (MENA) Region by Frontline AIDS by Robyn Dayton and Cherif Soliman (FHI 360), and Mahdy Charafeddin and Elie Ballan (Arab Foundation for Freedoms and Equality).

Acronyms

CCM	Country Coordinating Mechanism
CSO	Civil Society Organization
FSW	Female Sex Worker
GBV	Gender - based Violence
LAC	Latin America and the Caribbean
MOH	Ministry of Health
MSM	Men who have sex with men
NAP	National AIDS Program
PLHIV	People Living with HIV
PWID	People Who Inject Drugs
TW	Transgender Women
UIC	Unique Identifier Code
UN	United Nations

Table of Contents

1. Introduction

Background

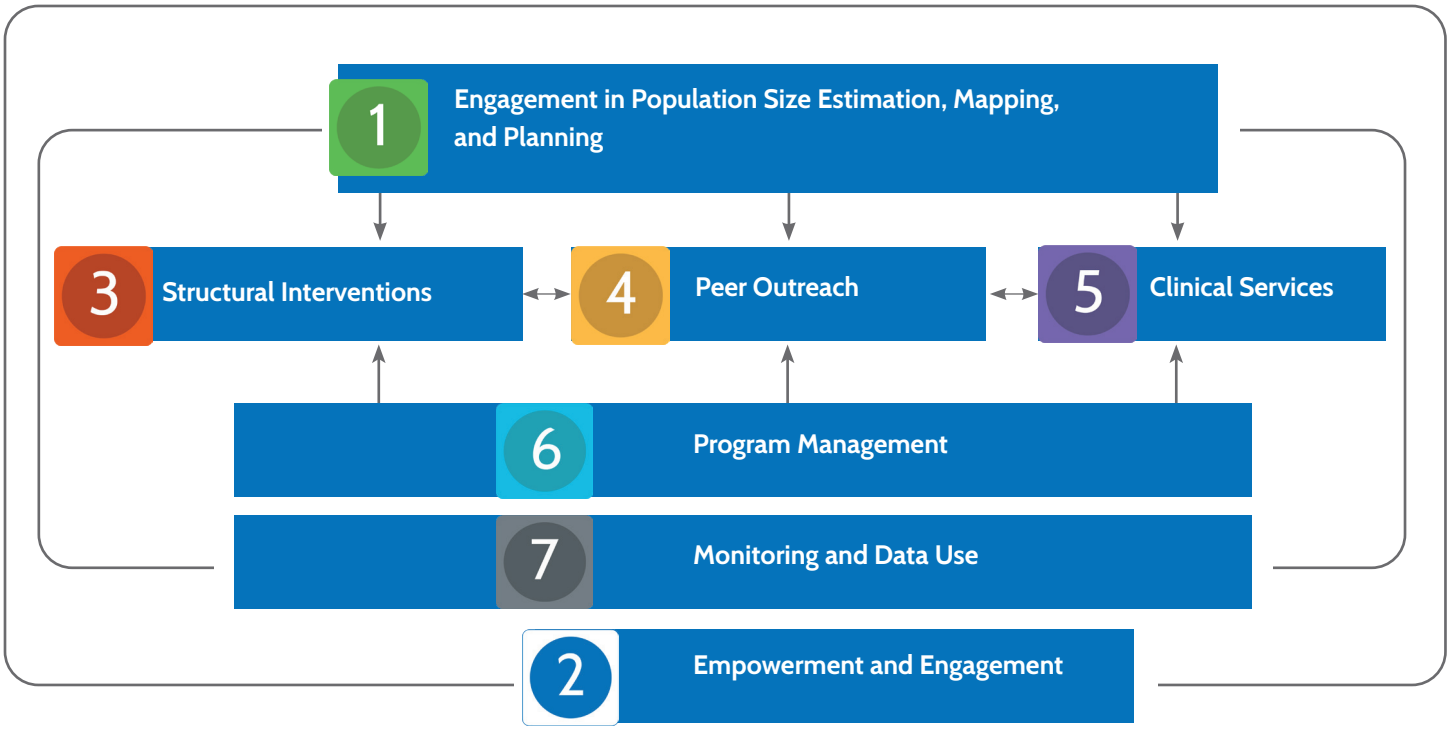
There is a growing awareness of the violence experienced by members of and individuals who work with key and vulnerable populations most affected by HIV, even more so when they are part of said populations.

Evidence of the impact of such violence—on the safety and security of individuals, families, and communities—has been documented by a range of organizations and, in turn, has been the subject of national, regional, and global advocacy. Countries in Latin America and the Caribbean (LAC) are no exception.

In recent years, a series of extreme situations across LAC have highlighted that hostile environments and rights violations affect the safety and security not only of KP members, but also the people, organizations, and programs that support them and their right to health. In this way, safety and security challenges can negatively affect all aspects of the HIV program cycle as illustrated in **Figure 1**, which is based on guidance produced by LINKAGES[1]. Additionally, in many HIV programs, the staff, volunteers, and associates are themselves KP members. As such, they experience safety and security challenges in both their professional and personal lives.

Some organizations and individuals operating HIV programs in the LAC region have found effective ways to limit or mitigate the harm from safety and security challenges and/or respond effectively in the face of violence. However, a greater and more systematic investment is needed to strengthen safety and security for the protection of implementers and programs working to achieve epidemic control.

FIGURE 1: SAFETY AND SECURITY CHALLENGE EXAMPLES IN SEVEN KEY AND VULNERABLE POPULATION PROGRAM AREAS IN LAC



1

It can be difficult to undertake behavioral or biomedical surveys or other health surveillance when data collectors cannot move freely due to safety concerns. Individuals conducting surveys, especially if they are peers, run the risk of arrest or having the data they have collected confiscated. Without reliable data, the HIV program is unable to understand the extent of need and to advocate effectively for a strengthened response..

2

Contratar a miembros de poblaciones 2. Hiring members of KPs or engaging civil society organizations (CSOs) led by KP members—which is acknowledged as a central component of effective HIV programming for key population[2] - is much more difficult when safety concerns require individuals and CSOs to reduce their visibility in order to prevent risks.

3

Widespread hostility toward KP members makes it more difficult to link them to services, such as support from a lawyer, that could address some of the structural risks—for example, discrimination in formal workplaces—that increase their vulnerability to HIV.

4

Harassment of workers during outreach by both the families of beneficiaries and law enforcement limits the times of day and locations where outreach can be safely conducted, thereby limiting the reach of the program. In many settings distributing condoms, lubricant, or harm-reduction materials is not safe under any condition or is safe only if the outreach worker carries very small quantities.

5

Doctors, nurses, psychologists, and other clinical staff may be targeted for their work with KP members, increasing burnout and making it more difficult to find qualified staff.

6

Managers of an HIV program might be unable to meet their programmatic objectives if a large proportion of their energy and project resources is required to respond to safety and security challenges.

7

A threatening environment - such as with regular police raids and cyberattacks—makes it difficult for HIV program implementers to ensure the safety of electronic data. Theft of equipment such as laptops, especially when project budgets do not cover replacement, can inhibit data entry and management.

1. Introduction

Safety and Security for organizations working with key and vulnerable populatons to strenghthen HIV programs in Latin America and the Caribbean

One of the greatest vulnerability factors associated with HIV is stigma and discrimination against the disease and against the main key populations: people living with HIV (PLWH), men who have sex with men (MSM), people who inject drugs (PWID), female sex workers (FSW), transgender people (TP) and, more recently, irregular migrant population. As in other regions of the world, community leaders working on issues related to HIV and the defense and promotion of human rights in Latin America and the Caribbean (LAC) are exposed to risks and threats associated with the activities carried out with these key populations

The impact of such risks on the safety and security of leaders, families and communities has been documented by a variety of organizations, and has been the subject of national, regional and global advocacy analyses. These threats are even greater in countries with political instability. One such example is the assassination in June 2021 of Andrea González, a transgender leader who was part of the Country Coordinating Mechanism (CCM) in Guatemala, and who led OTRANS, an organization that works for the rights of transgender people[3].

3.- https://www.dw.com/es/guatemala-asesinan-a-balazos-a-andrea-gonzález-dirigente-lgbtiq/a-57870338 [in Spanish]

1. Introduction

By being considered as human rights defenders of the populations they work with, leaders of key populations in LAC see their vulnerabilities increased. The Inter-American Commission on Human Rights (IACHR) has found that human rights defenders of LGBTI people and other key populations in LAC are more vulnerable to violence due to three factors[4]:

1. They identify themselves as LGBT or as members of other key populations who are already vulnerable to increased violence due to their sexuality, behavior, orientation and/or gender identity;

2. They experience additional vulnerability to violence due to their role as human rights defenders and because of the specific causes they advocate for; and

3. They face alarming levels of vulnerability to violence triggered by the intersection of their sexual orientation, gender identity, their occupation or behavior, and their role as defenders of causes linked to key populations.

In 2018, the former International HIV/AIDS Alliance (IHAA) (currently known as Frontline AIDS), a member of the Technical Advisory Group on Violence, Stigma, and Discrimination Against Key Populations, for the USAID LINKAGES Project, created the *Safety and Security Toolkit: Strengthening the Implementation of HIV Programs for and with Key Populations*[5]. This toolkit was developed to help program implementers, particularly community-based organization (CBOs) and others working in direct service delivery, to more effectively address safety and security challenges within their implementation of HIV programs. It was designed for use in hostile environments; for example, where members of key populations are criminalized and face elevated levels of stigma, discrimination, and violence. It seeks to amplify good programming through identifying and cataloging promising practices and tools, making overarching recommendations to address safety and security challenges, and providing a systematic approach to identify and respond to one's own safety and security gaps.

4.- Inter-American Commission on Human Rights (2015): Violence Against LGBT People.
5.- USAID, PEPFAR, Alliance, LINKAGES (2018). Safety and Security Toolkit: Strengthening the Implementation of HIV Programs for and with Key Populations

1. Introduction

The toolkit was developed due to the growing safety and security concerns of many local partners in the region who—in collaboration with the former International HIV/AIDS Alliance, LINKAGES, and other members of the TAG—implement programs for and with key populations. However, much of the content of the toolkit is relevant globally, and it is up to each implementer to determine whether a specific practice, recommendation, or resource is appropriate for their setting. In turn, this tool served as the basis for the composition in 2020 of the document titled "Secure in MENA region: Security Protections for Organizations Working with Key Populations to Strengthen HIV Programming in the Middle East and North Africa[6].

Both the Community, Rights and Gender Strategic Initiative (CRG SI) of the Global Fund, and the Latin America and the Caribbean Regional Platform/Vía Libre consider it of vital importance to have a similar tool adapted to LAC, given the risks that leaders, outreach workers, programme people, service providers and community mobilizers face in their work with key populations in these countries.

Accordingly, this toolkit has been adapted to the regional context of LAC, as well as to the realities and dynamics related to stigma, discrimination and security risks that leaders, outreach workers, programme people, service providers and community mobilizers face in their response to HIV.

This toolkit intends to provide information and recommendations to address security and protection issues for leaders, outreach workers, programme people, service providers, community mobilizers and CSOs working on human rights and HIV issues with key populations in LAC.

6.- USAID, FHI360, LINKAGES, UNAIDS, and others (2020) AMAN MENA, Secure in MENA region: Security Protections for Organizations Working with Key Populations to Strengthen HIV Programming in the Middle East and North Africa.

1. Introduction

· Purpose

This toolkit was developed to help organizations and individuals implementing HIV programs for and with key and vulnerable populations in the LAC region to more effectively address safety and security challenges

It can be used for KP and people living with HIV (PLHIV) initiatives and collectives; HIV program implementers (including health care workers and other medical staff); local, national, and regional networks working on KP issues and/ or HIV; international NGOs, donors, government ministries and national AIDS programs; and United Nations organizations operating in LAC. The toolkit focuses on implementer safety, although acknowledges that the safety and security challenges experienced by *implementers*, of HIV programs also, inevitably, affect *beneficiaries* of those services. While the toolkit was designed with CSOs in mind, public sector implementers, such as health care workers, will also find many of the challenges and strategies relevant to their work.

The toolkit amplifies good programming by identifying and cataloging promising practices and tools from the region, making overarching recommendations to address safety and security challenges and providing a systematic approach (via checklist) to identify and respond to one's own safety and security gaps. It is not prescriptive. While recommendations and specific examples are provided, readers should use the information presented to weigh the best options and determine whether a specific practice, recommendation, or resource is appropriate for their setting. All decisions should be made keeping in mind that HIV programs for and with KP members must strive to *"first do no harm"* [7]. This tool kit is also aimed at consultants who facilitate security and protection risk analysis processes, as well as the formulation of projects, programs and institutional policies on the subject.

1. Introduction

· Objetives

- To encourage a discussion between leaders, outreach workers, community mobilizers and members of CSOs about the risks they face in the course of their activities (defense of human rights, prevention, outreach to key populations, etc.).

- To provide general recommendations on how to address the safety and security risks faced by those who work with key populations.

- To serve as a guide in the formulation of action plans to reduce the vulnerability of leaders, outreach workers, community mobilizers and members of CSOs working with key populations.

· Who is this toolkit for?

- Leaders, outreach workers, community mobilizers and members of CSOs working with key populations (PLWH, MSM, PWID, FSW, TP, migrants) on Human Rights and HIV related issues in LAC.

- Funders that include amongst their priorities resources to reduce the safety and security risks of leaders, outreach workers, community mobilizers and members of CSOs working with key populations on Human Rights and HIV related issues.

- Consultants that aid in the safety and security analysis process for leaders, outreach workers, programe people, service providers, community mobilizers and CSOs working with key populations in the countries of the LAC region.

1. Introduction

· Description

The toolkit contains three tools, as described in **Table 1**. These tools are meant to be used together.

We recommend that an organization interested in making KP programs safer to implement begin by reading **Tool 1: Review of Issues, Promising Practices, and Recommendations to understand the issues**, their impacts, and how other organizations have responded to safety and security challenges. Once the reader understands the importance and general approach to investments in safety and security, they can use **Tool 2: Checklist** to assess their existing efforts to address safety and security challenges and identify areas for improvement. Each item on the checklist is also a potential strategy they can begin to employ or strengthen further. As such, after completing the checklist the reader may return to **Tool 1** to read examples of safety and security strategies that fall under strategy areas they wish to strengthen and/or the reader

Tool 3: Methodology for the development of safety and security workplans and projects. This tool offers participatory methodological guidelines for the development of projects, workplans and institutional policies to reducing security risks and protection of leaders and organizations.

Alternatively, organizations can begin by completing **Tool 2** to identify their strengths and gaps and read **Tool 1** with priority areas for investment in mind.

TABLE 1: SAFETY AND SECURITY TOOLKIT

TOOL 1: REVIEW

The review describes contextual factors shaping safety and security challenges in the LAC region, details the impact of such challenges on the HIV response, identifies promising practices, and makes recommendations to help mitigate and respond effectively to safety and security challenges in KP programs.

TOOL 2: CHECKLIST

It includes a checklist and instructions on how to use it to help HIV program implementers working in LAC conduct a systematic scan, self-assess, and plan how to respond to the security needs of their organizations. As the checklists are completed, a table allows implementers to score and monitor their progress in seven aspects and three cross-cutting areas.

TOOL 3: METHODOLOGY FOR THE DEVELOPMENT OF SAFETY AND SECURITY WORKPLANS AND PROJECTS

This tool offers participatory methodological guidelines for the development of projects, workplans and institutional policies to reduce safety and security risks of leaders and organizations

1. Introduction

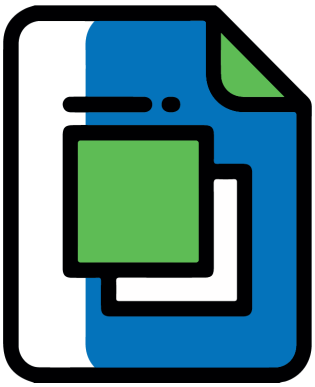
· Key Terms

The terminology used in the toolkit is informed by the resources of a range of CSOs, donors, and United Nations (UN) agencies, as well as security experts (see box "Definitions" for key terms).

Although there are different definitions of **key and vulnerable populations**, this toolkit focuses on four most vulnerable populations in our region and prioritized by GF actions:

- **Men who have sex with men**
- **People who inject drugs**
- **Female sex workers**
- **Transgender people**

This toolkit defines **HIV programs** as activities, services, and advocacy related to HIV prevention, care, support, and treatment. It primarily focuses on workers involved in the implementation of such efforts. This includes paid staff as well as paid and unpaid volunteers, associates, contractors, and casual workers. Examples include:



- Outreach workers and community mobilizers
- Peer educators/navigators
- Community health workers
- Community members
- Program directors and managers
- Program officers
- Drop-in center workers
- Clinicians (e.g., doctors, nurses)
- Counselors and psychosocial support providers
- Office staff (e.g., receptionists)
- Support staff (e.g., drivers, guards)
- Community activists, advocates, and campaigners
- Lawyers and paralegals
- Allies and championsi [8]

8 These may include donors, religious leaders, media, politicians, and law enforcement officers who promote the well-being of members of KPs.

1. Introduction

· Definitions

Violence against members of KPs violates their right to health and negatively impacts the ability of HIV programs to effectively respond to the epidemic. Violence refers to[9]:

- **Economic abuse** (e.g., blackmail, robbery, a client refusing to pay, withholding economic resources, charge fees to get the job done)
- **Psychological/emotional abuse** (e.g., humiliation, bullying, verbal abuse, making someone feel afraid)
- **Physical abuse** (e.g., choking, hitting, kicking, use of a weapon)
- **Sexual abuse** (e.g., rape, groping, forced sex without a condom)
- **Institutional and systemic violations of rights**, including extrajudicial killings, deregistration as retaliation, arbitrary arrest and/or detention, denial of the right to assemble, confiscation of essential HIV prevention commodities (e.g., condoms and lubricants)

Safety and Security: The terms security and safety are often used interchangeably, but have different definitions. Security is primarily concerned with intentional acts of violence, aggression, and/or criminal acts against agency staff, assets, or property, whereas safety relates to unintentional or accidental acts, events, or hazards [10]. The emphasis of the toolkit is on security, but safety is often addressed simultaneously.

Risk[11]: the probability that something harmful will happen.

Threat: indication/sign that someone wants to hurt, damage, or punish another; these are external.

Capacity: any resource (financial, ability, contacts, infrastructure, personality, etc.) that can be used to improve security; these are internal

Vulnerability: anything that puts someone at a higher level of exposure to those who want to harm them

TOOL 1

REVIEW OF CONTEXT, PROMISING PRACTICES, AND RECOMMENDATIONS

Purpose of Tool 1

This tool describes safety and security challenges faced by key population programs in LAC, details the effect of these challenges on the HIV response, and identifies best practices and recommendations to help program implementers mitigate and respond effectively to these challenges.

Factors shaping safety and security challenges

Preventing, mitigating, or responding to safety and security challenges

Recommendations to inform the response to safety and security challenges

Click on each circle to learn more

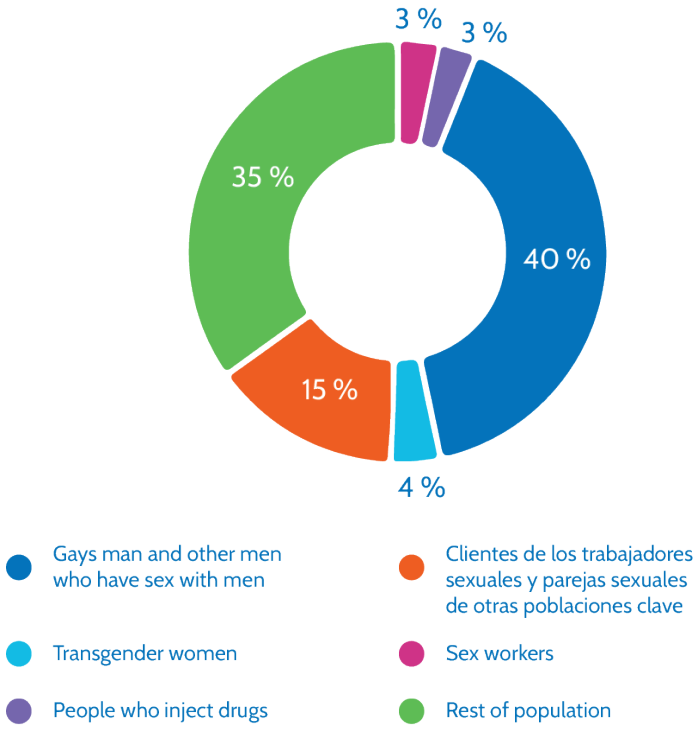
Factors shaping Safety and Security Challenges

Operating HIV programs in the LAC region is uniquely challenging. The epidemic in the region is concentrated; key population members and their partners accounted for more than 65 percent of new HIV infections in 2018.

By way of comparison, globally, KP members and their sexual partners accounted for 47 percent of new infections. This is represented dramatically by UNAIDS in their 2019 report that shows 35 % of infections in the region occurring among members of the "rest of the population" **(Figure 2)**.

While KP members and their sexual partners account for 95 % of HIV infections, and international guidance on effective HIV programming mandates a focus on key populations [12], a variety of factors make KP programming in LAC challenging. These factors are exploredin **Table 2**, and the unique combinations of these factors in different settings help to explain variation regionally.

FIGURE 2: Distribution of new hiv infections in LAC, 2018



Source: UNAIDS Special Analysis, 2019.

TABLE 2: ENVIRONMENTAL FACTORS AFFECTING THE SAFETY AND SECURITY OF HIV PROGRAMS IN LAC

FACTOR[13]	EXPLANATION AND EXAMPLES
CRIMINALIZATION	When same sex sexual relationships, drug use, and sex work are criminalized[14], individuals providing HIV services to KP members can be perceived as condoning illegal behavior, increasing their risk of being targeted by law enforcement. The criminalization of sex outside of marriage can also impact the safety with which commodities such as condoms can be carried and distributed.
STRENGTH AND CAPACITY OF THE MINISTRY OF HEALTH OR NATIONAL AIDS PROGRAM	The support of an influential Ministry of Health (MOH) or National AIDS Program (NAP) can help program implementers connect to other ministries (such as the Ministry of the Interior) to explain the importance of efforts to curb the HIV epidemic, including through work with KP members. The MOH or NAP can also be called upon to explain the importance of the program publicly if there are questions about government endorsement of implementers' activities. Identification cards with an MOH stamp and/or an official letter describing the MOH's support for the specific program activity can also be provided. The capacity and strength of the ministry primarily tasked with HIV response may also affect their coordination with other ministries in a way that impacts the security of KP programs. For example, if the MOH approves outreach to KP members but has not coordinated with the Ministry of Interior, or their attempts at coordination have been unsuccessful, outreach workers may be arrested by law enforcement even while participating in a government-supported initiative.
STRENGTH OF CIVIL SOCIETY	CSOs play an important role in advocating for HIV services that meet the needs of KP members—such as CSO- based HIV testing services—and in holding governments accountable when services do not meet local needs or abuses against implementers occur. Organizations operating in countries with strong civil society may be more able to seek formal approval of strategies that are safer to implement (e.g., there is less chance of stigmatizing behavior toward both implementers and beneficiaries when HIV tests are provided at CSOs; there is also less need for peers to travel with beneficiaries to government facilities, limiting danger during transit) and to prevent abuses from occurring with impunity. There is a worrying trend of reduced space for civil society to operate across the region [15].

13 While these factors can be changed overtime, and some HIV programs also engage in advocacy to address root causes of safety and security challenges, HIV programs operating now can use their local knowledge of each of these factors to decide what risk mitigation strategies are needed and which are feasible.champions.

14 Transgender people are often charged under laws criminalizing other KP members either because they also engage in criminalized behaviors or because gender identity and sexual orientation are inappropriately conflated.

TABLE 2: ENVIRONMENTAL FACTORS AFFECTING THE SAFETY AND SECURITY OF HIV PROGRAMS IN LAC

FACTOR	EXPLANATION AND EXAMPLES
POLITICAL WILL	When HIV prevalence is high or HIV incidence is increasing rapidly, there can be more pressure on the government to provide HIV-related services and more understanding among the public of the need for such services. However, particularly in places where surveillance efforts have been curtailed, the data needed to create political will may be lacking.
POLITICAL UNREST OR RAPID CHANGE	Rapid social change occurring during times of political unrest can create opportunities for coalition building between KP-serving and KP-led organizations and others working for positive change. However, it can also mean increased oversight by government over civil society or restricted/observed movements for everyone, including those operating HIV programs. KP members may also become targets of scapegoating if there is a desire to distract from dissatisfaction with those in power. Rapid or serial changes in government leadership can also make it difficult to form relationships with government players because of high levels of turnover at institutions such as the MOH. This can impact implementers' ability to form strong alliances that would allow them to look to government for support. The challenging political environment can represent difficulties to establish relationships with government actors due to high levels of turnover in institutions such as the Minister of Health, impacting implementers' ability to form strong alliances to seek government support.
FUNDING/ FUNDERS	**Inconsistent or inadequate funding** makes security more difficult for program implementers who lose experienced staff and institutional knowledge on how to safely program. The mental health of remaining staff also suffers. Inconsistent or inadequate funding can also cause important overhead costs, such as building insurance or updated computer software, to become unaffordable affecting the ability of the implementers to operate safely. Finally, when funders prioritize low costs per person reached without simultaneously setting security standards, the organization that is able to "win" a new contract may do so by saving money in unsafe ways, such as using only the cheapest forms of transport (even when it is not safe to do so) or sending out peer educators alone instead of in pairs. **Unintentionally divisive funding:** International donors may also make requests of programmers that increase harm to KP-serving organizations. For example, asking that an organization focus only on the rights of a few when so many others' rights are restricted can cause a backlash and position some key populations as privileged and working in alignment with Western interests instead of working to improve the rights of all people.

TABLE 2: ENVIRONMENTAL FACTORS AFFECTING THE SAFETY AND SECURITY OF HIV PROGRAMS IN LAC

FACTOR	EXPLANATION AND EXAMPLES
FUNDING / FUNDERS, CONTINUED	**Internal barriers to funding** mean it is not only donor willingness to support programming that determines HIV program implementers' access to resources. In places where government oversight or bureaucracy limits access to timely funding, even adequate funding cannot be absorbed and used by those who need it. **Failure by funders to contemplate security adequately**: Funders are rarely willing to cover expenses such as insurance for staff and volunteers or psychological support for implementers to avoid burnout. This has a direct impact on the type of support implementing agencies can provide for their workers. **Explicit funder commitments**: Funders' active engagement in security processes, such as budget line items dedicated to security measures or commitments to support HIV program implementers if they come under attack, also influence how safely HIV programs can operate. When country coordinating mechanisms (CCM) are strong, this can be an important setting for discussions on how to manage and resource security issues that occur.
PUBLIC OPINION	KP members across the region continue to be perceived negatively, even while views of younger generations diverge somewhat from those who are older. This is particularly true for men who have sex with men—an attitude that is attributed in part to holy books that speak clearly against homosexuality and in part to the perception that other KP members deserve sympathy as victims of their circumstances (sex workers) or are individuals with an illness (people who use drugs). In contrast, men who have sex with men and transgender people are often described as having chosen to act against culture and religion. Compounding the issue are attacks against gender and sexual minorities by governments seeking to rally conservative backers, often as a diversion from governance failuress [16].
RURAL/URBAN LOCATION	Services for KP members are often concentrated in urban areas and may be perceived as more normal/ acceptable in this setting. Urban areas are also generally less conservative than rural ones. Additionally, outreach efforts in rural areas require travel over greater distances, increasing the vulnerabilities that come with movement such as abuses on public transport or attacks on mobile clinics, which often have less security than permanent locations. As a result, organizations operating in rural spaces are more likely to face security challenges than those in urban areas.

TABLE 2: ENVIRONMENTAL FACTORS AFFECTING THE SAFETY AND SECURITY OF HIV PROGRAMS IN LAC

FACTOR	EXPLANATION AND EXAMPLES
RELIGIOUS INTERPRETATIONS	While KP members may be perceived to break with religious teachings, there are many aspects of any health program that explicitly align with Islam and Christianity, the two major religions in the region. Media, government, and religious leaders' interpretations of religious teachings influence whether efforts to protect and meet the needs of KP members are perceived as acceptable by the broader society, which has ramifications for implementer safety.
HEALTH AND ECONOMIC CRISES	Health crises, such as COVID-19, and economic crises, such as high levels of unemployment or rapid depreciation of local currency, impact everyone's security, including the implementers of HIV programs for key populations. Curfews and lockdowns related to COVID-19 can result in harms to outreach teams seeking to distribute medication or services to individuals who cannot safely leave their homes, and efforts to prevent COVID-19 can be used as excuses to track or arrest individuals working with KP members. Large-scale economic desperation also leads to increases in theft and crimes that are not targeted at KP programs but may view them as wellresourced, especially if they receive international support. Mental health stress to implementers is also exacerbated in these contexts. Concerns about their own safety on the job are compounded by the ever-increasing needs of beneficiaries during a crisis (such as nutritional support), limitations on the ability of the project to act to meet these needs (such as decreases in funding or limitations on movement), and workers' own personal anxieties and struggles.
QUALITY OF SERVICES PROVIDED	Poor service quality—particularly mishandling of confidential information or failure to offer services that meet a minimum standard for cleanliness and professionalism—and outdated service delivery models increase the chances that an organization will come under attack and have no one to rise to their defense. Staying up to date with WHO recommendations on services offered and the way in which these services are implemented can help build beneficiary and power-holder support for programming. Conversely, high-quality service provision and positive results can be highlighted nationally and internationally. In some cases, this can reduce the likelihood of attack because the organization becomes recognized as making an important contribution to local health.

Several factors related to operations and management, although not specific to security, impact how safely an organization can operate **(Table 3)**. While not the focus of this toolkit, strengthening any one of these areas will

- Nature and Impact of Safety and Security Challenges

The desk review, scoping visits, and workshop identified a number of safety and security challenges that can occur within the implementation of HIV programs for and with key populations in LAC. These can affect individuals, organizations, and workplaces.

The collective result of these incidents is often a pervasive climate of fear that threatens the existence of organizations and makes it extremely difficult, sometimes impossible, for them to work effectively.

TABLA 3: INTERNAL FACTORS AFFECTING THE SAFETY AND SECURITY OF HIV PROGRAMS IN LAC

FACTOR	EXPLANATION AND EXAMPLES
ORGANIZATIONAL MANAGEMENT STRUCTURES	Strong organizational management is important to ensure the effective operation of programs. This includes the ability to manage funds appropriately—reducing the opportunity for fraud—and to train workers to prevent mistakes or abuses.
WORKPLACE STANDARDS	Workplace standards for occupational safety increase the positive perception of services offered (i.e., fewer people injured when receiving services) and increase workers' well-being (i.e., fewer workers injured and more confidence from workers in the organization's ability/desire to protect them). This should include standards related to fraud, sexual harassment, safeguarding, and a grievance process. Enforcing workplace standards for the qualifications of individuals allowed to perform tasks, such as HIV tests, also helps protect the reputation of the organization and ensure quality.
STAFF TURNOVER	Organizations with high levels of staff turnover struggle to standardize the way in which workers behave (e.g., it takes time to train staff on codes of conduct and official duties) and lose institutional memory that may have helped them avoid or mitigate future harms.

The case studies below provide a selection of examples of real-life safety and security challenges experienced by organizations operating KP programs in MENA. A more detailed set challenges and impacts is provided in **Annex A**.

- Case Studies: Safety and Security in HIV Programas for and with Key Population

- 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 organization 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 neighbors and had to cease operations for a time.

- 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 organization due to the stress.

- A CSO's website was hacked and online trolling campaigns were organized 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 cyber-security.

- Verbal abuse, theft, and sometimes physical attacks against program implementer staff, including clinicians, were reported at drop-in centers. 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.

Preventing, mitigating, or responding to safety and segurity challenges

- Strategies

HIV program implementers have diverse strategies for keeping themselves safe.

Not all strategies are right or necessary for everyone, particularly because the nature of HIV programming and the local context differs from one implementer to another. We have divided the safety and security strategies used by program implementers into seven domains.:

1.- Cultivating and sensitizing externals allies

Strategies in this category are designed to build coalitions that can protect the operation of an HIV program. For example, public collaboration with and official endorsements by national ministries, United Nations agencies, or local authorities and law enforcement can protect an organization's operations because that organization is clearly supported by state and international actors, limiting scrutiny or suspicion of their actions.

ILLUSTRATIVE DECISION POINTS

- Whether to become officially registered— Benefits of this approach may include government protection and access to state and some additional international resources; drawbacks include more government oversight of operations, potential delays as processes may take many years, and exposure if the organization previously operated discretely.

- Who to engage with—Consider the strengthof various organizations and individuals in your area, what each can offer, and the amount offunding and effort required to engage each successfully.

- Benefits of engaging with religious leaders include their ability to speak positively about the actions of an HIV program implementer or to ask the community to refrain from inciting violence against the HIV program implementer and/or its beneficiaries. Drawbacks include the potential for conflict if the organization is seen as favoring a religion or religious sect and excluding others and difficulty overcoming distrust among

- Benefits of engaging with law enforcement may include reductions in arrests of workers performing program activities or safer travel during outreach; drawbacks include time required to engage safely and effectively, which often must begin with high ranking officials; and high turnover of law enforcement staff, which may require continual training.

ILLUSTRATIVE DECISION POINTS

- Benefits of engaging universities include having their assistance in conducting research and studies, ensuring the quality of the results and increasing acceptance by government officials; drawbacks may include increased time for implementation and less control over the process and research design.

- Benefits of engaging with public figures, such as popular singers, actors, athletes, philanthropists, business owners, and other famous individuals, include their ability to decrease stigma against KP members among a wider audience; drawbacks include their need for training, such as an ability to speak consistently and accurately about health issues and scientific literature.

2.- Influencing public perception of the projec or organization

Strategies to positively influence public opinion can provide safety through visibility and community support. A project or program implementer that is well known and well perceived is less likely to be attacked than one that is unknown or negatively perceived, including because potential attackers understand that they cannot act with impunity. Some organizations cast a broad net in their programming, offering services to many communities—such as pregnant women and migrants—not only to KP members. In this way, an organization can demonstrate a clear value to its neighbors who are less likely to turn against the organization, even if they are not supportive of work with KP members.

ILLUSTRATIVE DECISION POINTS

- Deciding to work in a coalition, while it can strengthen alliances, also limits the organization's ability to focus on its own mission as pursuing collective goals can take time and energy away from the CSO's original area of focus.

3.- Documenting harms for tracking and advocacy

Many organizations working with vulnerable communities seek to record abuses in order to facilitate advocacy goals and reduce for attackers. Documentation can also allow clearer understanding of ongoing trends and may help predict crackdowns or unsafe areas for operation.

ILLUSTRATIVE DECISION POINTS

- Whether the organization has the capacity to assist those whose experiences of abuse they document is an important consideration. If the organization is only able to document abuses but not respond to them, or if the organization does not have resources to analyze data and use it for advocacy, this approach may cause harm because the individuals reporting harm will not receive direct support, such as psychological first aid.

- Whether the organization can safely store data is an important practical and ethical consideration. If the organization does not have that capacity, then collecting information on abuses could put individuals at risk for additional victimization.

- Whether the organization has an ability to use information gathered should also be considered. If information is collected but never used, there can be fatigue or disillusionment from those sharing their stories and their mental health can be impacted. In addition, reporting of abuses may begin to decrease, which could falsely suggest less violations.

4.- Protecting offices, drop - in centers, and other physical locations

These strategies are important to deploy if theprogram implementer has workers at a specific physical location, and particularly if beneficiaries also come to this location (e.g., a drop-in center or clinic). These protections include locks, cameras or closed-circuit television, layouts that involve multiple entrances/exits, and procedures to govern flow of and behavior by beneficiaries while on the premises.

ILLUSTRATIVE DECISION POINTS

- When using cameras, remember to weigh the dangers of recording beneficiaries of KP programs (especially in criminalized contexts), the willingness of beneficiaries to visit a space that includes cameras, and the safety of staff and property. Using a camera also necessitates developing a policy to guide the use and destruction of recordings in a way that limits breaches in confidentiality and conveying this policy in a transparent way to beneficiaries.

- Locating a clinic in a neighborhood with fewer security incidents can help staff and beneficiaries feel safe but may also mean it is less accessible to those who most need the services it provides. Considering transportation options and routes for workers and beneficiaries is an important part of the process.

5.- Keeping workers safe during physical and digital outreach

These strategies focus on outreach and are relevant to programs that conduct outreach in the physical and/or digital world. They include approaches such as finding and monitoring safe routes for outreach, preventing sexual harassment by beneficiaries in the field (especially when connections to beneficiaries are made through forums like dating applications), tracking workers, and training workers to interact with law enforcement and potentially aggressive beneficiaries.

ILLUSTRATIVE DECISION POINTS

- Hosting outreach online may be safer than inperson operations. However, digital surveillance is a serious consideration, as are safety concerns when transitioning clients from online to offline which involves in-person meeting of an individual who may only be known to the outreach worker through their online interactions (versus interacting with an individual that other beneficiaries bring to the program). In addition, in a context in which KP members are not all online, there is a risk of increasing the digital divide between individuals with more and less access to technology, such as smart phones.

- Talking about individual risks to KP implementers requires organizations to take steps to prevent the advice they give to promote safety from causing harm. In the past, some security trainings for peer educators have emphasized the need for them to minimize any signs that they are KP members. For example, workers may be told to dress and act more in line with gender norms to avoid calling attention to themselves. While this advice may be viewed as simply practical, it can violate individuals' rights to autonomy or seem to blame them for any attacks that occur by suggesting that their nonconforming behaviors are the issue. Such advice also does not consider the harms done to individuals forced to live in a way that is not true to themselves, which has psychological ramifications. Security trainings should be practical but should also pose questions to those being trained instead of being prescriptive, making it clear multiple factors should be weighed in determining how to stay safe and that it is not wrong to be true to oneself.

6.- Developing functional and institutionalized security protocols, including for emergencies

Almost all organizations have some activities in place to protect safety, even if it is as simple as talking to workers about following their intuition. However, when strategies are not institutionalized, they do not protect everyone equally, put the onus on the workers and not the organization, and are less sustainable. Furthermore, some responses to safety challenges—such as psychological support to workers—must be institutionalized to avoid harm to workers who may not otherwise get the support they need.

ILLUSTRATIVE DECISION POINTS

- Developing protocols or policies while maintaining flexibility to be responsive to the dynamic nature of safety issues is another area where intensive thought is required. Policies and protocols need to be adaptable and flexible. At the same time, they should be explicit enough to clearly indicate who has decision-making power (emergencies, in particular, require a common understanding of what should be done and who can determine these steps). As such, when developing policies, organizations should also plan for regular opportunities to revise and renew them. There should also be a mechanism for emergency review and revision during crisis situations, such as the COVID-19 pandemic, where many policies may need to be revised or new policies developed to account for new risks and realities.

7.- Keeping data and communications safe

HIV programs handle sensitive data on beneficiaries. Their materials and messages between workers may also be sensitive. Protections for data and secure forms of communication can prevent leaks that may lead to blackmail or other abuse, including physical harm to workers.

ILLUSTRATIVE DECISION POINTS

- The level of technology to employ varies. Some data protections are low-tech, such as keeping paper files in a locked cabinet. Others require encryption, cloud storage, software updates that necessitate some comfort with technology, and funds to purchase and continually update software and equipment. When determining which options are appropriate and feasible, consider both the sensitivity of the data the organization handles as well as the current and future resources and staff available to support digital safety. All digital safety should also include continual sensitization of workers to ensure they use technologies (especially new technologies) appropriately.

- Case Studies

Given that this tool is an adaptation of a version for the Middle East and North Africa (MENA) region, the case studies that are presented correspond to that region, and will be complemented by case studies from LAC región as they are secured. Brief case studies from the MENA region are provided in **Table 4** for illustrative purposes. They represent strategies that have been implemented in real life, have demonstrated positive outcomes, and have potential to be adapted or replicated. These case studies highlight the combined nature of safety and security strategies. Rarely is one strategy used in isolation.

TABLE 4: CASE STUDIES OF PROMISING PRACTICES

STRATEGY TYPE	EXAMPLE
INFLUENCING PUBLIC PERCEPTION OF THE PROJECT OR ORGANIZATION	**ALCS in Morocco** uses several techniques to ensure the public knows about and understands their important work. This includes a standard approach to sharing information among their staff/workers via regular sensitization so that all workers are prepared to describe ALCS' work in a consistent way, creating a newsletter that is circulated to the public and donors on their efforts to keep Morocco healthy, and engaging with well- known and respected local scientists in a public way. They also engage in efforts to ensure the media knows how to report on their work. This includes establishing trusted contacts within the media, always writing press releases to avoid being misquoted, and training members of media on who KP members are and how to talk about issues such as HIV. See Tool 3 for their media training tool and newsletter. **OPALS in Morocco** works with a broad group of beneficiaries on topics that go beyond HIV, in a public and accessible way, to demonstrate their value to society as a whole. Activities include public health quizzes, such as the OPALS AIDS Quiz, which help users of any population to understand their own level of knowledge and personal risks regarding HIV, STIs, and cervical cancer. The quiz also improves their knowledge of sexual and reproductive health, while at the same time familiarizing a wider audience with the issues facing various sub- groups, including members of key populations. OPALS also offers a wide range of health services based on the"self-care" approach such as prenatal care, to ensure that they meet the wider needs of key population members while meeting the needs of larger groups, such as pregnant women.

TABLE 4: CASE STUDIES OF PROMISING PRACTICES

STRATEGY TYPE	EXAMPLE
CULTIVATING AND SENSITIZING EXTERNAL ALLIES	**LebMASH in Lebanon** runs a competition each year for medical students called "Break the Silence: Willing to be Allies." In this competition medical students are encouraged to work more openly on peer-reviewed research papers pertaining to KP health. The winner receives a partnership with GLMA USA (Health Professionals Advancing LGBT Equality) and participates in the yearly GLMA conference to learn from fellow allies in the United States. The winner then returns to present to their fellow students and faculty. In some cases, the winner also receives media attention, normalizing and celebrating quality health care for KP members. **AIDS Algérie and El Hayet in Algeria** work in partnership with the government of Algeria to design and implement programs for KP members. These programs are co-designed with the Ministry of Health to meet the country's HIV-related targets, and activities receive explicit permission, including letters for outreach workers to carry stating their purpose. **APCS in Algeria** is inclusive and works with a broad range of stakeholders to keep their workers safe. They sensitize religious leaders, uniformed service members, elected officials, and other NGOs so that these groups understand the work of APCS and its strategic importance to the health of all Algerians. **Freedom Programme in Egypt**, conducts meetings to share facts about key populations with religious leaders. This includes introducing these leaders to the families of KP members (such as parents and children) to help them see KP members as part of society and as whole beings, not simply as "behaviors." As part of these efforts, religious leaders participated in developing the *Cairo Declaration of Religious Leaders in the Arab States in Response to the HIV/AIDS Epidemic* (an activity led by FHI 360). This document was signed by Muslim and Christian leaders across the region and described their commitment to realizing the value of each human being. See Tool 3 for the declaration.

TABLE 4: CASE STUDIES OF PROMISING PRACTICES

STRATEGY TYPE	EXAMPLE
PROTEGER OFICINAS, CENTROS DE ACOGIDA Y OTRAS INSTALACIONES FÍSICAS	**El Nour in Egypt** helps KP members feel safe at government-run facilities without sacrificing their own safety as implementers. They do this by sensitizing providers in the government facilities on key issues such as confidentiality and the importance of KP members to the HIV response to ensure that they respect the peers accompanying KP members to services. **An organization in Tunisia** works to ensure the mental health of their staff as part of their holistic approach to security at their drop-in centers. Beneficiaries at these centers experience a range of extreme stresses and can take out their frustration on the staff. As a result, the psychologist at the center works not only with the beneficiaries—thereby preventing outbursts toward staff—but also supports the service providers and reminds them that their mental health is an important asset to both themselves and the goals they are working toward. **DAMJ in Tunisia** works with allied realtors to review new locations for offices in order to find locations with fewer dangers from neighbors or landlords who may not be supportive of KP programming. **Bedayaa in Egypt** follows strict rules when welcoming new beneficiaries into HIV testing/counselling and referral systems. This is in order to ensure that no one who wishes to cause the organization or its beneficiaries harm is allowed on the premises. Potential clients submit an online application and must then be vouched for by an existing staff person or volunteer. If a new client is accepted, an appointment is arranged in a way that limits contact with others receiving services in order to protect confidentiality and avoid the gathering of groups. Finally, program participants receive instructions on appropriate behaviors before they visit the premises for the first time. This extensive process keeps beneficiaries, staff members, volunteers and consultants safe.
DOCUMENTING HARMS FOR TRACKING AND ADVOCACY	**AFE operating regionally** trains journalists and activists to report on attacks and rights abuses against KP members without sensationalism while highlighting their shared humanity and the harms to collective health and well-being that arise from anti-KP abuse.

TABLE 4: CASE STUDIES OF PROMISING PRACTICES

STRATEGY TYPE	EXAMPLE
KEEPING WORKERS SAFE DURING PHYSICAL AND DIGITAL OUTREACH	**SIDC in Lebanon** keeps their workers safe during outreach by adopting several complementary measures. First, the peer selection process ensures that chosen peer outreach workers can abide by the rules that govern outreach. Second, once hired, peers receive training to ensure that they understand the risks and limitations of their work. This includes training on what SIDC stands ready to do to support its workers should an incident occur—an important part of helping workers decide the level of risk they feel comfortable taking on. The training also builds peers' capacity to conduct outreach safely, covering topics such as nonviolent communication and how to interact with law enforcement safely. In addition, each peer is provided with an ID card that is signed by the National Aids Program, allowing peer outreach workers to clearly and quickly demonstrate that their work is endorsed by the government. **MENA Rosa in Lebanon** ensures that their focal points in the MENA Region have the self-esteem and information they need to speak to individuals from all different backgrounds. The training includes learning about different communication styles, network and advocacy, how to create strong relationships with key stakeholders, and the local legal context in which each focal point operates. **AMSED in Morocco** tracks outreach workers while they are in the field to ensure that if they experience security issues, the organization can intervene promptly. This includes using phones to track the GPS location of staff and regular check-ins via phone between managers and peer educators when outreach begins and ends. **ANISS in Algeria** works with their outreach staff to ensure they feel safe during activities by planning routes with the staff and allowing them to decide on the number of commodities they will carry with them. **ATP+ in Tunisia** provides counseling to peers who are harassed during outreach or who experience abuse from their families because of their participation in the key population program. Counseling focuses on mitigating the psychological harm of the abuse and helping the peer prevent or avoid further abusive situations.
DEVELOPING FUNCTIONAL AND INSTITUTIONALIZED SECURITY PROTOCOLS, INCLUDING FOR EMERGENCIES	**M-Coalition members in Tunisia** successfully applied to the international coalition of Dignity for All for funds to address a pattern of robberies affecting their organization. The funds were able to cover improved physical security measures. **ALCS in Morocco** institutionalized expectations for appropriate staff behavior via a code of ethics that all workers must sign when they begin to work with the organization. This code prevents abuse of beneficiaries or inappropriate behavior by staff that could lead to a security incident. It includes charters on confidentiality, anonymity, and appropriate data management. To ensure the code is taken seriously, it is in the contract of each person joining the organization and is revisited during all large organizational meetings.

TABLE 4: CASE STUDIES OF PROMISING PRACTICES

STRATEGY TYPE	EXAMPLE
KEEPING DATA AND COMMUNICATIONS SAFE	**FHI 360 in Egypt** instituted unique identifier codes (UIC) codes to ensure that data on KP members could not be used to identify individuals. All those handling data were asked to sign a code of ethics and immediate action was taken if a breach in data safety occurred, including retraining workers as appropriate.
CROSSCUTTING: DIGITAL SAFETYL	**AFE** along with others organizations in the MENA region, are part of a Facebook advisory board. Via this mechanism, organizations can provide information directly to Facebook administrators about individuals or pages inciting violence against KP members in the MENA region.
CROSSCUTTING: COVID-19	**Caritas in Egypt** has begun virtual support groups for implementers of KP programs to help them manage the COVID-19 crisis. These support groups meet by using ZOOM Cloud meetings in addition to psychological support through helpline to share accurate information about the virus while helping workers sort through their own fears and anxieties as well as those of their beneficiaries.

Recommendations to inform the response to safety and security challenges

The review, scoping visits, and security workshop also led to the development of broad recommendations to help inform current and future programming for and with key populations in LAC to improve security issues:

Not all strategies are right or necessary for everyone, mainly because the nature of HIV programs and local contexts differ from one implementer to another. Here, the security strategies used by program implementers have been divided into seven areas:

1.- Make HIV Program principles and approaches the Foundation of Security efforts.

Responses to safety and security should follow the same good practice principles and approaches as other aspects of HIV programming. Examples include:

- **Do no harm**. Prioritizing the well-being of program implementers and ensuring that actions do not make situations worse, especially for those who have already been harmed, in either the short- or long-term.

- **Nothing about us, without us**. ensuring that security efforts are informed and led by program implementers themselves, including KP members who implement programs

- **Rights-based approach.** ensuring the rights and dignity of program implementers are protected and respected and responses do not, for example, require them to stop being true to themselves in order to stay safe

- **Country-led/owned approach. ensuring that decisions are made by local/national organizations (where appropriate and useful, supported by regional and international stakeholders).**

2.- Make Security a priority and resource it explicitly.

Safety and security in KP programs should never be assumed or left to chance. Ideally, it should be contemplated from the proposal stage of a project. In the risk assessment portion of the proposal, the applicant should identify priority risks while the proposal itself details activities to respond to these risks. **Annex A** offers examples of security challenges that organizations can review and use as they consider their own risks.

BUDGETING FOR SECURITY

Upfront investment in planning and prevention is significantly easier and more cost-effective than having to take reactive measures (such as relocating an office). Setting aside funds to support outreach workers or others who experience harm, for example, to cover hospital fees in case of violence, allows for immediate action when a crisis occurs and demonstrates to workers that an organization is committed to their well-being.

Safety and security safeguards should be an organizational priority and an essential component of all HIV programming for and with KP members. As such, security activities should have specific budget line items **(Budgeting for Security)**. Such safeguards are not a luxury or added extra, but a necessity. When activities to promote safety are not explicitly included in donor requests for proposals, it is important to lobby for their inclusion in budgets and work plans. The Inclusion of security in budgets supports the recommendations of normative guideline such as the World Health Organization Key Populations Implementation Tools that prevention of and action in response to violence against key populations memvers is critical enable of effective responses to HIV[17, 18, 19, 20, 21].

3.- Make a safe workplace the employer´s responsability.

Many gaps must be addressed to ensure a safe and secure environment for KP program implementers, whether at established offices and clinics or in the field. Many donors do not fund safety and security activities in their HIV programming and, in some cases, organizations seeking to provide employees with insurance also find that local structures— such as policy plans available—do not meet their needs. The result too often is that workers are left responsible for their personal safety and security.

However, global standards require that employers bear and fulfill an ethical duty of care to ensuring the safety and security of their employees (e.g., guidelines provided by the International Labour Organization)[22]. In the case of CSOs where resources are limited, donors need to be stronger advocates for safety and security in programming and provide a means for implementing organizations to budget and plan for safety and security so that they can uphold their duty of care to their employees. Holding up successful and responsible organizations as positive examples can not only give them the accolades they deserve, but also influence the field.

TABLE 5. ASSESSING THREATS AND LIMITING AN ATTACKER'S ABILITY TO ACT

A systematic approach to **assessing threats** [23] includes asking the following questions:

1. What are the facts surrounding the threat?
2. Is there a series of threats that became more systematic or frequent over time?
3. Who is the person who is making the threats?
4. What is the objective of the threat?
5. Do you think the threat is serious?

Threats can be countered by considering and removing (when possible) **what an attacker needs** [24] to carry out an act of violence.

- **Acces**: to the potential victim/organization physically or virtually
- **Resources**: anything that can be used to carry out the attack— information on the victim's location or weaknesses; weapon, transport, money, etc.
- **Impunity**: legal and/or social
- **Motive**:reason to act

4.- Plan ahead and make sure that everyone knows the plan (while maintaining flexibility).

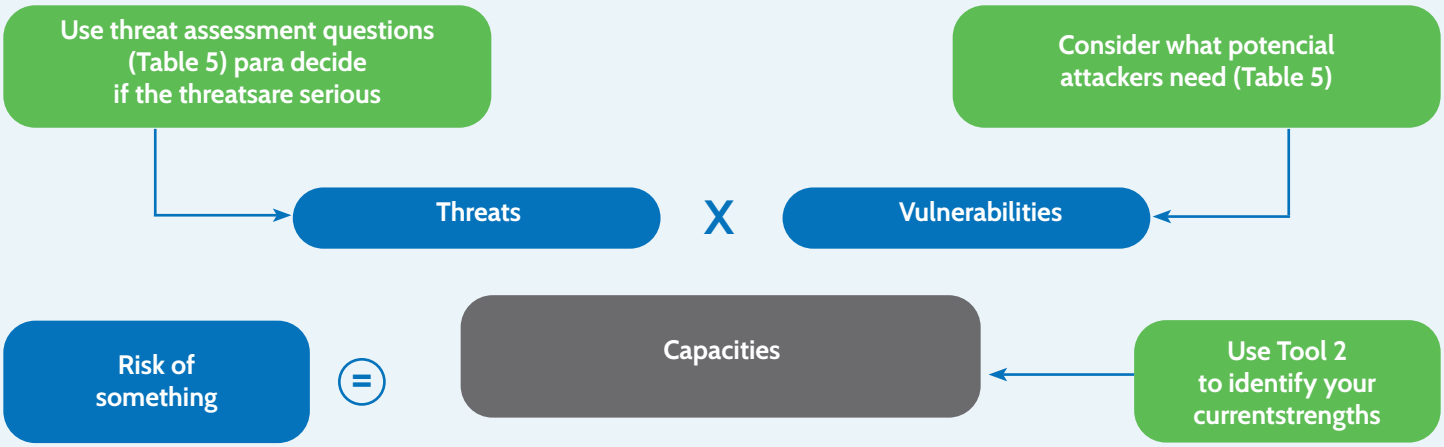
Prevention and response measures for safety and security should be carefully identified and mapped out within an organizational security plan that is developed, known, and owned by the whole organization or institution. The plan should be rationalized, systematic, and informed by evidence in the relevant local context. It should identify critical threats and risks to safety and security and provide a clear, step-by-step guide for what actions should be taken, by whom, and when. A successful plan complements the emergency plans of key partners, such as key-population-friendly HIV clinics.

The plan should also be responsive to which threats are most serious and include actions designed to limit the ability of an attacker to carry out violence. See **Table 5** for more on assessing the seriousness of a threat and identifying the resources that an attacker needs to perpetrate abuse.

Finally, a good security plan requires systematically deciding which specific threats are the priority by identifying which carry the most risk to the organization (e.g., not only those that are serious but also will have the largest impact). Since it will not be possible to take all desired steps to improve security at one time, respond to the most pressing safety and security challenges first.

See **Figure 3** for a formula to identify the priority security challenges by determining the risk of specific harmful outcomes that the organization believes may occur. It includes an example.

FIGURE 3: FORMULA TO DETERMINE RISK THAT A SPECIFIC HARM WILL OCCUR



EXAMPLE	
Pick a specific risk (location, activity, person):	Our CSO is worried that our outreach workers will be physically assaulted during outreach to bars.
Consider threats that make the risk more or less likely:	Verbal abuse, including threats of physical violence, have occurred since the project began and have recently increased (systematic/frequent); the perpetrators are often the bar owners (who is making the threat) who do not want outreach to occur in their businesses (objective).
Name your vulnerabilities:	Outreach is done by sex workers who are seen as unlikely to report abuse (impunity for perpetrators); outreach occurs at night on a regular basis (resources—their location is known); transport is on foot (access to carry out an attack); bar owners do not want the outreach workers to encourage sex workers to use condoms because they believe clients will pay less (motive).
Name your capacities:	Peer outreach workers wear ID cards that show they are connected to the Ministry of Health and include a phone number to reach a locally trained police officer; peers go out in pairs; peers have phones with pre-paid airtime in case they encounter issues; peers have a noncontroversial message to describe their work; peers whereabouts are tracked via logbook and GPS; peers have safe havens in each neighborhood they work in because they are known and respected by other sex workers.
Decide what to do:	Given all of these factors, decide whether the capacities to prevent the harm from occurring are sufficient to outweigh the threats and vulnerabilities. If not, develop a security plan that will help you to decrease vulnerabilities (when possible) and increase capacities. For example, the program may decide to begin sensitizing bar owners to decrease their abusive behaviors or it may decide to relocate outreach activities to other places sex workers gather.

5.- Explicitly discuss the level of risk that is acceptable organizationally and individually.

Activities to improve safety and security should be based on an appreciation that every individual, organization, and program has a different level of comfort with and tolerance of risk. An organization's security plan should not, for example, be based solely on the risk appetite of the director, who may, personally, be more used to or prepared to face threats. Realistically, in hostile environments, it is likely that all work with key populations will be associated with some degree of risk. However, no one should feel forced to take risks they are uncomfortable with. All workers should have— preferably before a security incident occurs— the opportunity to think through and articulate what they, personally, are comfortable doing. Examples of options include accepting the level of risk, reducing the level of risk, sharing the risk, or avoiding the risk[25]. Once the individual levels of risk appetite are understood, individuals and their organizations can make informed decisions about how to respond to actual risks that are identified.

When environments change, risks change as well. This means conversations should be ongoing about identifying risks, discussing acceptable levels of risk, and helping workers understand what the organization will do to help mitigate risks. For example, during COVID-19, the risk of participating in outreach efforts changed dramatically. Individuals who were more likely to have severe complications from infection—such as those with underlying health conditions—were now at greater risk during outreach then those without underlying health conditions. As these risks were new, it was important for organizations to help workers assess their own risks and then decide how much risk they felt comfortable taking on, ideally with support from their organizations to be assigned to other tasks if in-person outreach was deemed too risky.

6.- Operate with a knowledge of both the actual risks and their underlying causes (including legal frameworks).

Responses to safety and security incidents need to be informed not only by the immediate causes (the trigger) but the longer-term influencing factors (the root causes). Equally, responses must be tailored to the specific context—cultural, political, legal, etc.—in which challenges occur. As discussed in the Illustrative Decision Points in Section 3 of Tool 1, something may be feasible and effective in one context (e.g., dialogue with the police) while it causes harm in another.

An important component of understanding the risks and their causes is a review of the legal framework in a country to determine what activities, if any, may come under scrutiny from law enforcement and to understand and be able to articulate your rights as a program implementer. This information should be shared broadly with workers who also receive capacity building on how to articulate these rights to local authorities or others who may have questions about their activities.

7.- Acknowledge the different vulnerabilities and capacities of each worker in security planning.

Safety and security responses must be based on a constant mindfulness that staff and volunteers for HIV programs who are themselves members of KPs face double vulnerability in both their professional and personal lives. This is also the case for individuals living with HIV and those who are undocumented or part of refugee communities. All the individuals working in KP programs have distinct vulnerabilities and capacities that should be taken into account instead of using a one-size-fits- all approach. It is especially important to consider issues related to:

- **Gender**. For example, in some contexts, staff members who are cis female [26], transgender, or cis male with more feminine gender expressions may be especially vulnerable to GBV within the implementation of HIV programs and, in turn, may need more and/or different prevention and response measures compared to other colleagues. Power dynamics within organizations can also be affected by gender and specific attention should be paid to ensuring a workplace free of sexual harassment.

26 Cisgender refers to individuals whose gender identity aligns to their sex assigned at birth. A person who sees herself as a woman and who was assigned female at birth is a cis female.

- **Age**. For example, there may be power dynamics within the organization that favor older or younger workers. A worker's age is also likely to impact threats they experience during outreach; younger workers experience greater surveillance by police in some settings, especially during periods of political upheaval.

- **Different groups and subgroups of key populations**.

  There are issues to consider:

  - **Between key populations**. For example, staff members working with specific key populations (such as people who inject drugs) will need safety and security responses tailored to concerns relating to overdose, drug interaction, and safe injecting practices. Also, some key populations may face unique challenges within responses to incidents (for example, transgender people may lack official documentation and be unable to lodge an official complaint).

  - **Within KP programs**. For example, safety issues may be different when doing outreach with men who have sex with me at hotspots, in residences, or online.

  - **Multiple vulnerabilities**. For example, workers that support individuals who belong to more than one KP group may be vulnerable to multiple safety and security challenges and require a unique set of responses. For instance, workers who serve sex workers who inject drugs may need to carry a range of commodities (syringes, condoms, etc.) that might heighten their risk of arrest and detention.

- **Different legal status**. This includes considerations for individuals who may be in a country without legal documentation or those with criminal records who may face tougher penalties if they interact with the judicial system.

8.- Get to know all stakeholders, not just obvious allies.

It is critical to try to reach out to the individuals and institutions that either directly or indirectly lay behind safety and security challenges. This may involve building relationships with stakeholder groups such as law enforcement, religious leaders, and community leaders. Such partnerships may take time and require significant patience but can bring important rewards. For example, when such stakeholders become members, rather than opponents, of local emergency response teams. Taking time to make personal connections and learn from other groups working with different communities is a useful tactic.

9.- Identify both threats (physical, digital and psychological) and security strategies holistically.

Safety and security challenges in KP communities and HIV programs are rarely one-dimensional. They also change over time. As such, responses need to be:

- **Holistic**: addressing physical, psychosocial, and digital safety and security, as suggested by the Tactical Technology Collective [**see Figure 4**][27]. Responses should involve both inward-facing initiatives (e.g., developing and communicating an emergency plan) and outward-facing initiatives (e.g., building relations with local stakeholders).
- **Comprehensive**: using a multilevel and multifaceted approach [**see Figure 5**][28].
- **Flexible**: having the potential to modify plans and adapt quickly and effectively, such as in response to a sudden change in the security environment.

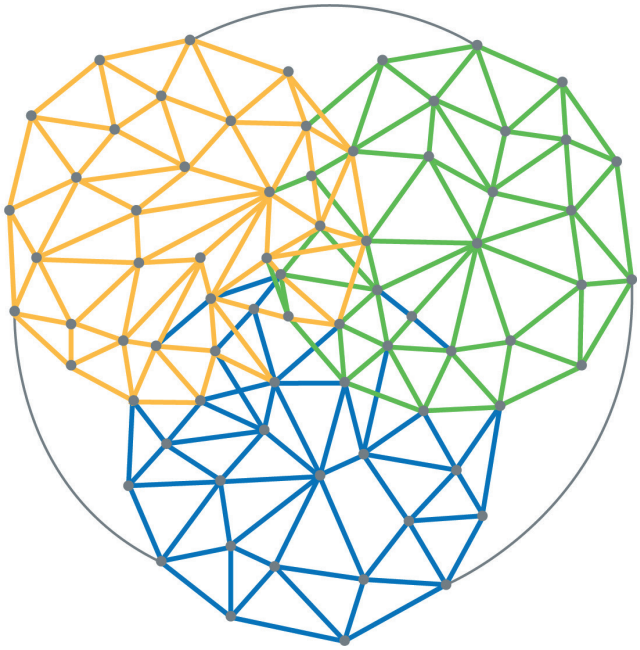
FIGURE 4: A HOLISTIC APPROACH TO SAFETY AND SECURITY

PHYSICAL SECURITY
Threats to our physical integrity.
Threats to our homes, buildings, vehicles.

PSYCHO-SOCIAL SECURITY
Threats to our psychological well-being.

DIGITAL SECURITY
Threats to our information, comunication and equipment.

— Holistic security analysis, strategies and tactics.

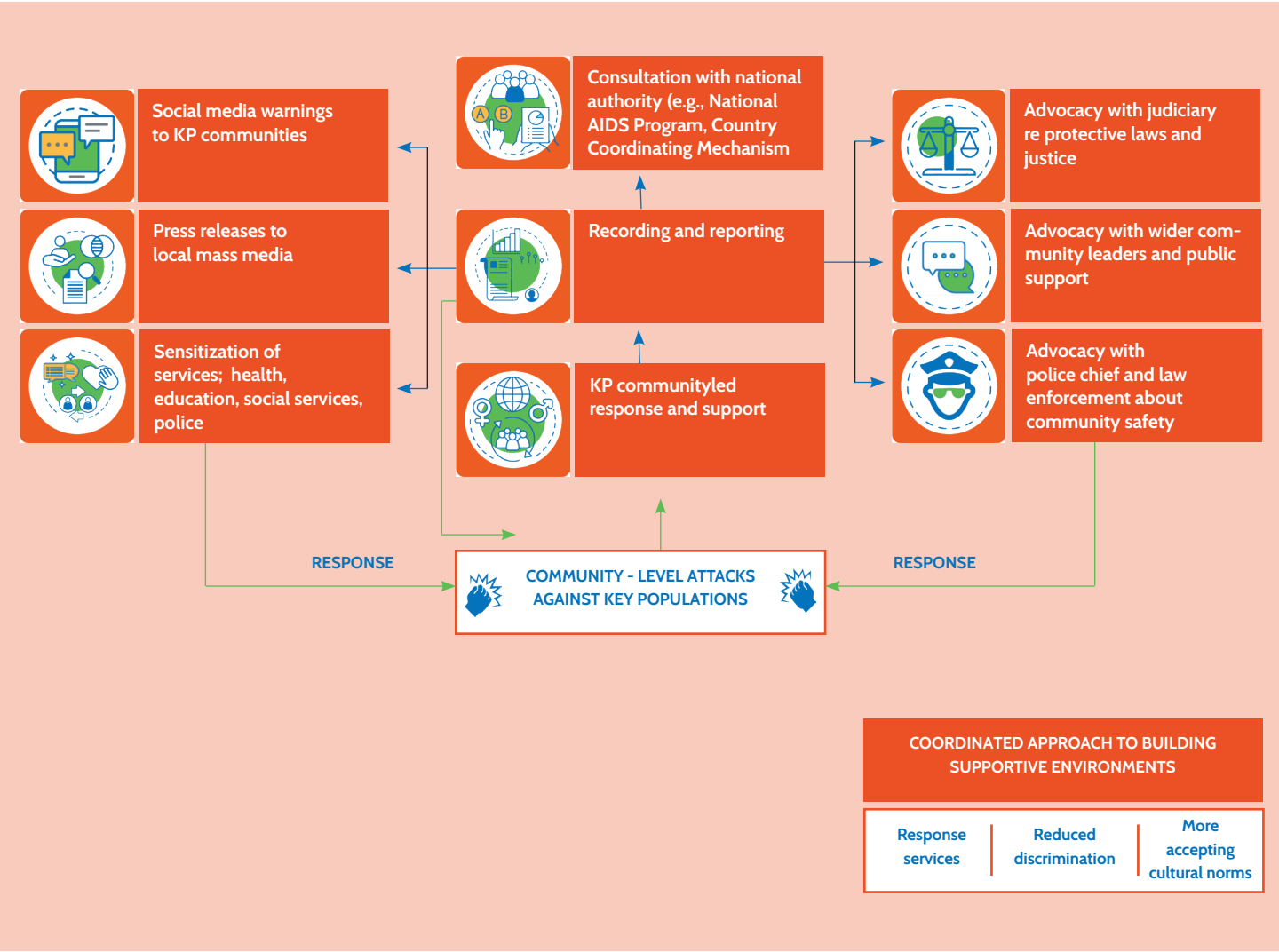


Source: Tactical Technology Collective. Holistic Security: A Strategy Manual for Human Rights Defenders. Berlin: Tactical Technology Collective; 2016.

10.- Be together, work in colalition, and learn from one another

Be aware of safety and security as a collective. While each KP program or implementing organization has distinct safety and security challenges, overlaps exist. Sharing challenges, successes, and questions provides an opportunity to learn from and reflect critically on experiences, strategies, and resources that can then be leveraged to strengthen safety and security responses.

FIGURE 5: A COMPREHENSIVE APPOACH TO VIOLENCE WITHIN PROGRAMS[29]



29 Source: United Nations Development Programme (UNDP), IRGT: A Global Network of Transgender Women and HIV, United Nations Population Fund, UCSF Center for Excellence for Transgender Health, Johns Hopkins Bloomberg School of Public Health, World Health Organization, Joint United Nations Programme on HIV/ AIDS, U.S. Agency for International Development. Implementing Comprehensive HIV and STI Programs with Transgender People: Practical Guidance for Collaborative Interventions. New York: UNDP; 2016.

TOOL 2

CHECKLIST OF SAFETY AND SECURITY STRATEGIES

· Purpose and Content

This tool explains how to use a practical checklist, which is provided, to help program implementers systematically explore and make plans to respond to their safety and security needs. It includes questions about strategies under seven areas of safety and security —described in more detail under **Section 3 of Tool 1**—as well as cross-cutting questions on emergency preparedness, digital security, and COVID-19.

How to use the checklist

Identifying needs and opportunities in advance

Completing the checklist

Considerations throughout the process

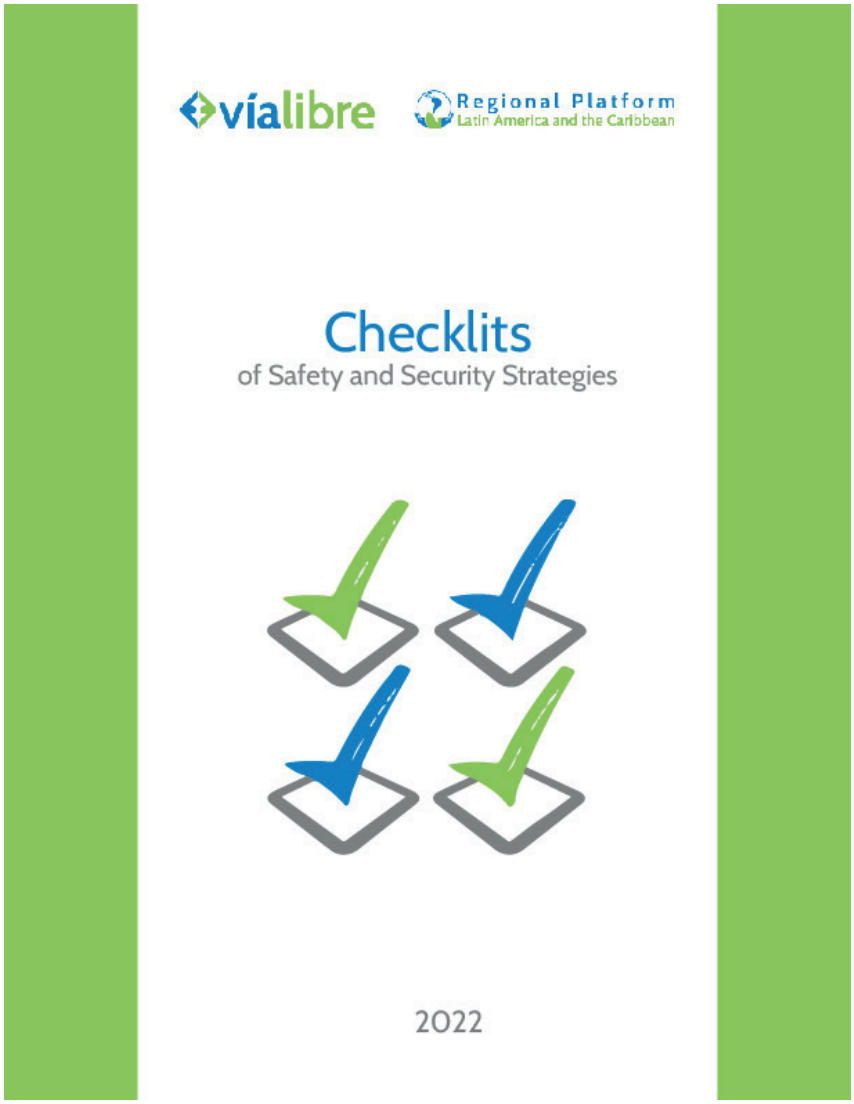
Scenarios to test existing responses to safety and security

TOOL 2

How to use the checklist

This user-friendly checklist poses straightforward questions to support you in planning and implementing actions to improve your safety as you work on HIV programming for key populations.

The tool is designed to complement, not replace, organizations more detailed strategies and polices on areas such as security, human resources, risk management, and protection to ensure the full range of safety and security issues is addressed.



TOOL 2

Identifying needs and opportunities in advance

Conducting a safety and security needs assessment before implementing **Tool 2** may be useful. Such an assessment could involve hiring an expert to help identify and then brief your organization on the pressing safety concerns that pose a risk for your program or staff.

The assessment may include a review of relevant details of the criminal law and examples of how others implementing programs have responded to those laws, contact information of local allies within the police and other law enforcement agencies who may be able to assist your group, any hot spots where the prevailing social attitudes are particularly hostile and might jeopardize outreach, and a mapping of recent violence in your area that could be linked to threats to your program or organization. However, a needs assessment is not required, and organizations may already be aware of their main risks and potential allies based on their years implementing programs or their active monitoring of security incidents.

Completing the checklist

Key workers involved in reviewing the checklist and implementing activities in response to identified gaps are the members of a safety and security management team. If no such team exists, the first step in this process is to form one (see box titled **Safety and security management team).**

Once the team is formed, you should collectively agree on when you will use the checklist. The checklist can be used regularly as part of routine safety and security planning in your organization or program. For example, you could review the checklist every six months at a meeting of the safety and security management team. It may also be used when a specific safety and security incident occurs or begins to happen more frequently to help you systematically think about options for mitigating future harms.

Whenever the checklist is used, it should be completed in a safe and private space where it is possible to speak openly. Because Tool 2 is designed to inform policies and procedures governing activities wherever program design, implementation, and monitoring occurs, the safety and security team should visit those sites or speak to representatives from those sites to better understand the unique challenges and needs in different settings. When completing the checklist, refer to each section heading to determine what type of organization should complete this portion.

SAFETY AND SECURITY MANAGEMENT TEAM

MEMBERS

The size and composition of this team will vary depending on the size of your organization. Each organization should identify a **safety and security focal point**—someone who coordinates the organizational response, who has been trained in safety and security, and who sensitizes and updates colleagues on internal safety and security policies. Ideally, the safety and security management team should include:

- Safety and security focal point
- One person from senior management (or an individual with decision-making power)
- One or two staff members from different levels in the organization
- Someone with information technology expertise if digital security will be discussed

RESPONSIBILITIES

Beyond the completion of the checklist, the duties of the safety and security management team should include making strategic decisions about, developing procedures for, and coordinating the implementation of safety securitypolicies.

For all those completing the various sections of the checklist, please read each question, After each question put a "X" under either yes or not to indicate the response that best aligns with your organization's reality.

- **Yes**: This answer indicates that the organization routinely implements this strategy. For example, under question 1. "Does the organization take actions to be visible to the public, portraying a positive image?" if the organization has a continued campaign to be visible in a positive way, they would put a "X" under "yes."

- **No**: This answer indicates that the organization has never engaged in this strategy and does not currently implement it. For example, under question 1. "Does the organization take actions to be visible to the public, portraying a positive image?" if the organization has never conducted activities to have positive public visibility, they would put a "X"under "no."

In the column following the yes / not responses there is room for the person(s) completing the survey to explain their answer under "notes."

See Notes for more.

NOTES:

While it is not required that an organization fill out the "notes" column after each question, filling it out will help make decisions on next steps, particularly if you select "somewhat" as a response and wish to provide details explaining your choice.

Considerations throughout the process: Communication, confidentiality, and review

It is important that the safety and security management team communicates consistently with and has opportunities to receive feedback and questions from other workers at the organization.

While the team's communication is not limited to this activity, in regards to **Tool 2**, the team should share the results from completing the checklist, next steps to address gaps, and any updated information—such as changes to emergency procedures or contact information for the safety and security focal point—as it becomes available.

When communicating with others working within the program or to external audiences about cases of violence—including when using this information to complete the checklist—respect confidentiality by keeping identifying information as private as possible. The principle of "do no harm" should be at the center of (1) all decisions regarding what, how much, and with whom information about specific incidents should be shared and (2) the actions taken both when completing the checklist and whenever supporting victims of violence.

As with any tool, the checklist's usefulness will be determined by how it is used. Each time the safety and security management team uses the checklist, consider including time to discuss the tool itself. Update and revise as needed to best fit your needs and your local context.

TOOL 2

Scenarios to test existing responses to safety and security

After completing the checklist, which only allows you to respond with "yes," and "no," you may find it useful to talk through the scenarios below to determine in a more practical and applied way whether the policies and procedures you have in place are sufficient to manage each of these cases.

You may also want to add your own scenarios for discussion, based on what has been happening in and around your community.

Your answers to these scenarios can also help you think concretely about content to include in any new safety and security policies and procedures that the checklist helped you determine are needed.

Ask yourselves "What would we do as an organization if...?" in each of the following examples. See Annex B for example solutions after you have brainstormed your own. There are no one right answers. Each will depend on your context.

1. The local safety and security situation suddenly gets much worse, with daily reports of verbal/physical abuse against KP beneficiaries involved in our HIV program.
2. We need to use the program budget to address urgent safety and security needs (e.g., security for the office, software to protect online files), but if we do, we won't have sufficient funding to meet our original targets.
3. A worker reports that he or she has been harassed by another worker.
4. An outreach worker is arrested while distributing condoms and is being held by police.
5. After an HIV outreach activity among a KP community, a beneficiary posts photos of the outreach workers and community members on Facebook and tags them.
6. The office is raided by the police and they take all the files and computers.
7. A hostile article about your organization is printed in the newspaper; it gives the address of your clinic and includes photographs of two of your clinicians.
8. A peer outreach worker at your organization is blackmailed by a beneficiary who threatens to tell the worker's parents that the worker is gay.

Develop your own scenario, based on the primary concerns in your context.

vialibre

Regional Platform
Latin America and the Caribbean

Checklits

of Safety and Security Strategies

2022

TOOL 2

Checklist of Safety and Security Strategies

One of the greatest vulnerability factors associated with HIV is stigma and discrimination against the disease and against the main key populations: people living with HIV (PLWH), men who have sex with men (MSM), people who inject drugs (PWID), female sex workers (FSW), transgender people (TP) and, more recently, irregular migrant population. As in other regions of the world, community leaders working on issues related to HIV and the defense and promotion of human rights in Latin America and the Caribbean (LAC) are exposed to risks and threats associated with the activities carried out with these key populations.

In 2018, the former International HIV/AIDS Alliance (IHAA) (currently known as Frontline AIDS), a member of the Technical Advisory Group on Violence, Stigma, and Discrimination Against Key Populations, for the USAID LINKAGES Project, created the Safety and Security Toolkit: Strengthening the Implementation of HIV Programs for and with Key Populations. This toolkit was developed to help program implementers, particularly community-based organization (CBOs) and others working in direct service delivery, to more effectively address safety and security challenges within their implementation of HIV programs. It was designed for use in hostile environments; for example, where members of key populations are criminalized and face elevated levels of stigma, discrimination, and violence. It seeks to amplify good programming through identifying and cataloging promising practices and tools, making overarching recommendations to address safety and security challenges, and providing a systematic approach to identify and respond to one's own safety and security gaps.

Both the Community, Rights and Gender Strategic Initiative (CRG SI) of the Global Fund, and the Latin America and the Caribbean Regional Platform/Vía Libre consider it of vital importance to have a similar tool adapted to LAC, given the risks that leaders, outreach workers, programme people, service providers and community mobilizers face in their work with key populations in these countries. For that reason, this proposal intends to adapt the tools described above to the regional context of community outreach. This assessment tool is designed as a first approach to determine the security and outreach related issues of CSOs and communities working on HIV, as well as to identify the potential risks they face in the course of their activities. The results of this preliminary evaluation will serve as an input for the adaptation of the toolbox both to the Latin American context and to the safety and security needs of their leaders and organizations.

This tool consists of three sections: general information; a set of checklists intended to help organizations and individuals to make plans for responding to their safety and security needs; and a segment dedicated to the characterization of safety and security risks.

TOOL 2

Checklist for assessing risks and needs related to the safety and security of organizations and people working with HIV

This checklist intends to be a first approach to assessing the safety and security of people and organizations working with HIV, and identifying the potential risks when carrying out their activities. The results derived from this assessment will serve as input for developing plans, policies, and programs to improve the safety and security of people and organizations working with key populations in LAC.

The tool has 71 questions divided into six sections, as described below:

1. **General information:** This section includes questions aimed to characterize organizations, their geographic location, populations with which they work, populations to which their members belong, and the kind of activities they carry out.

2. **Checklist for organizations:** This includes questions to verify general safety and security aspects. The setting here is related to the organization, understood as groups of people working for a common cause.

3. **Checklist for individuals:** It focuses on individuals and includes questions to review the needs and response capabilities to situations of vulnerability from the point of view of all the organization members, both volunteers and hired personnel.

4. **Checklist for workplaces:** The setting here is comprised of physical spaces. This section includes questions related to their needs, threats, and vulnerabilities.

5. **Survey on risks and situations to which leaders, outreach workers, programme people, and service providers of CSOs working on HIV are exposed:** This includes questions on the identified types of risks that staff face at the physical, psychological, and virtual levels. It also assesses risk perception.

6. **Survey on risks and situations to which organizations working on HIV are exposed:** It includes questions on the type of risks identified in organizations.

The answers to these questions will help identify the settings and the response stages (prevention, immediate response, and long-term response) which require fulfilling safety and security needs.

How to use the checklist for risk and needs assessment?

This checklist intends to be user-friendly. These simple (yet numerous) questions will help plan and execute actions to improve safety and security while implementing HIV programs for and with key populations.

The tool aims to analyze and generate information to assist in elaborating projects, programs, or institutional policies that improve the safety and security of individuals and organizations. The checklist development does not replace actions to mitigate risks or respond to safety and security situations.

Filling out the checklist

The key workers involved in applying the checklists and implementing activities in response to identified breaches should be members of a safety and security management team. If no such group exists, the first step in this process should be to create one (**Figure 6**)

Figure 6: Safety and security management team

Members
The scale and composition of this team may vary depending on the organization's size.

Each organization should appoint a safety and security focal point: a person who coordinates the organization's response, has received safety and security training, and updates colleagues on internal safety and security policies.

Ideally, the safety and security management team should include:

- A safety and security focal point
- One member from senior management
- One or two employees or volunteers from different levels in the organization

Responsibilities
In addition to filling out the checklist, the safety and security management team's duties should include making strategic decisions, developing procedures, and coordinating the implementation of safety and security policies.

After appointing the team, members should agree upon the periodicity of use of this tool. It can be employed regularly as part of the organization's routine safety and security planning (for instance, the checklist could be applied every six months at a safety and security management team meeting). When a specific safety and security incident occurs, it can also be used to help the organization think systematically about options for mitigating future damage.

Participants should fill out checklists in a safe and secure space where open discussion is possible. This tool aims to identify potential needs and risks at all sites where HIV-related program activities occur. For that reason, the security team should visit those sites to understand better the unique needs in different environments.

If possible, use an online survey form: this will facilitate systematizing the information into a database. Generate graphs with each of the questions.

Analysis of the checklist results

To interpret the data, consider the different settings, i.e., each of the sections of the tool. Also, try to place the result in a response stage: "We lack something like this in the prevention stage / the immediate response stage / the long term stage."

Share the results with the organization members and generate discussion processes to improve the interpretation of the results. At the same time, try to raise awareness of the importance of developing individual and organizational actions regarding these issues.

Use the results to generate actions that reduce the vulnerability of individuals and organizations to safety and security-related risks. If any victim of a violent act comes to light during the process, offer immediate help.

Considerations throughout the process: communication, confidentiality, and review

The safety and security management team should be in constant two-way communication with the organization members. They should share the results of the checklist application, the following steps to address identified gaps, and any other information updates as they become available—such as modifications to emergency procedures or changes to the safety and security focal point contact information.

Ensure confidentiality when communicating with people in the organization or external audiences about security incidents (including checklists applications). The principle of "do no harm" should be at the heart of all decisions regarding what, how much, and with whom the team should share information about specific incidents. This principle also applies to filling out checklists and offering support to victims.

The utility of the checklist is determined by how it is employed. Each time the security management team applies one, analyze the tool itself beforehand. Update and revise as necessary to best fit your needs and local context. After a specific incident or breach of safety occurs, review the tool to see how to strengthen it to help prevent or respond to a similar incident in the future. The safety and security focal point can lead these activities.

1. General information

1 Name of organization:

2 Do you belong to any of the following key populations?

PLWH MSM PW FSW PWID Others

3 What is your position in the organization?

4 City:

5 Country:

6 What activities does your organization carry out in response to HIV?

Advocacy Prevention Care

Political lobbying Others

7 What populations does your organization work with?

PLWH MSM PW FWS PWID Others

which ?

2. Checklist for organizations

"Organizations" refers to groups of people who are working together for a common cause. This checklist is useful for organizations that are formally registered as well as those that are considering registration and/or are operating as informal networks.

	Do we have the following in place?	Yes	No
8	Systems for workers to document the details of safety and security incidents that occur (e.g., through log books and a database)		
9	Clear referral pathways for health services (e.g., for injuries, for psychosocial counseling/support, for any other medical needs) after a safety or security breach has occurred?		
10	A designated spokesperson prepared to speak to the media who is known by other workers who can refer to him/her?		
11	A clear pathway for communicating with regional and international stakeholders to keep them informed about safety and security challenges and request their support if/when desired		
12	Please add any additional points you consider relevant		

3. Checklist for individuals

"Individuals" refers to workers or members, for whom an organization has a duty of care to protect their safety and security. While policies and procedures should also provide for the safety and security of clients or service users when visiting or engaging with an organization, these are beyond the scope of this checklist.

	Do we have the following in place?	Yes	No
13	Guidelines for specific types of workers – such as outreach workers and peer educators – outlining their roles and responsibilities and sources of support in relation to safety and security?		
14	Training for workers (e.g., covering first aid and nonaggressive communication) to support them to prepare for and respond to safety and security challenges		
15	A range of support for workers (e.g., counseling, workers' meetings) to enable them to share their experiences, concerns, and ideas about safety and security		
16	A consistent and noncontroversial message for all workers to use to explain their work (e.g., to the police or community leaders)		
17	A system to ensure that there are safe routes for all workers to the office and outreach activities		
18	Communication systems for workers to keep in touch on an on-going basis (e.g., through a WhatsApp group) and in an emergency (e.g., through a phone tree)		
19	Protocols for managers to track workers (e.g., addressing how regularly to check in and confirm return from an activity)?		
20	Up-to-date lists of friendly contacts (e.g., among the police, public health professionals, and community leaders) who can provide support in an emergency?		
21	Safe havens identified (e.g., in communities where outreach occurs) where workers can go in case of threat?		
22	Information materials (e.g., ID cards and "know your rights" cards) to support workers?		

4. Checklist for Workplaces

A "workplace" is a physical location, including places such as an office, an outreach site, or a drop-in center.

	Do we have the following in place?	Yes	No
23	Results from a mapping exercise or needs assessment that identified safety and security vulnerabilities at our workplace		
24	A systems to assess, plan and implement appropriate physical s ecurity for our workplace		
25	Security guards or watchmen		
26	Alarm systems		
27	Security cameras		
28	A clear admission procedure to monitor workers, volunteers, and visitors entering and leaving our workplace		
29	A process to verify identity that is respectful of gender identity, that can enable self-disclosure, and can honor gender identity during a visit		
30	A visitor registration system		
31	A call logging system		
32	A system to track disruptive behavior and identify if or when previously disruptive visitors return		
33	A policy to help identify if or when unauthorized access to files has taken place or if materials have been tampered with		
34	Measures to protect physical information in the workplace (e.g., locked filing cabinets, anonymous codes for client files)		
35	Measures to protect electronic data (e.g., back-up system, encryption of files) and procedures in place to prevent hacking		

	Do we have the following in place?	Yes	No
36	A procedure for first-line response to a safety or security incident at the workplace and roles and responsibilities clearly communicated with all workers (e.g., who to contact and steps to be taken)		
37	Clear exit and client flow signage at the workplace, to guide the movement of visitors and to mark areas that are restricted access for workers only		
38	Bathrooms that are safe and gender neutral, for everyone to use		
39	Rules or a code of conduct in place about appropriate behavior for workers and visitors at the workplace		
40	Organizational registration information clearly visible to authorities (legal identity)		

5. Risks and situations leaders, outreach workers, programme people, service providers and community mobilizers working on HIV in LAC are exposed to in the course of their activities

	Have you or any member of your organization been a victim of the following attacks?	Yes	No
41	Rape		
42	Sexual harassment by coworkers from the organization		
43	Sexual harassment by beneficiaries		
44	Verbal abuse and intimidation (including death threats)		
45	Privacy invasion (e.g. home or social networks)		
46	Blackmail and/or extortion by the police or illegal armed groups		
47	Defamation		
48	Incitement to hatred and calls to violence (including those promoted by the media)		
49	House eviction		
50	Expulsion from social groups (e.g., religious groups, family networks)		
51	Police harassment (including detention)		
52	Harassment by illegal armed groups		
53	Confiscation of work items (condoms, lubricants, needles, etc.) by the police or illegal armed groups		
54	Workplace raids by the police or illegal armed groups		

	Have you or any member of your organization been a victim of the following attacks?	Yes	No
55	Cyber-attacks against your organization		
56	Harm or abuse in police custody		
57	No support from authorities when abuses against you or members of your organization are reported		
58	Personal property theft		
59	Threats to partners, children, or family members		
60	Physical assault		
61	Murder		
62	On a scale of 1 to 5, with 1 being “very safe” and 5 being “very unsafe”, how would you rate your safety in the performance of your activities?		

6. Risks and situations organizations working on HIV in LAC are exposed to in the course of their activities

Has your organization or any other known organization working with key populations been a victim of the following attacks?

		Yes	No
63	Looting and assault on premises		
64	Damage to facilities (broken doors or windows, fires, etc.)		
65	Damage to work equipment (computers, vehicles, mobile units, etc.)		
66	Stolen or confiscated equipment (computers, mobile devices, etc.)		
67	Hacked email / social accounts		
68	Destruction or breach of confidential information (physical and online records) in order to harm beneficiaries and staff		
69	Harassment or stalking (e.g., by the police or illegal armed groups)		
70	Defamation of the organization's reputation (including surreptitious or secret filming)		
71	Please describe other assaults considered to be serious in to your experience		

Finally, please provide any additional information you consider relevant to the safety and security of individuals and organizations working with key populations.

TOOL 3

METHODOLOGY FOR THE DEVELOPMENT OF ACTION PLANS TO INTEGRATE SAFETY AND SECURITY

· Methodology for the Development of Action Plans

The present methodology for the development of action plans that allow the integration of security and protection issues for CSOs that work on Human Rights and HIV with key and vulnerable populations

This chapter offers methodological guidelines for the development of activities intended to:

- Encourage a discussion between leaders, outreach workers, community mobilizers and members of CSOs about the risks they face in the course of their activities (defense of human rights, prevention, outreach to key and vulnerable populations, etc.)

- Provide general recommendations on the response to safety and security risks faced by those who work with key and vulnerable populations.

- Guide in the formulation of integration plans to incorporate institutional measures and policies to reduce the vulnerability to safety and security risks for leaders, outreach workers, programme people, service providers, community mobilizers and CSOs working with key and vulnerable populations.

Session 1: Introduction and basic concepts

Session 2: Identification and analysis of safety and security risks

Session 3: Analysis of objectives and solution alternatives to reduce safety and security risks

Session 4: Developing a plan to reduce safety and security risks for CSOs working on HIV with key and vulnerable populations

2. Methodology

Preliminary considerations

To achieve the objectives described above, we propose the development of participatory methodologies that involve the knowledge and experiences of leaders, outreach workers, community mobilizers, program people and service providers from CSOs in the context of working with key and vulnerable populations.

These methodologies are organized in **four working sessions** of 4 hours each (for a total duration of two days) as described below:

- **Session 1:** Introduction and basic concepts
- **Session 2:** Identification and analysis of safety and security risks
- **Session 3:** Analysis of objectives and solution alternatives to reduce safety and security risks
- **Session 4:** Development of an integration plan to incorporate institutional measures and policies to reduce safety and security risks for CSOs working with key and vulnerable populations on Human Rights and HIV issues.

Each of the sessions includes: duration, session objectives, proposed session agenda, topics, methodological recommendations (activities) and resources. According to the local reality, the facilitators can make adjustments to the methodologies, without this affecting the fulfillment of the objectives.

· Facilitator's / Consultant's Skill Profile:

- Acquaintance with CSOs and communities working on HIV issues
- Communication and facilitation skills
- Basic knowledge of safety and security mechanisms in their country (access routes to protection, denunciation and restitution of rights)
- Ability to facilitate group work sessions
- Strong synthesis and writing skills
- Experience in project formulation and intervention strategies

2. Methodology

Participants

This workshop is directed at leaders, outreach workers, community mobilizers, program people and service providers from CSOs working on HIV-related issues and the defense of Human Rights in key and vulnerable populations. It is also intended for those responsible for safety and security within the organization (if any), among other people.

Depending on the context, facilitators may adjust and adapt the suggested methodologies; for example, they may work with a single organization or a group of organizations, as deemed appropriate.

- If the process is implemented in a single CSO, we suggest the participation of all the people: leaders, outreach workers, community mobilizers, program people and service providers working with key and vulnerable populations.

- If the process brings together multiple CSOs, we suggest that key people involved in program implementation (leaders, outreach workers, community mobilizers, program people and service providers working with key and vulnerable populations) participate. For the process to be successful, at least 3 to 5 key actors from each organization should participate. Participants discuss how they will share and review the safety and security action plan developed during the working sessions with the rest of their colleagues.

Notes on Activity Preparation for the Facilitator

- Facilitators should review the toolbox contents to prepare and organize the necessary resources (slide shows, materials, activity guides, etc.).
- Participants should fill out the checklist in advance and have it ready before the work sessions.
- Facilitators should conduct a preliminary analysis of the results.
- Facilitators should invite an expert on the topic to explain access routes to protection, denunciation and restitution of rights (oversight bodies, ombudsman offices, attorney general's offices, police department, cooperation agencies, etc.) in the first session.

2. Methodology

Session 1: Introduction and Basic Concepts

Duration: 4:00 hours

Objectives: Participants will analyze the results of the previously applied checklist; they will recognize basic concepts and national regulations related to safety and security.

Topics: Workshop agenda and objectives; experiences related to safety and security in the course of their activities; learn about the results of the applied checklist; basic concepts on safety and security (see section 3 of the toolbox); national and international protection routes and regulatory frameworks.

Suggested Agenda for Session 1

Activities	Duration
Welcome, participant introductions, objectives and methodologies	15 min
Setting rules of participation	15 min
Experiences and basic concepts on safety and security – group work	90 min
Presentation and discussion of the checklist results	45 min
Expert presentation on access routes to protection, denunciation and restitution of rights, and group discussion to link the participants' experiences with the conceptual framework.	60 min
Closing	15 min

2. Methodology

Methodological Recommendations:

- **Group discussion:** Given the number of concepts covered in the Basic Concepts, we encourage working in groups. The size of the groups will depend on the number of participants. Each group will be given several cards with previously elaborated definitions. The group will read the contents of the cards, discuss their meaning, and identify examples or references based on their own experiences. Then, one member of each group will present the concepts to the rest of the participants, offering instances based on experience.

- **Lectures and dialogues:** We propose lecture-type methodologies with slide shows for the topics Results and Basic Concepts. These should include spaces for discussion, questions and answers, and a group discussion to link the participants' experiences with the conceptual framework.

- **Experto invitado:** As suggested for the topic Routes and Regulatory Frameworks, it would be ideal to have an expert on the topic. If this is not possible, the facilitator should have previously researched the subjects of routes and frameworks to present them in the workshop.

Resources:

- Slide show on objectives, methodologies and rules of participation
- Cards with basic concepts on safety and security
- Slide show on the checklist results
- Slide show on the routes to protection, denunciation and restitution of rights
- Audiovisual equipment

Session 2: Identification and analysis of challenges related to safety and security

Duration: 4:00 hours

Objectives: Participants will analyze and identify the challenges related to t safety and security for their organizations (causes, consequences and manifestations).

Topics: Challenges tree; causes, consequences and manifestations of safety and security risks; causal relationships.

Suggested Agenda for Session 2

Activities	Duration
Summary of Session 1	15 min
Introduction and explanation of objectives and activities	15 min
Slide show on the challenges tree methodology	15 min
Brainstorming: core problem, causes, consequences and effects, manifestations	60 min
Elaborating a challenges tree	60 min
Presentation of the challenges tree(s)	60 min
Discussion and final consensus	15 min

Methodological Recommendation: Problem Tree

The problem tree is a participatory methodology for understanding a situation or a problem. It identifies the negative aspects of the issues faced by people and organizations, establishing relationships between **causes and effects**[30]. However, for the fulfillment of our objective, we will use the methodology so that people recognize that the challenges (consequences) are so dangerous that they require an immediate approach, so we cannot simply work on the fundamental causes. Indeed, it is very difficult to work effectively on long term strategies to address underlying causes, while we are constantly under daily threats. It is for this reason that in this methodology we will use the term "security challenge tree".

According to this methodology the challenges can be identified in the branches of the tree (consequences). This facilitates the identification of solution alternatives and the planning of policies and projects. This methodology can serve as the first step in identifying the objectives and areas of intervention of a project: the representation of the problem in the form of a diagram helps the analysis, clarifies the relationships of cause and effect, and allows the identification of the challenges.

30.- Ortegón, E. Pacheco J. y Roura H. (2005) Metodología general de identificación, preparación y evaluación de proyectos de inversión pública. (General Methodology for the Identification, Preparation and Evaluation of Public Investment Projects) ILPES, Santiago de Chile.

2. Methodology

When developing a project, it is necessary to identify the problem to be solved, its causes, consequences and challenges. We suggest the following steps to achieve that goal:

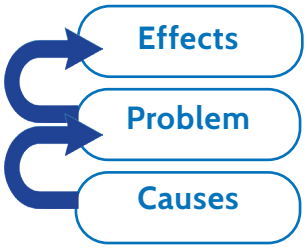
Encourage participants to analyze and identify what they consider to be the main problem in the focal situation. The safety and security risks of both leaders and organizations are the main problem to be addressed. However, to generate ownership among the participants, it is necessary to examine how they perceive this situation.

Use brainstorming to::

- Define the **core problem** affecting the organization, apply prioritization and selection criteria, and attempt to generate consensus on the most suitable option..

- Formulate the **causes** of the core problem identified (this means looking for what elements are or could be causing it). What are the difficulties that cause or directly precede the core problem?

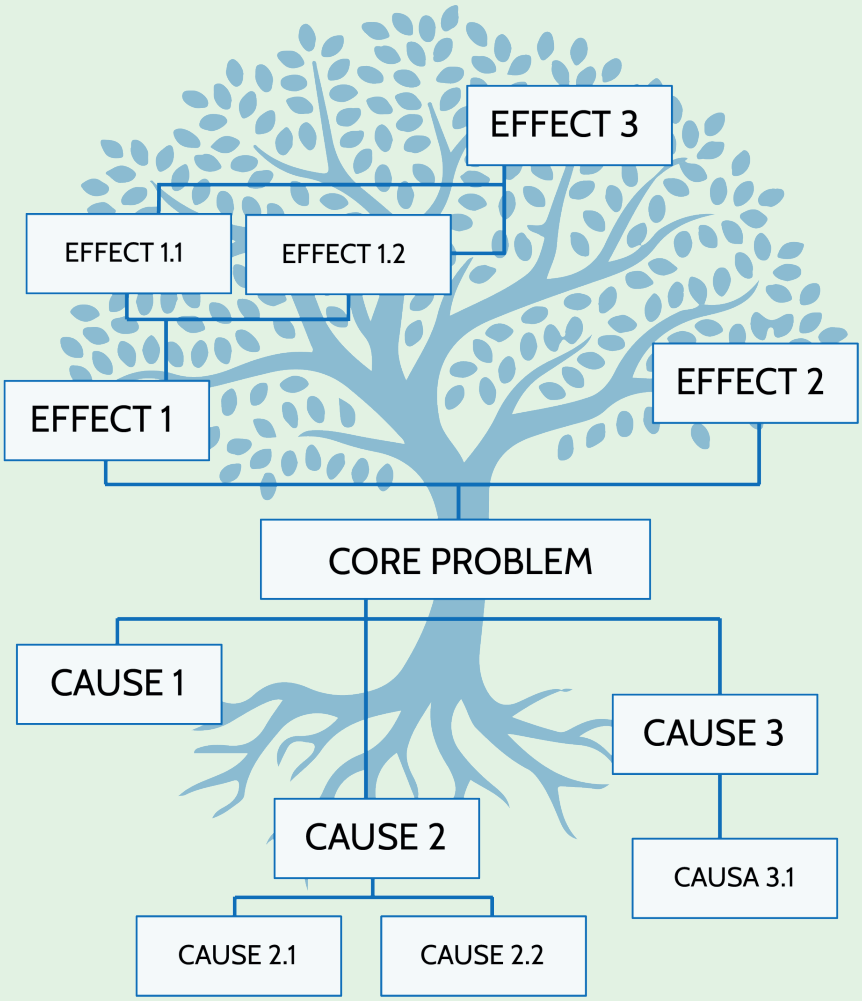
- Determine the most significant **consequences or effects** of the core problem. Analyze and verify their importance. What will be the consequences or effects of the core problem if it is not solved?, What are the main challenges to solve the core problem?



Point out that both causes and consequences (effects) and challenges are linked to the core problem by causal relationships. Discuss this with the participants.

2. Methodology

Identifying and addressing root causes is crucial to creating fundamental change. However, in this exercise we will not focus on removing the root causes, we will focus on analyzing the challenges that the causes represent and that could be impediments to the implementation of the programs, as well as guaranteeing that the people who implement them have conditions of protection and security [31].

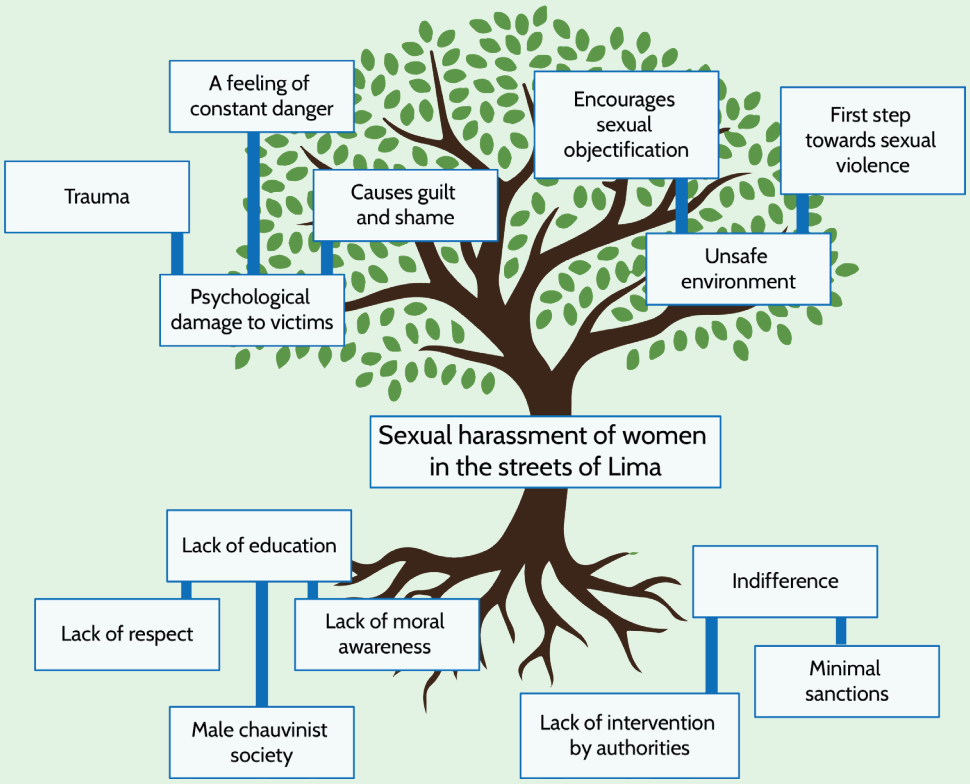


31.- Source: ILPES, Projects and investment programming area.

Once participants identify the core problem, causes, consequences and challenges, they can design the **problem tree**, i.e., a complete picture of the existing negative situation to be addressed.

2. Methodology

Participants can use markers on paper sheets or post-it notes or employ some electronic tool (PowerPoint, Excel, infographics, mind maps, etc.) for this activity. Causes should be placed at the roots of the tree, consequences at the top branches, and the core problem at the trunk, as illustrated below:



Show causal relationships using arrows.

If you are working with a single organization, elaborate the problem tree based on situations and problems identified by the participants.

If you are working with several organizations, a problem tree should be developed for each organization. We recommend that teams share the exercise developed during the workshop with the rest of their organization upon their return.

The validity and completeness of the drawn tree should be verified as many times as necessary. Make sure that causes do represent causes, and effects do represent effects, that the core problem is correctly defined and that the (causal) relationships are correctly expressed. Remember, sometimes causes can also act as consequences.

Relating the results from the checklist applied to the outcome of the problem tree will highlight the validity of the exercise. Request feedback from other participants. Ask if anything is missing.

2. Methodology

Resources:

- Slide show on the problem tree methodology
- Markers, paper sheets, post-it notes, or electronic devices to elaborate the problem tree
- Audiovisual equipment

Session 3: Analysis of alternative solutions to security and protection challenges

Duración: 4:00 hours

Objectives: Participants will identify and analyze solution alternatives to address safety and security challenges for their organizations.

Topics: Safety and security challenges; solution alternatives; objectives, actions and strategies; logical framework matrix; responsible parties; development of an integrated plan and budget (project).

Suggested Agenda for Session 3

Activities	Duration
Summary of session 2	15 min
Introduction and explanation of objectives and activities	15 min
Slide show on the objective tree methodology	15 min
Turning negatives into positives – group work	30 min
Elaborating an objective tree – group work	60 min
Objectives and solution alternatives – group work	30 min
Presentation of the objective tree(s)	60 min
Discussion and final consensus	15 min

Methodological Recommendation: Solution Alternatives Tree

The easiest way to define strategies and objectives is by identifying the desired situation, i.e., a problem situation solved. For this reason, in this session, we will work from the tree of security and protection challenges developed in the previous session, to obtain a tree of alternatives to address the identified security challenges.

Transform each negative situation in the challenges tree into a positive, feasible and achievable state. In this way, In this way, all challenges are transformed into alternative solutions, and the core problem will become the general objective or project purpose in the solution alternatives tree. This new diagram is of utmost importance, as the solution alternatives to overcome the problem must originate from it.

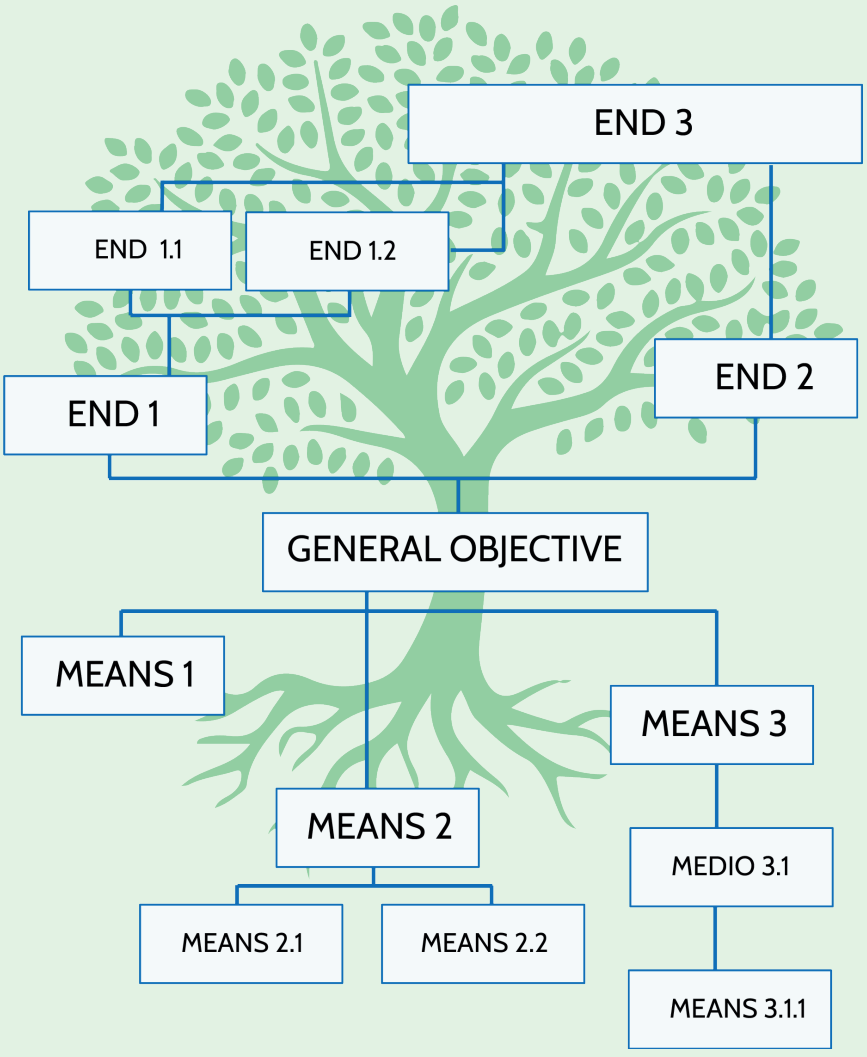
For instance, if the core problem is "High vulnerability of outreach teams to safety and security risks", the desired situation would be "Reduced vulnerability of outreach teams to safety and security risks". In turn, this would be the general objective or project purpose.

As we know, many of the causes of security and protection risks are structural, here we recommend that the analysis and prioritization be oriented towards those challenges that are most immediate and viable to modify through projects or institutional policies, that is, prevention and mitigation of immediate and direct risks and damages related to the safety and security of people and institutions. Being constantly bombarded by threats and emergencies makes it very difficult to manage an organization activities.

Remind participants that addressing these issues also enables the organization to focus and allocate the space and energy to work on the root causes of problems addressed by the programs targeting key and vulnerable populations in the long term.

2. Methodology

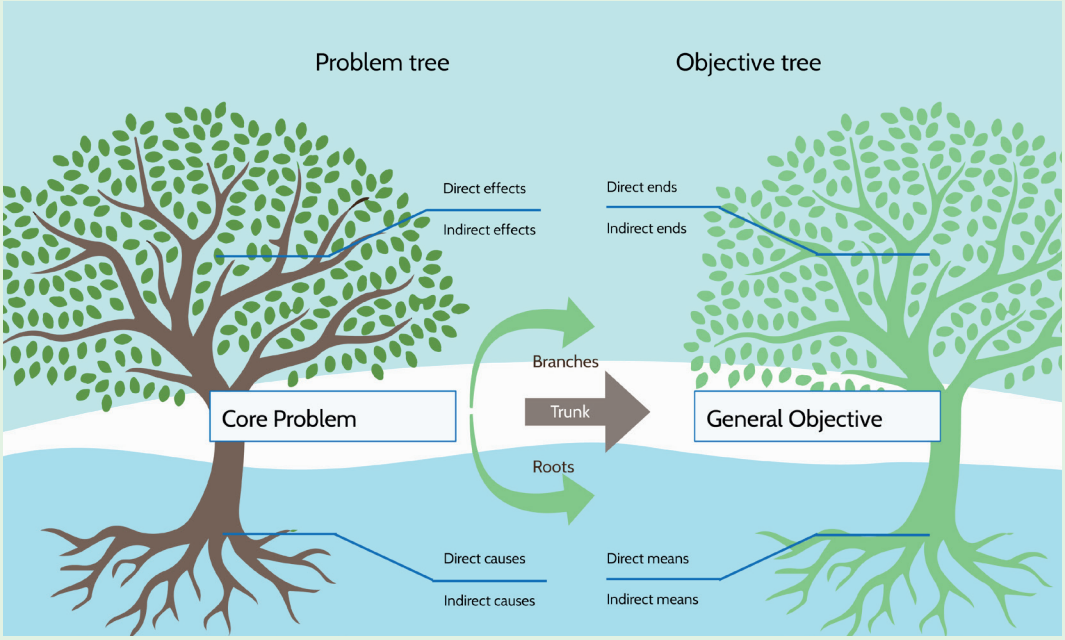
If you are working with a single organization, elaborate the problem tree based on situations and problems identified by the participants. If you are working with several organizations, a challenges tree should be developed for each organization. We recommend that teams share the exercise developed during the workshop with the rest of their organization upon their return.



Once the challenges tree has been created, it is necessary to verify the means-ends relationships established with the core problem to ensure the validity and integrity of the analysis scheme. If deemed necessary, and always bearing in mind that the method should be as flexible as needed, adjust any incorrect formulations, incorporate new relevant solution alternatives not included, and eliminate those that were not effective or viable.

Ask: **Is there something missing?**

2. Methodology



Source: Digital portfolio of an educational project [32]

To identify solution alternatives, it is necessary to formulate actions that would help to respond to the challenges identified. For this reason, the challenges tree should be used as a tool to creatively search for actions that would provide an effective solution in practice. For example:

Core problem:	**Cause (-):**	**Means (+):**	**Action:**
High vulnerability of outreach teams to safety and security risks.	Lack of an institutional security protocol in place	Possession of an institutional security protocol in place	Development of an institutional security protocol

32.- Retrieved from: http://leon-vera-proyectoedu.blogspot.com/2016/05/arbol-de-objetivos.html [in Spanish]

2. Methodology

Reading this diagram from right to left, we can observe that the action proposed respond to a challenge identified, which addresses one of the causes of the problem.

Once the respective actions for the challenges have been formulated, participants should:

- Prioritize viable and relevant actions
- Establish complementary relationships and group them
- Configure a solution alternative and a specific objective with each group of complementary actions.
- Assess the level of impact of the different solution alternatives and prioritize those with the highest impact
- Verify the feasibility (physical, technical, budgetary, institutional, cultural, etc.) of the alternatives

Based on the above process, participants are now able to formulate the objectives of the integration plan to incorporate institutional measures and policies to reduce safety and security risks for their organization and work teams.

Bear in mind that objectives must meet the following criteria:

- Realistic: they can be achieved with the resources available within the given general conditions.
- Effective: not only should they address present concerns, but they should also respond to those that will exist in the future where the objective is located.
- Coherent: attainment of one objective should by no means preclude the attainment of another.
- Quantifiable: they are measurable over time.

Formulate your own objectives!

Resources:

- Slide show on the objective tree methodology
- Markers, paper sheets and post-it notes, or electronic devices to elaborate the problem tree
- Audiovisual equipment

Session 4: Development of an integration plan to incorporate institutional measures and policies to reduce safety and security risks for CSOs working with key and vulnerable populations on Human Rights and HIV issues

Duración: 4:00 hours

Objectives: Participants will have the ability to develop a plan to incorporate institutional measures and policies to reduce safety and security risks for their programs.

Topics: Logical framework matrix (goals, indicators and sources of verification); integration plan to incorporate institutional measures and policies to reduce safety and security and budget; organizational safety and security policy; lobbying activities for funding; resource mobilization; resource mobilization for safety and security.

Suggested Agenda for Session 4

Activities	Duration
Summary of session 3	15 min
Introduction and explanation of objectives and activities	15 min
Slide show on basic concepts	30 min
Development of a logical framework matrix	30 min
Presentation of the logical framework matrix and feedback	30 min
Development of an integration plan to incorporate institutional measures and policies in their programs and budget	30 min
Presentation and feedback on the integration plan and budget	30 min
Development of an organizational safety and security policy	60 min

Methodological Recommendation: Logical Framework Matrix

For this activity, the facilitator will guide the development of a **logical framework matrix** , for an intervention proposal to reduce the vulnerability to safety and security risks for the organization and its members.

The logical framework is a standardized methodology to strengthen the design, implementation and evaluation of social projects. This simplified tool promotes a logical understanding of the intervention: it helps to reflect on and communicate the project proposal. It is objective-oriented and enables the participation of different actors. At this point, participants have already completed the problem analysis phase and the search for solution alternatives. They should now structure a project proposal in a logical framework matrix.

An example that can serve as a guide in creating a logical framework matrix can be found in **ANNEX D.** If the facilitator is not familiar with the logical framework methodology, we suggest examining this model to guide the process.

Logical framework matrices help develop **integration plans and budgets**, following the guidelines used by organizations. Support participants in elaborating their integration plans and budgets, if necessary.

Special Considerations:

- It is indispensable to ensure the full integration of safety and security measures into the programs.

- It should be an organic and cross-cutting component, like monitoring, assessment, and strategic supervision. Safety and security actions should be present in peer educator training components; security protocols should be designed to safeguard data; security procedures should accompany field activities; and they should be present in protecting the security of the organization's facilities, to cite a few examples.

- However, an "integration action plan" could be developed to outline the steps necessary to integrate security throughout the program.

- Keep in mind that not all security actions will require a budget; some may simply require different work methods.

- It is essential to identify potential support resources (such as referral networks) that can anticipate, mitigate and respond to potential risks for key and vulnerable populations.

Development of an organizational safety and security policy

Institutional policies formalize the informal and make the implicit explicit. These internal documents establish basic operating guidelines and guiding criteria for action. Internal policies do not guarantee organizational implementation or the eradication of safety and security risks, nor do they alone establish a certain organizational culture or practices; however, they do contribute to generating certainty, predictability and clear rules[33]. They also validate and confirm that organizations have a duty of safety and security towards their staff and volunteers.

Moreover, when institutional policies are properly developed through a transparent and participatory process, they contribute to the organization's mission and legitimacy by showing consistency between what the organization says externally and its internal practices. In the area of safety and security, institutional policies may:

- Ensure compliance with the organization's objectives and activity implementation.
- Integrate safety and security actions for both the organization and its members.
- Ensure the safety and security of both the organization and its members.
- Guarantee access of beneficiary populations to goods and services.
- Establish consistency criteria for complex situations.
- Validate that organizations have a duty of safety and security towards their staff, systems and goods.

Institutional policies may take the form of protocols, handbooks or policy documents. Developing an **institutional safety and security policy** requires time for its formulation and approval; for this reason, we suggest the following steps and recommendations for its formulation..

Resources:

- Slide show on the logical framework methodology
- Computer equipment for group work
- Audiovisual equipment

33 .- Wigodzky, Victoria y Martha Farmelo. "Cómo elaborar un manual de políticas institucionales: Una guía práctica para organizaciones no-gubernamentales en América Latina" (How to Write an Institutional Policy Manual: A Practical Guide for Non-Governmental Organizations in Latin America), developed with the support of the William and Flora Hewlett Foundation, 2015. Available at: https://gife.issuelab.org/resources/24153/24153.pdf [in Spanish]

Recommendations to be taken into consideration in the development of a safety and security policy:

- Base the policy on the results of the safety and security checklist, as they would justify the regulation.
- Identify sources for funding the policy. Although many actions can be implemented without resources, there is no doubt that such resources are necessary. Examples include lobbying funders to include a budget line for safety and security issues; mobilizing own resources, donations, social responsibility, etc.
- Include a person or team responsible for the policy follow-up and implementation. If properly integrated, responsibility should be distributed among all members of the organization.
- Include strategies for policy evaluation and monitoring, as well as periodic reviews to update the policy according to changing conditions.
- Use simple and clear language that does not lend itself to multiple interpretations, and that can be understood by any member of the organization.
- Include (if necessary) annexes such as safety and security protocols, etc., to make the document more user-friendly.
- Make clear that all members must respect and comply with this policy. In case of non-compliance –and depending on its seriousness–, the organization may take corrective actions, including termination.
- Establish guidelines for:
  - Outreach trips in areas where (potential or confirmed) risks to physical and emotional integrity are identified
  - Outreach worker teams (never a single person)
  - Transportation during home-to-office travel (if necessary)
  - Trips to locations that may pose (potential or proven) risks
  - Office security
  - Computer security
  - Routes and key contacts in case of security and safety incidents (e.g., a telephone tree or call chains)
  - Natural disasters
  - Ensuring that, as soon as possible after the incident, the entire team is provided with safe spaces for discussion and reflection, where they can learn from the experience, share lessons, and identify improvements for the future
  - Logging all safety and security incidents
  - This list is illustrative and can be expanded according to the context of each organization.

ANNEX A

UNDERSTANDING SAFETY AND SECURITY CHALLENGES AND THEIR IMPACTS

Many organizations implementing HIV programs are asked to undertake risk assessments as part of applying for funding.

This annex provides examples, that the organization and donor may consider based on their context.

SAFETY AND SECURITY CHALLENGES WITHIN THE IMPLEMENTATION OF HIV PROGRAMS AND THEIR IMPACT ON WORKERS AND HIV PROGRAMS

FACTOR	EXPLANATION AND EXAMPLES	IMPACT
INDIVIDUALS INVOLVED IN IMPLEMENTING HIV PROGRAMS	• Sexual assault, including rape • Sexual harassment by other workers and unwanted sexual advances by beneficiaries • Outing as a KP member or an individual who works with KP members • Verbal abuse and intimidation, including death threats • Intrusion of privacy (e.g., at home or in social media) • Blackmail and extortion • Defamation of character • Hate speech and calls for violence (including by media) • Eviction from home • Eviction from social groups (e.g., religious groups, family networks) • Law enforcement harassment, surveillance, and crackdowns, including unlawful arrest, detention, strip-search, and confiscation of commodities (e.g., condoms, lubricant, and needles) • Harm while in law enforcement custody, including forced anal examination or lack of access to ARVs • Lack of law enforcement support when abuses are reported • Theft of personal property • Threats to partners, children, and family • Accusations of terrorism • Physical attack (e.g., beating, stabbing, shooting) • Murder	• Short- and long-term trauma • Loss of privacy and anonymity • Loss of reputation • Isolation from family, community, religion • Loss of employment and income (this is especially true of individuals who volunteer with KP programs and have other paid employment elsewhere) • Loss of property and possessions • Fear (e.g., of going out alone or of being blackmailed) • Homelessness • Loss of liberty (e.g., due to arrest or detention) • Government monitoring • Harassment on/inability to safely employ social media for personal use • Mental health problems (e.g., anxiety, isolation, depression, suicide) • Burnout • Restricted movement or forced to hide • Forced to seek asylum outside the country • Physical injury (e.g., bruising, broken bones, lasting disability) • Death

SAFETY AND SECURITY CHALLENGES WITHIN THE IMPLEMENTATION OF HIV PROGRAMS AND THEIR IMPACT ON WORKERS AND HIV PROGRAMS

FACTOR	EXPLANATION AND EXAMPLES	IMPACT
ORGANIZATIONS AND OFFICES INVOLVED IN IMPLEMENTING HIV PROGRAMS	• Sites ransacked and raided • Sites vandalized (e.g., windows broken, rooms set on fire) • Equipment damaged (e.g., vehicles, mobile outreach units) • Equipment stolen or confiscated (e.g., computers) • Email systems/social media hacked • Physical and online records destroyed or confidential information used to harm beneficiaries and staff • Commodities removed or stolen (e.g., condoms, lubricants) • Surveillance (e.g., by police or vigilantes) • Electricity or water supplies stopped or damaged • Defamation of organization's reputation (including through surreptitious filming)	• Forced relocation or going underground • Property missing or damaged • Loss of data • Forced purchase of new equipment (e.g., computers) using organizational funds (not programmatic funds) or managing without equipment • No or reduced services offered • Limited access to clients • Reduced ability to distribute commodities • Loss of staff (e.g., due to fear, burnout, or ill health) • Provision of fewer and lower quality HIV interventions (e.g., testing events) • Inability to meet deliverables for programs funded by donors, decreasing opportunities for future funding • Withdrawal of partner organizations (especially those working primarily with the general population) and isolation from mainstream civil society • Breakdown of referral systems when partnering agencies no longer wish to collaborate • Forced reassignment of time, resources, and energy to safety and security issues (detracting from core work and services) • Damage to organizational profile and reputation • Deregistration as an organization • Temporary or permanent closure

Safety and security challenges affecting HIV programming for and with key populations in LAC occur in a wide variety of locations. These locations are in addition to abuses that often affect KP members in their personal lives, including violence

- On the way to/from program activities
- On the way to/from offices (e.g., on public transport)
- In communities
- At offices
- At drop-in centers
- At clinics and other service delivery points
- At educational organizations
- In social settings (e.g., parties)
- At police stations
- At outreach locations (e.g., streets, bars, injection sites, HIV testing events)
- At decision-making locations (e.g., government meetings, officials' offices, religious organizations)
- During research activities (e.g., focus group discussions)
- In the media (e.g., in newspapers, on the television)
- Online (e.g., on Facebook, Instagram, or Grindr)

There are a wide variety of perpetrators of violence responsible for safety and security challenges. Each of these perpetrators can play both a direct role (such as a community vigilante who physically attacks an outreach worker) and an indirect role (such as a journalist whose article inspires acts of violence or outs someone as a member of a KP). Because KP members' behaviors are often illegal and stigmatized, outing someone serves to weaponize society against them. At the same time, almost all of the individuals in this list can also be allies to KP program implementers, helping them to prevent or mitigate the impact of violence against themselves as well as beneficiaries.

- Law enforcement officers, sometimes acting within the law and other times abusing their authority
- Local and national authorities, including Ministries of Interior, Finance, Health, and Justice
- Landlords of spaces used by CSOs
- Community leaders
- Neighbors and community members located near the CSO
- Community mobs and vigilantes
- Student groups
- Disgruntled CSO workers or former workers
- Family members, intimate partners, and friends of workers
- Program beneficiaries and their families (especially if there are unrealistic expectations about what the program can offer)
- Health care providers
- Religious leaders, including lay leaders such as women's groups within religious organizations
- Decision-makers (e.g., politicians, judiciary)
- Journalists and the media
- Influential figures on social media
- Anonymous attackers online
- Members of other CSOs (especially competitors)
- Educational institutions (e.g., school directors abusing CSO representatives in schools)
- Other KP members at hot spots or third parties such as drug dealers or madams/pimps
- Human traffickers
- Donors who do not adequately fund security in KP programs
- Current or former intimate partners of CSO staff

ANNEX B

POSSIBLE SOLUTIONS TO SCENARIOS IN TOOL 2

Below are the sample security incidents from Scenarios to Test Existing Responses to Safety And Security in Tool 2 along with ideas for both preventing these incidents and mitigating their impacts regardless of whether preventative measures were taken.

Please note that the answers below are not meant to be prescriptive. An action that would result in positive outcomes in one context will cause harm in another. As such, there are no "right" answers and each organization must decide what is applicable and appropriate in their own context.

1. The local safety and security situation suddenly gets much worse, with daily reports of verbal/ physical abuse against KP beneficiaries involved in our HIV program..

In advance:

- Put a tracking system in place to record security incidents affecting the organization and a system to document abuses against beneficiaries. Reviewing the events documented in these systems can help identify trends, and you can share this information with others that you may wish to activate or prepare for future action.

After the incident:

- Pause program activities that involve outreach or are otherwise higher risk.

- Call allies, such as larger organizations (ministries, police, more established NGOs) to ask for their support

- Have the organization's security team complete **Tool 2** to identify priority gaps that will help you mitigate risk during this time of heightened danger

- Report back to the donor with the issue, proposed responses, and any anticipated changes in ability to meet objectives/targets

2. We need to use the program budget to address urgent safety and security needs (e.g., security for the office, software to protect online files), but if we do, we won't have sufficient funding to meet our original targets.

In advance:

- Negotiate with the donor to have the flexibility to dedicate resources to organizational security or to have specific line items for security-related emergency funds.

After the incident:

- Apply for security grant from Dignity for All, Frontline Defenders, or another similar funding source
- Before acting, report back to the donor with the issue, proposed responses, and any anticipated changes in ability to meet objectives/targets

3. A worker reports that he or she has been harassed by another worker..

In advance:

- Develop policies to address grievances that ensure multiple levels of accountability, such as complaints directly to the board, and socialize all workers on their policies as part of on-boarding

After the incident:

- Follow existing policies to address the harassment without putting the victim at risk of retaliation OR develop new policies if no relevant policies exist.
- Retrain workers on the code of conduct (or provide an initial training).
- Offer mental health support to the person who was harassed.

4. An outreach worker is arrested while distributing condoms and is being held by police.

In advance:

- Work with local authorities to receive permission for all outreach activities, and train senior and front-line law enforcement officers on their role in the HIV response, including creating an enabling environment for outreach activities..
- Train outreach staff to explain the nature of their activities to law enforcement and provide them with official documentation (such as ID cards or letters from local authorities or the Ministry of Health) describing their purpose.
- Identify lawyers who can support the organization as needed if issues arise.

After the incident:

- Call allied lawyers or an in-house attorney to follow up immediately (if there is no funding for a lawyer and no opportunity to engage a lawyer pro bono, reach out to Dignity for All [focused on LGBT communities], Frontline Defenders, The Lifeline Embattled CSO Assistance Fund, or other funds for support).
- If contacts with the police exist, call these individuals to discuss next steps.
- If there is a desire to make the issue more publicly visible (for example, by activating allies), ensure that this case is thoroughly investigated before taking this step.

5. After an HIV outreach activity with KP members, a beneficiary posts photos of the outreach workers and community members on Facebook and tags them.

In advance:

- Inform people who come to any events whether the space is photo-friendly (this can also help beneficiaries who see others taking photos to remind them of policies or report them as needed)

After the incident:

- If the photos are posted without negative intent, reach out to the person to take them down and explain the importance of not posting such photos in the future.
- If an individual knowingly violated clear policies or will not take down photos, do not allow them to participate in future events.
- Report the individual to Facebook administrators who can suspend their profile.
- Notify those who were identified and explain the steps being taken to address the issue. Provide them with support as needed if the posting causes emotional or physical abuse.

6. The office is raided by the police, and they take all the files and computers

In advance:

- Protect all technology that includes stored information with passwords and encryption.

After the incident:

- Create a plan that describes what will happen to support those named if data are leaked (for example, helping people who are identified on the files).
- Reach out to senior allies within the police force to give you advice on how to proceed. For example, clarify what will be done with these materials and encourage them not to misuse or share medical files and other personal information.
- If the seizure was not legal, consider contacting a lawyer to challenge materials taken without a warrant.
- Report back to the donor with the issue, proposed responses, and any anticipated changes in ability to meet objectives/targets.

7. A hostile article about your organization is printed in the newspaper; it gives the address of your clinic and includes photographs of two of your clinicians.

In advance:

- Connect with local authorities and law enforcement to explain, in conjunction with a local Ministry of Health official, the nature of the activities undertaken by the organization.
- Register your organization.
- Work to build relationships with power holders, such as religious leaders, who can defend your organization.
- THave a clear policy that describes how your organization interacts with journalists and use press statements instead of interviews, from which comments may be distorted or taken out of context.

After the incident:

- Inform allied local authorities of the issue and ask for their support in case violence against the organization or individual providers occurs.
- Support the clinicians to relocate briefly if they believe they will be in danger at their homes.
- Have the Ministry of Health write an article clarifying the role of the organization and its importance to the health of the community.
- Stop operations at the clinic and support beneficiaries to receive services elsewhere until the issue passes.
- Report back to the donor with the issue, proposed responses, and any anticipated changes in ability to meet objectives/targets.

8. A peer outreach worker at your organization is blackmailed by a beneficiary who threatens to tell the worker's parents that the worker is gay.

In advance:

- Have a clear code of conduct for program participants that includes expectations of confidentiality and describes consequences of a failure to meet these expectations..

After the incident:

- Support the mental health of the worker by providing active listening and linking them to a counselor if desired.
- Explain the local legal context (for example, is the beneficiary's action illegal) and options to the worker; these include no action (blackmail is often not carried out) and blocking the beneficiary on social media and phone. Once the worker decides on an option, provide support as relevant as they carry out their choice.
- Prevent the beneficiary from returning to any future program events.

ANNEX C

Matrix example

Integration plan to incorporate institutional measures and policies to reduce safety and security risks in the programs of an NGO working with key and vulnerable populations in Latin America

Objectives	Indicators	Means of verification	Assumptions
End: Contribute to reducing the vulnerability of people and organizations working on human rights and HIV in Guatemala	Number of security incidents involving social organizations in Guatemala	Statistics on the security of social leaders and organizations in the country	Information systems do not record security incidents of social leaders and organizations in the country
General Objective: Reduce the vulnerability of Good Life Foundation (GLF) members to safety and security risks	Number of security incidents involving GLF members	Record of security incidents in GLF	GLF does not record security incidents
Specific Objective 1: Implement a field safety and security protocol for GLF field teams	Number of GLF members who know how to act in the event of a security incident, according to the institutional protocol	Safety and security checklist	No resources are available to implement the GLF security protocol
Specific Objective 2: Provide the organization with security equipment	Number of security cameras installed and functioning Number of security software installed and running in equipment Number of security alarms installed and functioning	Safety and security checklist	No resources are available to implement the GLF security protocol

Objectives	Indicators	Means of verification	Assumptions
Specific Objective 3: Develop safety and security skills and strategies in GLF members	Number of GLF members who identify risks in the field Number of GLF members who know how to activate the protection route in the event of a security incident	Safety and security checklist	Team members do not recognize the importance of safety and security
Specific Objective 4: Coordinate with local authorities and other key actors to reduce vulnerability	Number of local authorities who are aware of GLF's work and who can respond to security incidents	Minutes of meetings with local authorities in which they commit to responding to security calls	Local authorities do not show interest in ensuring the safety and security of GLF and its personnel
Component 1: Develop a safety and security protocol for GLF	A well-developed safety and security protocol for GLF	Document of the safety and security protocol for GLF	
Component 2: Purchase and installation of security cameras, alarms and security software	Number of security cameras purchased and installed Number of security software purchased and installed on equipment Number of security alarms purchased and installed	Purchase invoices Security and safety checklist	
Component 3: Design and implement safety and security training for GLF teams	Training methodology Number of GLF team members participating in training sessions	A methodological document Attendance list and photographic record	

BIBLIOGRAPHY

1. U.S. Agency for International Development (USAID), Linkages across the Continuum of HIV Services for Key Populations Affected by HIV (LINKAGES), U.S. President's Emergency Plan for AIDS Relief (PEPFAR), FHI 360. Key population implementation guide. Durham (NC): FHI 360; 2016.

2. World Health Organization. (2014). Consolidated guidelines on HIV prevention, diagnosis, treatment and care for key populations.

3. https://www.dw.com/es/guatemala-asesinan-a-balazos-a-andrea-gonzález-dirigente-lgbtiq/a-57870338 [in Spanish]

4. Inter-American Commission on Human Rights (2015): Violence Against LGBT People.

5. USAID, PEPFAR, Alliance, LINKAGES (2018). Safety and Security Toolkit: Strengthening the Implementation of HIV Programs for and with Key Populations.

6. USAID, FHI360, LINKAGES, UNAIDS, and others (2020) AMAN MENA, Secure in MENA region: Security Protections for Organizations Working with Key Populations to Strengthen HIV Programming in the Middle East and North Africa.

7. Beyrer C, Grady C, Bekker L, McIntyre J, Over M, Jarlais D. A framework for ethical engagement with key populations in PEPFAR programs. [no date; accessed 2018 Jan 23]. PEPFAR.

8. These may include donors, religious leaders, media, politicians, and law enforcement officers who promote the well-being of members of KPs.

9. United Nations Population Fund, Global Forum on MSM & HIV, United Nations Development Programme, World Health Organization, United States Agency for International Development, World Bank. Implementing comprehensive
HIV and STI programs with men who have sex with men: practical guidance for collaborative interventions (the "MSMIT"). New York: United Nations Population Fund; 2015.

10. Bickley S. Security risk management: a basic guide for smaller NGOs. London: European Interagency Security Forum (EISF); 2017.

11. Synergía Security Training. Delivered in Lilongwe, Malawi. 2016.

12. World Health Organization (WHO). Consolidated guidelines on HIV prevention, diagnosis, treatment and care for key populations–2016 update. Geneva: WHO; 2016.

13. While these factors can be changed overtime, and some HIV programs also engage in advocacy to address root causes of safety and security challenges, HIV programs operating now can use their local knowledge of each of these factors to decide what risk mitigation strategies are needed and which are feasible.champions.

14. Transgender people are often charged under laws criminalizing other KP members either because they also engage in criminalized behaviors or because gender identity and sexual orientation are inappropriately conflated.

15. Freedom House. Freedom in the world 2018: the annual survey of political rights and civil liberties. Washington (DC): Freedom House. Disponible en: https://freedomhouse.org/sites/default/files/2020-02/FreedomintheWorld2018COMPLETE-BOOK_0. pdf.

16. Human Rights Watch. Human Rights Watch: world report 2018. New York: Seven Stories Press; 2017. Available from: https://www. hrw.org/sites/default/files/world_report_ download/201801world_report_web.pdf.

17. World Health Organization (WHO). Consolidated guidelines on HIV prevention, diagnosis, treatment and care for key populations–2016 update. Geneva: WHO; 2016.

18. United Nations Population Fund, Global Forum on MSM & HIV, United Nations Development Programme, World Health Organization, United States Agency for International Development, World Bank. Implementing comprehensive HIV and STI programs with men who have sex with men: practical guidance for collaborative interventions (the "MSMIT"). New York: United Nations Population Fund; 2015.

19. United Nations Office on Drugs and Crime, International Network of People Who Use Drugs, Joint United Nations Programme on HIV/ AIDS, United Nations Development Programme, United Nations Population Fund, World Health Organization, et al. Implementing comprehensive HIV and HCV programs with people who inject drugs: practical guidance for collaborative interventions (the "IDUIT"). Vienna: United Nations Office on Drugs and Crime; 2017.

20. World Health Organization, United Nations Population Fund, Joint United Nations Programme on HIV/AIDS, Global Network of Sex Work Projects, World Bank. Implementing comprehensive HIV/STI programs with sex workers: practical approaches from collaborative interventions (the "SWIT"). Geneva: World Health Organization; 2013.

21. United Nations Development Program (UNDP), IRGT: A Global Network of Transgender Women and HIV, United Nations Population Fund, UCSF Center for Excellence for Transgender Health, Johns Hopkins Bloomberg School of Public Health, World Health Organization, Joint United Nations Programme on HIV/AIDS, U.S. Agency for International Development. Implementing comprehensive HIV and STI programs with transgender people: practical guidance for collaborative interventions (the "TRANSIT"). New York: UNDP; 2016.

22. International Labour Organization (ILO). Health and life at work: a basic human right. Geneva: ILO; 2009.

23. Synergía Security Training. Delivered in Lilongwe, Malawi. 2016.

24. Synergía Security Training. Delivered in Lilongwe, Malawi. 2016.

25. Protection International (PI). Protection manual for LGBTI human rights defenders. Brussels: PI; 2010.

26. Cisgender refers to individuals whose gender identity aligns to their sex assigned at birth. A person who sees herself as a woman and who was assigned female at birth is a cis female.

27. Tactical Technology Collective. Holistic security: a strategy manual for human rights defenders. Berlin: The Collective; 2016.

28. Implementing Comprehensive HIV and STI Programs with Transgender People.

29. Source: United Nations Development Programme (UNDP), IRGT: A Global Network of Transgender Women and HIV, United Nations Population Fund, UCSF Center for Excellence for Transgender Health, Johns Hopkins Bloomberg School of Public Health, World Health Organization, Joint United Nations Programme on HIV/ AIDS, U.S. Agency for International Development. Implementing Comprehensive HIV and STI Programs with Transgender People: Practical Guidance for Collaborative Interventions. New York: UNDP; 2016.

30. Ortegón, E., Pacheco, J. F., & Roura, H. (2005). Metodología general de identificación, preparación y evaluación de proyectos de inversión pública (General Methodology for the Identification, Preparation and Evaluation of Public Investment Projects). Cepal. Available at: https://repositorio.cepal.org/handle/11362/5608 [in Spanish]

31. Source: ILPES, Projects and investment programming area.

32. Retrieved from: http://leon-vera-proyectoedu.blogspot.com/2016/05/arbol-de-objetivos.html [in Spanish]

33. Wigodzky, Victoria y Martha Farmelo. "Cómo elaborar un manual de políticas institucionales: Una guía práctica para organizaciones no-gubernamentales en América Latina" (How to Write an Institutional Policy Manual: A Practical Guide for Non-Governmental Organizations in Latin America), developed with the support of the William and Flora Hewlett Foundation, 2015. Available at: https://gife.issuelab.org/resources/24153/24153.pdf [in Spanish]

Resources

- The International HIV/AIDS Alliance and the LINKAGES Project. Safety and Security Toolkit: Strengthening the Implementation of HIV Programs for and with Key Populations. Durham, NC: FHI 360; 2018. Available at: https://www.fhi360.org/sites/default/files/media/documents/resource-linkages-safety-security-toolkit.pdf [in English]

- U.S. Agency for International Development (USAID), Linkages Across the Continuum of HIV Services for Key Populations Affected by HIV (LINKAGES), U.S. President's Emergency Plan for AIDS Relief (PEPFAR), and FHI 360. Key Population Program Implementation Guide. Available at: https://www.fhi360.org/sites/default/files/media/documents/resource-linkages-implementation-guide.pdf [in English]

- Programa somos defensores (2019): Un canto para la protección, "Manual para la protección a personas defensoras de derechos humanos y organizaciones sociales en Colombia". (A Song for Protection, "Handbook for the protection of human rights defenders and social organizations in Colombia") Available at: https://somosdefensores.org/2019/08/04/un-canto-para-la-proteccion/ [in Spanish]

Videos

- Tres Pi Medios (2018). Cómo proteger líderes sociales en Colombia - Vídeo explicativo 2018. (How to protect social leaders in Colombia - Explanatory video 2018.) Video describing the routes social leaders should take to be protected by the state. Colombia. Available at: https://www.youtube.com/watch?v=eH6FwVkiR0I [in Spanish]

- Protection International (2021). 10 Pasos para protegerse durante la defensa de los derechos humanos. Available at: https://www.youtube.com/watch?v=Bf_QtQKRcKM [in Spanish]

- Protection International (2021). 10 Steps to Improve your Protection While Defending Human Rights. Available at: https://www.youtube.com/watch?v=qx3-RFm7t34 [in English]

- Protection International (2021): 10 Mesures pour mieux vous protéger lorsque vous défendez les droits humains. Available at: https://www.youtube.com/watch?v=-vmvqGXeJYM [in French]