Strengthening the Security of HIV Service Implementers Working with Key Populations

A virtual training for organizational leadership

April 2021

PEPFAR USAID FROM THE AMERICAN PEOPLE EpiC LINKAGES

Acknowledgments

This training was developed by Robyn Dayton (Senior Technical Advisor, FHI 360), and includes adapted content from Synergía Initiative for Human Rights and the AMAN MENA Toolkit: Security Protections for Organizations Working with Key Populations to Strengthen HIV Programming in the Middle East and North Africa. Iterations of this virtual training have been conducted with FHI 360 staff and partner organizations around the world, including Algeria, Cote d'Ivoire, Central Asia, Liberia, Lebanon, Kenya, Malawi, Mali, Nepal, Senegal, and Tanzania. Their experiences attending the training and sharing the learnings with their organizations, and their feedback and insights on what works virtually helped shape the final content.

Reviewers included Chris Akolo, Meghan DiCarlo, Rose Wilcher (FHI 360); and Michael Marco (USAID). Stevie Daniels served as editor, and Lucy Harber provided design assistance.

This document is made possible by the generous support of the American people through the United States Agency for International Development (USAID) and the U.S. President's Emergency Plan for AIDS Relief (PEPFAR). The contents are the responsibility of FHI 360 and do not necessarily reflect the views of USAID, PEPFAR, or the United States Government.

Suggested citation: LINKAGES and EpiC. Strengthening the security of HIV service implementers working with key populations: a virtual training for organizational leadership. Durham (NC): FHI 360; 2021.

Linkages across the Continuum of HIV Services for Key Populations Affected by HIV (LINKAGES) is funded by the U.S. President's Emergency Plan for AIDS Relief (PEPFAR) and the United States Agency for International Development (USAID). The project is a cooperative agreement (#AID-OAA-A-14-00045) led by FHI 360 in partnership with IntraHealth International, Pact, and the University of North Carolina at Chapel Hill.

Meeting Targets and Maintaining Epidemic Control (EpiC) project, funded by the United States Agency for International Development (USAID) and the U.S. President's Emergency Plan for AIDS Relief (PEPFAR), is a five-year global cooperative initiative (7200AA19CA00002). The project is led by FHI 360 with core partners Right to Care, Palladium International, Population Services International (PSI), and Gobee Group.

Table of Contents

Acronyms and abbreviations

COVID-19 – Coronavirus disease of 2019

CSO – Civil society organization

GBV – Gender-based violence

HIV – Human immunodeficiency virus

INGO – International nongovernmental organization

IP – Implementing partner

PEPFAR – U.S. President's Emergency Plan for AIDS Relief

SOPs – Standard operating procedures

STI – Sexually transmitted infection

USAID – United States Agency for International Development

Snapshot of the training

Audience and purpose

This training package is for use by HIV programs offering services to key populations—gay men and other men who have sex with men, people who inject drugs, sex workers, and transgender people. It is designed to be given to a core group including members of leadership and implementing partner staff to help them identify and prioritize the security risks their organizations face, catalogue their security strategies to identify both current gaps and strengths, develop security plans to address priority gaps, and determine how to fully implement security plans. Multiple implementing partner core teams should be brought together in one training as a core training strategy is cross-organization learning.

The training may be conducted virtually, in person, or as a hybrid between the two. After the initial training of a core group from each implementing partner, those who have been trained can adapt the slides to share security guidance with their entire staff to support the full operationalization of security plans.

Contents

The training package contains:

1. This facilitator's handbook with a participant and facilitator training agenda, pre-/post-test, pre-/post-test key, guidance on effective training implementation, detailed activity instructions, and handouts for use in the training
2. Training slides with clear guidance on where facilitators should add or substitute content, and detailed speaker's notes.

Workshop objectives

The core team from each implementing partner will be trained to:

- Identify safety and security strengths and gaps and share strengths among implementers
- Prioritize safety and security risks faced by the program and determine the most important gaps for the civil society organization (CSO) to address
- Draft CSO-specific security plans that address priority risks and how skills will be built to manage that risk
- Plan for security plan rollout

Time and preparation requirements

Before the training begins, or at least 24 hours before the second session begins, all participating implementing partners should complete a checklist of their current security strategies. The checklist can be found here in Arabic, French, and English. Instructions on how to complete the checklist are in Annex A.

The training, when delivered virtually, is designed to be given over four two-hour periods, with participants completing homework after the first and second sessions. To allow for completion of homework between sessions, the training should ideally be implemented on

nonconsecutive days. It should be co-facilitated by two people—one who has expertise and experience on the security of HIV implementers, and one familiar with the participants who can track their progress toward achieving a certificate.

An illustrative agenda for hosting the training virtually is provided below. The time needed on the third day will depend on the number of organizations presenting and could be more or less than two hours. Most people who host the training in person do so over two days. See Annex B for an example in-person agenda. This gives more time for participants to practice and digest skills, including covering what would have been homework assignments during the training itself.

Participants' virtual agenda

Time	Session	Objectives
	DAY 1	
8:00	Welcome, introductions, and background	● Welcome all participants and introduce participants to one another. ● Come to a shared understanding of training content and goals as well as participants' involvement in the training. ● Identify implementer security as an important and new area of HIV programming.
8:45	Key terms and overarching recommendations	● Define security, risk, threat, capacity, and vulnerability, and discuss the key recommendations for security of implementers in KP programs.
9:15	Threat identification and assessment	● Identify threats and determine their seriousness.
9:55	Day 1 closing	● Evaluate the day.
	DAY 2	
8:00	Recap of Day 1 and HW #1	● Share HW #1 answers. ● Remember the topics covered on Day 1.
8:25	Limiting an aggressor's capacity to harm	● Describe what can be done, and by whom, to limit an aggressor's ability to cause harm.
9:00	Digital security	● Describe the vulnerabilities inherent to digital platforms; identify risk-reduction strategies within each.
9:40	Review of our capacities and plan for skill sharing	● Review collective responses to the security assessments. ● Assign each implementing partner to a skill to be presented in the next session.
9:55	Day 2 closing	● Complete Day 2 evaluation

DAY 3 - Special Session, Group Presentations		
As needed	Group presentations	● Share a security strategy assigned to your CSO. ● Ask questions about all presented strategies to gain understanding of implementation, and pros and cons of the strategy.
DAY 4		
8:00	Day 2 recap and special session reflections	● Reflect on strategies presented during the special session ● Remember the topics covered on Day 2
8:10	Using what you've learned: security challenge case studies	● Brainstorm what your organization could do if faced with a variety of security challenges. ● Discuss whether the "possible solutions" after each scenario would be appropriate in the local context.
8:45	Risk assessment formula	● Become familiar with the formula for determining the likelihood that a given harm will occur.
9:05	Security planning	● Recognize the elements of a security plan and practice using the template to develop your own plans. ● Identify your top three risks and create a security plan for each by considering vulnerabilities, existing capacities, and needed capacities.
9:35	Next steps	● Discuss opportunities for: immediate no and low-cost action, continued cross-CSO learning, linking security activities into ongoing violence prevention and response, and seeking international support. ● Identify action steps to finalize and build buy-in for security plans at each CSO.
9:50	Reflections and closing	● Share thoughts on and evaluate the workshop; provide closing reflections.

A facilitators' agenda for the virtual training can be found in Annex C.

Rationale

Organizations implementing HIV programs for key population members are the targets of a range of abuses because of their efforts to address the health needs of marginalized and, in some cases, criminalized communities. These attacks—ranging from verbal abuse from the general public, isolation by their families and communities, physical assault from law enforcement or vigilantes to attacks on their reputations by local media or religious institutions—are often even more intense when the workers themselves are members of key populations. Such attacks have negative and often extreme impacts on individuals, organizations, and HIV programs. These include short- and long-term trauma among workers, damage to individuals and an organization's reputations, restricted movement of

workers in their personal and professional lives, lost property (including lost data), deregistration of organizations, inability to provide HIV services effectively and, in some cases, even the loss of life.

Strengthening the security of implementers is an ethical and practical requirement for an effective HIV program. This is reflected in the 2021 PEPFAR Country/Regional Operating Plan Guidance where a specific section on safety and security acknowledges the need to "monitor and track progress on issues pertaining to safety and security..." and "…determine the best strategies to provide support in preventing and addressing instances of violence and harassment against individuals and community-based organizations"[1] as a part of key population programming.

In light of COVID-19, security training for implementers are more important than ever—particularly in cases where the same organizations implementing HIV programs also implement COVID-19 prevention or mitigation efforts, placing them at risk of new threats—and must be available virtually to mitigate COVID-19 risks.

Using this facilitator's handbook

This facilitator's handbook offers tips to help you conduct the training in a way that engages participants, particularly those joining virtually. It also provides additional information on topics covered in the training. Please read the full handbook before organizing and implementing a training. The Detailed Session Instructions, combined with the speaker's notes in the PowerPoint presentation, provide implementation guidance.

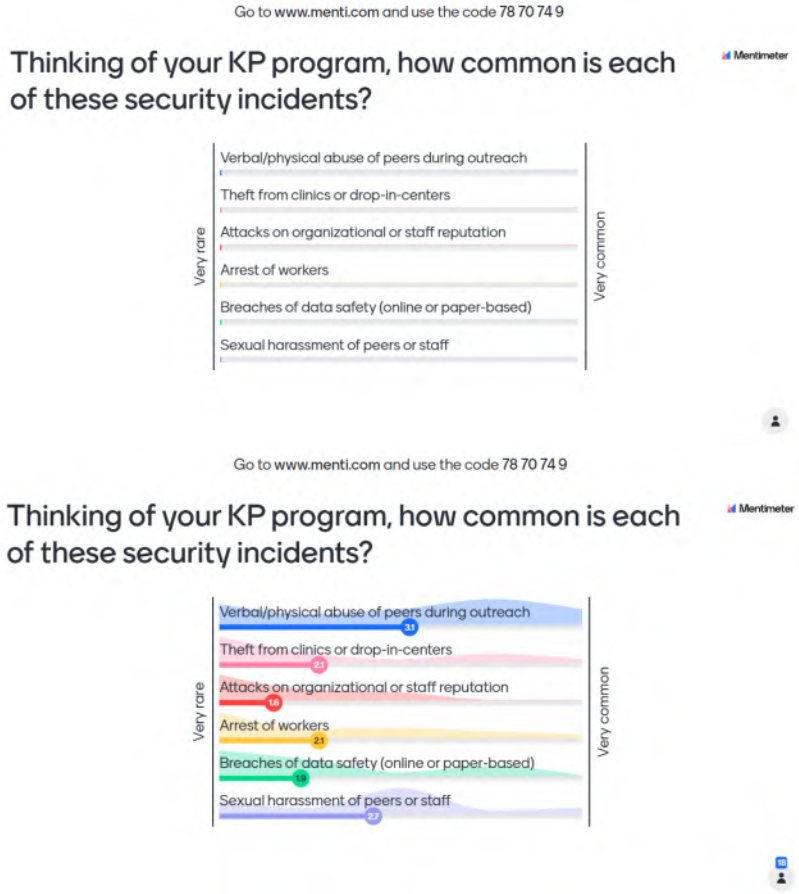
Connectivity

When conducting this training virtually, please ensure that you have a plan in place for the following:

- **What platform(s) will you use to conduct this training?** We have used Microsoft Teams and Mentimeter for presentation and real-time surveys/quizzes. Mentimeter is an online survey/quiz platform by which you can ask questions of the participants who enter their answers into a computer or smartphone. Their answers are then visible to the facilitator—and to participants if the facilitator shares their screen—as they are received. This creates an opportunity for the facilitator to collect information from participants, check their understanding, and clarify anything that is not well understood (see Figure 1 for images from Mentimeter). We used Google Forms for post-test and daily evaluations. Whatever platform(s) you choose to use, make sure that all participants can access them and use their features, such as chat and "unmute" to speak. As necessary, build in extra time before the first session to test each participant's ability to use the platforms successfully to avoid frustration and low participation later.

[1] PEPFAR. PEPFAR 2021 Country and Regional Operational Plan (COP/ROP) Guidance for all PEPFAR Countries. Washington (DC): PEPFAR; 2021. p. 419.

Figure 1. Images from Mentimeter



- **How will you address inevitable issues of disconnection in virtual training?** When providing trainings virtually, there is almost always someone who will not be able to attend at least part of a session due to connectivity issues. Plan a workaround, such as recording your trainings and making them available to participants afterwards. Make sure to get permission before recording. If you would like to record, ask participants if they have any concerns before beginning to record. If there are concerns, you can either avoid recording or advise those who do not wish to be recorded speaking or chatting to contribute in other ways. For example, they may wish to send their thoughts via email after the training.

  Also consider how participant requirements can be tweaked for those who try to engage but encounter connectivity issues. For example, those who miss a live session could send the facilitator their questions and observations by email after watching the recording.

If you need more resources on conducting the training in a low-connectivity setting, please see below.

- **CCCM Cluster** hosted a webinar on adaptations to capacity building, mentoring, and coaching approaches for humanitarian workers in the time of COVID-19. Although directed at camp coordination and management professionals, there are

helpful pointers from guest speakers and participants on strengthening operational capacity when connectivity and access are limited. A YouTube recording is available here.

- **UNESCO** compiled a list of distance learning solutions by category, including systems with strong off-line functionality.
- Outside the development and health sectors, **TalentLMS** put together a guide for facilitators on tweaking eLearning opportunities for users with poor connectivity. **EdTech** also provides tips on using off-line access in remote learning.

Language and names

This training material is currently available in English. However, all slides can be edited and translated into other languages as needed. When translating or adapting to a local context, please also change the names used in the scenarios to be more locally relevant. This can avoid confusion for participants unfamiliar with the names currently used in the slides. Try to avoid using names of training participants in the scenarios.

In addition, you as the facilitator(s) can add information about yourself to make it more interesting. For example, the slides, “Search for yourself,” and “Activity Q” include information about the author of the training. Consider replacing these with the same information about yourself.

Number of participants

Ensure that participants understand what is expected of them from the beginning, which includes their continual participation. Invite no more than 25 participants to each training, even if it is delivered virtually; this allows the facilitator to engage each participant at some point during the training. As mentioned, this training is designed to be given to core groups from different implementing partners. We have found that it works well to have three people from each IP and no more than eight IPs present during a training.

Participant accountability and mastery of skills

Share expectations with all participants before the training. The recommended expectations are below. If a participant cannot commit to meeting these requirements, they will not receive a certificate.

We recommend that all attendees meet each of the expectations below.

- As a group, complete the security checklist in advance. It can be found here in Arabic, French, and English. The checklist should be completed and sent to the facilitators at least 24 hours before the second session of the training.
- Participate in all sessions for the entirety of each session
- Contribute verbally (substantively) at least twice per session
- Contribute via chat at least five times during each session
- Complete homework assignments after sessions 1 and 2
  - Reflect on the security recommendations for IPs
  - As a group, prepare a presentation with others from your CSO on your assigned security strategy
- Score 85% on the post-test

Accessing additional resources

The content presented here builds on the 2020 security resource, AMAN MENA Toolkit: Security Protections for Organizations Working with Key Populations to Strengthen HIV Programming in the Middle East and North Africa. Reading this resource will help facilitators and participants deepen their understanding of the topic and will help facilitators feel more confident presenting on this topic if it is new to them. The AMAN MENA Toolkit is a regional adaptation and update of the 2018 LINKAGES and Frontline AIDS resource: the Safety and Security Toolkit: Strengthening the Implementation of HIV Programs for and with Key Populations.

Strengthening the security of implementers is part of any effective key population program but can play a particularly important role in efforts, such as community-led monitoring, that seek to improve the overall program's ability to meet the holistic needs of clients. Incorporating activities to strengthen implementer security in community-led monitoring ensures that the voices and concerns of those implementing programs are addressed alongside those of clients. Addressing both at once helps to ensure that changes adopted to improve the accessibility of services, for example later operating hours, are accompanied by measures, such as a provider transport allowance, that prevent program adaptations from inadvertently endangering implementers. For more on the full EpiC community-led monitoring package, please visit: https://www.fhi360.org/resource/community-led-monitoring-resources.

Making the content engaging

During virtual trainings, it can be particularly difficult to keep participants engaged. This training is designed to foster participation in virtual spaces. However, keeping participants engaged will also be up to the facilitators, whose role it is to continually call on participants and engage them via chat to make sure that everyone is learning the skills presented.

If you will be presenting virtually, depending on COVID-19 restrictions, consider having some small groups come together (for example, in a training of 15 people, they could be

at five different locations in groups of three). Below is a table with more ideas on how to make different types of activities more engaging in in-person and virtual training.

Activity	In person	Virtual
Question that needs the entire groups' response	Note cards; dot voting	Mentimeter; type in chat (short answer only)
Pre-test/post-test	On paper or online	Online using Google Forms
Daily evaluation	Dot voting to indicate favorite activity; open brainstorm on what went well and what can be improved; post-it notes for anonymous response for what went well and what can be improved	Google Forms or Mentimeter
Small group activities	Divide into groups and give each group space and time to formulate a response	Assign small group work outside of sessions and designate someone in each group to ensure that the group meets; have participants call one another on cell phones for short conversations during the training; use breakout room features in Zoom or Teams.
Make presentation more engaging	If you can extend the time needed for presentation, consider making slides that are text heavy into small group activities where small groups prepare to teach one another the content. For example, slide 15 on *How do security challenges affect KP programs?* could be revised to become an activity where participants brainstorm potential impact under each of the seven areas presented.	Have participants use the chat to talk to each other about what is being presented and to raise questions for the presenter. The presenter should summarize the chat and respond to questions shared there.

Preparation for training

The steps below are useful for preparing either a virtual or in-person training unless otherwise indicated.

Step 1. Review the slides and read this complete handbook. You will note that many of the slides contain green text. Green text in the slides should be removed or replaced before you give the training.

If you plan to revise activities to increase interaction between participants or to make the training in person, make these changes after doing a complete review of this handbook and the slides.

Step 2 (required if virtual, optional if in person). Prepare interactive polls using Mentimeter.com (or another platform of your choice) and a pre-/post-test and evaluation using Google Forms (or another platform of your choice). The sessions that require the use of these platforms are indicated below. This is also noted in the slide presentation by highlighted text that must be replaced before conducting the training.

Step 3. Review all instructions for participatory components of the training. While most slides include a script to guide what the facilitator says, the activities marked with stars are interactive and require understanding and/or advance planning by the facilitators.

Step 4 (if virtual). Create a tracker for virtual participation. It should include the following:

Participant organization	Participant name	Session 1 contributions		Session 2 contributions		Session 3 contributions		Session 4 contributions		Completed HW #1	Post-test score
		# Chat	# Verbal	# Chat	# Verbal	Gave presentation	Asked others questions	# Chat	# Verbal		

This will allow you to document the participation of each person and determine who has met minimum requirements to go on and train others. See Participant accountability and mastery of skills to learn more.

Step 5. Send out invitations that share the dates of the training, the expectations for all participants, the learning objectives, agenda, and information on how the training will be conducted (for example, it may include a link to Zoom if it will be conducted this way). If participants have not used these platforms before, schedule time in advance to practice their use. Do not use the time meant for training to troubleshoot technological issues. You can also look for instructional videos on how to use the technologies you will employ. For example, by searching on YouTube for a “how to” video in the language of your participants. These links can then be shared in advance to support participants’ technology use.

Step 6. At the end of each day of training, share the slides covered and a recording of those slides (if recorded). All participants should agree to recording before this option is used.

Detailed session instructions

Day 1

Time	Session	Objectives
8:00	Welcome, introductions, and background	● Welcome all participants and introduce participants to one another. ● Come to a shared understanding of training content and goals as well as participants' involvement in the training. ● Identify implementer security as an important and new area of HIV programming.
8:45	Key terms and overarching recommendations	● Define security, risk, threat, capacity, and vulnerability, and discuss the key recommendations for security of implementers in KP programs.
9:15	Threat identification and assessment	● Identify threats and determine their seriousness.
9:55	Day 1 closing	● Evaluate the day.

Online preparation for Day 1

- Use Mentimeter.com to create two survey questions. You will show these when you come to the slide for Activity C.

  Question 1. Thinking of your KP program, how common is each of these security incidents?

  - Verbal/physical abuse of peers during outreach
  - Theft from clinics or drop-in centers
  - Attacks on organization and/or staff's reputation
  - Arrest of workers
  - Breaches of data safety (online or paper-based)
  - Sexual harassment of peers or staff

  Question 2. Who perpetrates violence against KP program implementers?

  - Police
  - Religious leaders
  - Media
  - General public
  - KP beneficiaries
  - Other

- Use Mentimeter or Google Forms to collect information on how the first day went. This is relevant to Activity I. Questions should provide you, the facilitators, with information on how to proceed. Illustrative questions include:
  - This session was interesting to me. (strongly disagree to strongly agree, scale)
  - This session will help me do my job. (strongly disagree to strongly agree, scale)
  - The facilitator was knowledgeable. (strongly disagree to strongly agree, scale)
  - I had the chance to share my opinions. (strongly disagree to strongly agree, scale)
  - I would recommend this session to others. (strongly disagree to strongly agree, scale)
  - What changes would you like to see in the next session (open-ended question)

Instructions for activities on Day 1

Use the slide presentation to direct the flow of the training; the slides and speaker notes either summarize key messages or provide instructions for activities. All activity-based slides are denoted with a star. This notation means the facilitator should not simply present the information on the slide, but instead should engage participants to generate the answers. Each activity slide is described further below.

- **Activity A. Introductions.** Giving people the opportunity to speak at the beginning of any training is vital. It encourages them to participate throughout. Take the time needed for each person to introduce themselves, even if the activity goes slightly over time. In an online training it can be hard for people to know when to introduce themselves. No one likes to speak over others or be spoken over. You can make this process easier by having the table in Activity A already filled out. Then, it is just a matter of asking each person to go in order to share the information requested. If you do not have this information in advance, ask those from a specific organization to begin and then continue to the next organization until everyone has the chance to introduce themselves.
- **Activity B. Group norms.** We want to make sure that participants understand what is expected of them in the training. They also need to know what to expect of each other, especially keeping information private; after all, we are discussing security issues. You can change the suggested norms in advance. Just make sure that whatever is listed addresses recording (if recording will occur). The norms should also have content on whether personal experiences recounted during the training can be shared with others outside of the training space.
- **Activity C. What, who, why?** Use Mentimeter to create questions in advance that allow you to understand the most common types of incidents and who the perpetrators are. If you are aware of other security challenges not described in the slides, feel free to add them. The questions needed are described under “Required online preparation for Day 1.”

  After getting answers to these questions, ask individuals to “unmute” themselves and reflect on the answers on the screen. Specific examples are useful. During

reflections, ask those sharing not only *what* is happening, but *why* they believe it is occurring.

- **Activity D. Definitions.** This activity covers all five definitions. Read the question and possible answers out loud (or ask a participant to read). Then, ask respondents to put their choice for answers into the chat. Give several seconds for answers to be provided. Then ask someone who has answered correctly in the chat to unmute and explain their answer. Following their answer, advance the slide to show the correct answer. Then, advance the slide again to show additional clarifying text. Read this text out loud.
- **Activity E. Homework: Overarching recommendations –** This activity will be completed as homework. However, it is important to clearly explain during the session. It asks that groups (described during Activity A) each examine one recommendation from the list. The letter of their group is next to the number of the relevant recommendation. Each group must do the following before the next session:
    - Review their recommendation, including the additional information in the "cheat sheet."
    - Discuss how their organization is already using this recommendation and could use this recommendation.
    - Be prepared to share the recommendation and its current and potential use with all participants during the next session. This should include selecting one person to speak for their group.
    - Groups will need the "security training cheat sheet" available in Annex D to complete the assignment. It is called a "cheat sheet" because it summarizes all the information they will need to take away from the training and pass the post-test. Email it to them immediately after the session.
- **Activity F. Label each threat.** Participants practice using the classifications they have just learned. Read each one and then ask participants to write either "indirect threat, direct threat, or security incident" in the chat. After many have responded, ask someone who answered correctly to unmute and explain their answer. Then, advance the slide and show the correct answer.
    - After doing this for all incidents, ask if there are any questions.
    - Note that if many incorrect answers are being typed into the chat, it is important to take more time to clarify.
- **Activity G. Assessing threats based on impact.** In this activity you ask participants to make a judgment call on how dangerous they feel the example threat is. They should put a number into the chat. Call on a few people to explain their choices. If different people chose different answers, ask for those with different answers to explain their thinking.

  There is no one correct answer. As long as participants can provide justification for their answer, this is fine. If people have different opinions, it is an opportunity to

point out that people have different risk appetites and that security measures are determined in context. In some places this threat may cause a lot of harm. In others, it may be easily neutralized.

- **Activity H. Considering our own threats.** This activity provides an opportunity for the group to do their own threat analysis. Ask one of the participants to unmute and answer each of the questions. If no one volunteers, think back to the threats described in Menti, and ask someone who spoke up then to further describe what was experienced.

  Change out of presentation view into editing view and then type into the slide as the participant speaks, capturing the important parts of what is said. Ask clarifying questions as needed so that you understand what is being shared. Once they have answered all five questions, ask them how dangerous the threat is on a scale of 1–5. Ask if any other participants have comments on the number assigned. Again, there is no one right answer. It is all about using what you know to make sense of how much danger there is in a systematic way.

- **Activity I. Menti, Day 1 closing.** The daily evaluation can be done publicly using Menti by showing your screen as survey results come in. Alternatively, you can leave the survey open as the session ends and then check the responses on your own without sharing the screen. Sample questions are included under “Online preparation for Day 1.”
- **Wrap-up activities.** After the first session is over, the facilitator should send the slides, a link to the recording (if available), and the handouts for the cheat sheet (Annex D) and security incident log (Annex E) to all participants via email. The email should also include a reminder of the homework assignment. See Annex F for a sample email to send at the end of Day 1.

Day 2

Time	Session	Objectives
8:00	Recap of Day 1 and HW #1	● Share HW #1 answers. ● Remember the topics covered on Day 1.
8:25	Limiting an aggressor's capacity to harm	● Describe what can be done, and by whom, to limit an aggressor's ability to cause harm.
9:00	Digital security	● Describe the vulnerabilities inherent to digital platforms; identify risk-reduction strategies within each.
9:40	Review of our capacities and plan for skill sharing	● Review collective responses to the security assessments. ● Assign each implementing partner to a skill to be presented in the next session.
9:55	Day 2 closing	● Complete Day 2 evaluation

Online preparation for Day 2

- For activity K, use Menti.com to ask the following question. Note that "***" shows correct answer and should not be included in the survey question itself.

  Question 1. You are a peer educator. You learn that two other peer educators in your province were arrested during outreach. What kind of threat is this to you?

  - Direct threat
  - Indirect threat***
  - Security incident

- For activity O, use Menti.com to ask the following questions. There are no correct answers.

  Question 1. Which of these devices do you use?

  - Non-smartphone
  - Smartphone
  - Laptop
  - Desktop
  - Tablet
  - USB/thumb drive/flash drive

  Question 2. What could someone learn about you if they accessed your device?

  - Where I work
  - My family members' names
  - My financial information (such as my banking information and credit card numbers)
  - The websites I visit
  - Names and contact information of my friends

Instructions for activities on Day 2

All activity-based slides have a star. This means the facilitator should not simply present the information, but instead should engage participants to generate the answers. Each activity slide is described further below.

- **Activity J. Recommendation reflections.** This activity is the opportunity for small groups or individuals to share their responses to the first homework assignment (described under Activity E). One of the facilitators should call on each group by name (e.g., "Mary and John, you had recommendation #1, could one of you please share your reflections?") and give a maximum of two minutes to share their responses. As a reminder, the homework asked each group to: (1) describe this recommendation, (2) share how your program is already using this recommendation, and (3) how the program could use this recommendation.
- **Activity K. Menti Day 1 recap.** Use Menti to develop a survey question in advance. This is described under "Online preparation for Day 2." When displaying the question, provide the link to Menti and the code in the chat.

  While the group is answering, ask someone to unmute and explain their answer. Highlight that this threat is indirect because it is not at you, but is direct at someone in the same occupation or organization as you, so you are also likely to feel threatened. If numerous participants give the incorrect answer, return to slide 27, "Threat types," to remind the group of definitions for each threat type.
- **Activity L. What does a potential attacker need?** This activity asks participants to consider what an attacker needs to be able to successfully harm a target. This could be in a virtual or a physical space. Ask participants to type their answers into the chat. Then, call on individuals to clarify or expand on their responses. For example, if someone writes that the attacker would need a "cause," you can clarify that this refers to a motive.
- **Activity M. Scenarios.** This activity allows participants to think about how they could use their knowledge of what an attacker needs to prevent attacks from occurring. For each scenario, you'll read (or ask a participant to read) the scenario. Then, ask three or four volunteers to explain what could be done. Individuals who are not called upon are welcome to type into the chat. After getting their answers, go to the next slide and review some of the options.
- **Activity N. What do these solutions have in common?** This activity is an opportunity for participants to see the importance of the organization taking the lead in worker security. Show the slide with the four slide images and ask for a volunteer to explain what these four scenario solutions have in common. If a clue is needed, say that you are looking for commonalities in terms of who has the biggest role to play in limiting access, information, motive, and impunity.

  Once a volunteer responds, advance the slide to show the red circles. Explain that the commonality in each case is the organization with the largest role to play.

  Advance again and review the text of the slide.

- **Activity O. What devices are you using and what do they say about you?** This opportunity for reflection gives participants the chance to think about what devices they use and what others could learn about them from that use. Ask participants to use the Menti.com survey to answer the questions under "Online preparation for Day 2." After they have completed both questions, note that we all use a range of devices every day and that more and more of our most private information is available online if others know how to access it. So, it is up to us to use these devices as safely as possible, which is what we will talk about now.
- **Activity P. What are we sharing on social media?** This brief brainstorm is done via chat. Ask participants to reflect on which social media platforms they use and what they share. Ask a few people who write in the chat to unmute and elaborate on their answers. Close the conversation by noting how much we share online.
- **Activity Q. What could someone learn about me from these social media posts?** This activity asks participants to analyze Facebook posts to determine what kinds of information could be gained about the person posting. The slides in the generic slide deck include posts from the training author's Facebook page. The facilitators should replace them with their own social media posts (being careful not to share anything that they do not wish to have known). The facilitator should ask a few volunteers to note what could be learned about the person from their posts. Those in the generic deck could indicate:
    - That the person posting voted in 2020 and where voting occurs (which could give information on where they live)
    - That the person posting has children and what those children look like
    - That the person posting supports LGBT rights
    - If you clicked on the GoFundMe link, you could learn how much the person donated unless they did so anonymously

  End by stressing that it is important to think critically about what you share, especially because it could be shared further than with those you intended.
- **Activity R. Have you used any of these methods?** If there is time for reflection, a powerful activity is hearing individuals' experiences using these different options to deal with online harassment. Ask if anyone wants to share this information, but do not obligate anyone. If someone speaks up, thank them for their willingness to share this experience with the group. Stress that they did not deserve to be treated this way and that experiences like theirs can be very difficult.
- **Activity S. Linking problems to solutions.** This activity allows participants to think about high and low technology options for solving their digital security issues. Read problem #1 and ask participants to use the chat to suggest which of the "solution options" would be a good fit. Select a few respondents to explain their choice. Then, advance the slide to show the solutions. Do the same for problem #2 and problem #3.

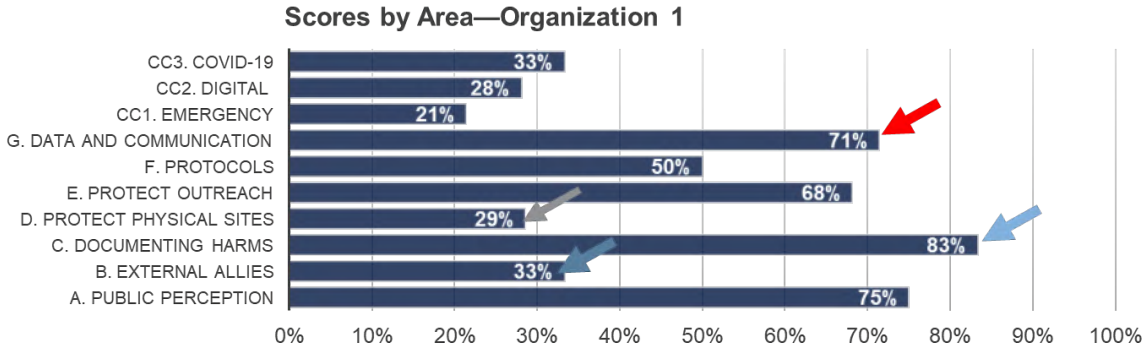
After completion, note that many solutions can help mitigate or solve multiple problems. For example, for problem #3:

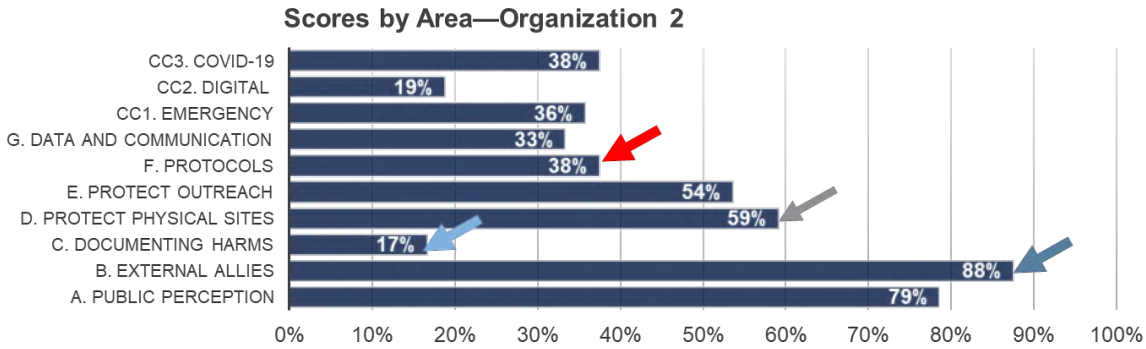
- If peers do not share their photos, names, or locations, they are hard to identify (making them harder to blackmail).
- If peers have scripts that help them respond to sexual advances, they may not make clients angry, which could remove a motivation for blackmailing.
- If you use a closed Facebook group, there is less impunity because everyone is known to at least one other group member. You can also be more careful about who is invited to begin with.
- Sharing photos and identification of habitual harassers means fewer peers will deal with these individuals, limiting their risks.
- Having a clear policy on this topic can prevent romantic relationships from beginning, limiting motivation for blackmail if the relationship does not work out.

- **Activity T. IP teaching assignments.** This is another homework assignment for the group. Please copy each organizations' score summary graph into the presentation.

  "Activity T (part 1)" is the example slide. If you need to use multiple slides to fit all the graphs, please do so. Depending on sensitivities in the group, you may decide to post these graphs without the organizations' names.

  You should have selected, in advance, which IPs would teach each skill by looking at their comparative strengths per the checklists. For example, if you were doing this training for Organizations 1 and 2 below, you would assign Organization 1 to teach area C because of their relatively high score (both compared to their other scores and compared to Organization 2's score in area C). You would assign area B to Organization 2, again because it is one of their strongest areas and a big weakness for Organization 1.





In this session, share the assignments and give instructions for how the assignments should be completed. To assign each IP to an area, adjust the green text on the "Activity T (part 2)" slide.

During the session explain that all IPs are assigned to a specific domain. They should go back into the checklist and look at that domain. There is an example of this on "Activity T (part 3)" slide. They will see that all domains include several strategies. The IP should choose at least one strategy from their assigned domain to teach to the group. This includes developing slides and planning a 10-minute presentation.

As the facilitator, make sure that the date and time of Day 3's session, when these presentations will be made, is also on the slide.

- **Activity U. Day 2 closing.** The daily evaluation can be done publicly using Menti, by showing your screen as survey results come in. Alternatively, you can leave the survey open as the session ends and then check the responses on your own without sharing the screen. Sample questions are included under "Online preparation for Day 1."

  After the session ends, share the slides with all participants and remind them of their assignments. A sample email to send after Day 2 can be found in Annex G.

Day 3 – Special Session

Time	Session	Objectives
As needed	Group presentations	● Share a security strategy assigned to your CSO. ● Ask questions about all presented strategies to gain understanding of implementation, and pros and cons of the strategy.

Online preparation for Day 3

There is no online preparation required in advance of Day 3. The participants may wish to share their presentations with the facilitator so that the facilitator can project them during the presentations.

Instructions for activities on Day 3

- **Activity V. Implementing partner presentations**. This session is devoted to presentations by each implementing partner, followed by questions from other participants. The facilitator should track time to ensure every organization gets the chance to present for roughly 10 minutes, followed by five minutes of question and answer. The facilitator should offer to project from their own screen if the presenting groups struggle with connectivity. This requires that the facilitator have the slides in advance of the session. If the facilitator does not have all slides before the session begins, they should collect slides at the end of the session. Unless there are security concerns, all collected slides should be circulated to the group.

  At the end of the session, the facilitator should mention the incredible resources that we are for one another as we all build our security capacity. After the session, the facilitator should share all the implementing partner slides. An example email for the end of Day 3 is in Annex H.

Day 4

Time	Session	Objectives
8:00	Day 2 recap and special session reflections	● Reflect on strategies presented during the special session ● Remember the topics covered on Day 2
8:10	Using what you've learned: security challenge case studies	● Brainstorm what your organization could do if faced with a variety of security challenges. ● Discuss whether the "possible solutions" after each scenario would be appropriate in the local context.
8:45	Risk assessment formula	● Become familiar with the formula for determining the likelihood that a given harm will occur.
9:05	Security planning	● Recognize the elements of a security plan and practice using the template to develop your own plans. ● Identify your top three risks and create a security plan for each by considering vulnerabilities, existing capacities, and needed capacities.
9:35	Next steps	● Discuss opportunities for: immediate no and low-cost action, continued cross-CSO learning, linking security activities into ongoing violence prevention and response, and seeking international support. ● Identify action steps to finalize and build buy-in for security plans at each CSO.
9:50	Reflections and closing	● Share thoughts on and evaluate the workshop; provide closing reflections.

Online preparation for Day 4

- Create two questions on Menti. Note that stars show correct answers and should be removed.

  Question 1. What does an attacker need to harm us? (select all that apply)

  A. Motive**
  B. Resources**
  C. Supporters
  D. To see us face-to-face

  Question 2. What can we do to protect ourselves online?

  A. Do not share information that we do not want a potential attacker to have.**
  B. Use strong passwords.**
  C. Use safer texting apps, like Signal, instead of WhatsApp.**
  D. Update security software, like antivirus protection programs.**

- Create a post-test using Google Forms (example of post-test in Annex J; answer key to post-test in Annex K).
- Create an evaluation using Google Forms (example in Annex L).

Instructions for activities on Day 4

All activity-based slides have a star. This means the facilitator should not simply present the information, but instead should engage participants to generate the answers. Each activity slide is described further below.

- **Activity W. Key takeaways.** This activity allows participants to think about how they will apply what they learned from their colleagues. The facilitator should ask for two to three volunteers to share what they learned during the last session and, most importantly, how they will use what they learned at their own organization.

  After sharing occurs, the facilitator should stress again that we all bring a lot of practical knowledge to this work, and we can always learn from one another. Depending on project need, the facilitator could also help organize a Signal group to discuss security challenges and solutions going forward.

- **Activity X. Remembering Day 2.** This slide can quickly remind the group what was covered in Day 2. Questions can be found in "Online preparation for Day 4."

  Ask everyone to go to Menti.com (put the link and code in the chat). After they have answered the first question, ask a volunteer to explain their thinking. Then show the correct answers.

  During the discussion of correct answers for the first question on what an attacker needs, note that C is not correct because an individual can act alone, and D is not correct because attacks can also occur online.

  Then go to the next question on online protections. Again, ask that everyone complete the survey online and then ask for a volunteer to explain their thinking. Then mention that all answers are correct. Each of these can help keep us safer online.

- **Activity Y. Using what you've learned.** In this activity small groups will work together in either breakout rooms, by phone, or in person (if they are gathered in small clusters). Each organization should be assigned to a case study/scenario. Paste all case studies in the chat for easy reference. If there are fewer groups than there are case studies, select those case studies that you think are most relevant to the context. For example, you may assign IPs to only case studies 3, 5,7, and 8.

  Tell the group that they should take their case study and consider two questions. First, what can this organization do now? Second, what could they have done—before this issue occurred—to mitigate or prevent the harm caused?

  Explain that they will have five minutes to discuss, and then you will call on each group to share their thoughts. After that, you, as the facilitator, will share some possible solutions for their comments.

After five minutes, move to the next slide on scenario 1 and ask the first group to present. If no group was assigned scenario 1, answer the question yourself by going to the next slide to review the possible answers. Do the same thing for each scenario.

At the end, congratulate all of the teams and reinforce that they have answers to tricky problems. All security is contextual, and they know their contexts better than anyone else.

- **Activity Z. Reflections on the scenarios.** This activity helps participants understand that it is not just *what* you do, but also *when* that affects security. Read the question on the slide, and ask for a few volunteers to unmute and answer. After receiving several answers, advance the slide and review the answers.
- **Activity AA. Risk assessment example.** Risk assessment formulas appear complex because they seem like complicated math problems. However, this formula is a tool to help participants think about the relationships between vulnerabilities and capacities and does not have to be used with actual numbers. The formula is also a tool for bringing together all the content that has been presented throughout the training. This activity makes risk assessments more concrete by presenting a specific example and allowing participants to generate their own ideas on how to decrease vulnerability and increase capacity.

  On the first Activity AA slide, the question "What could you do to reduce vulnerabilities and increase capacities?" appears at the bottom. Give participants a few minutes to think about this and then call on two to three people to answer. After receiving answers, go to the next Activity AA slide. The second slide shows possible solutions for removing vulnerabilities in red and adding capacities in blue. There is one removed vulnerability so a "-1" appears next to vulnerabilities. Four ways to increase capacity appear, so a "+4" appears next to capacities.

  If participants suggest that some vulnerabilities, such as outreach at night, should also be removed, let them know that each program will have to decide what is appropriate based on their individual context. In this example, the program may have felt that conducting outreach only during the day was too restrictive or would limit program beneficiaries' access to services too much.

- **Activity BB. Local example.** In this activity, the facilitator will walk the group through a real-life example. Ask a volunteer to share a risk they are concerned about. One person (or one organization) will be filling in most of this chart as all information should be connected to the original risk. Fill in the slide using the information they provide on risk, threats, vulnerabilities, and existing capacities. When you come to required capacity, ask the person/organization who has been filling in the chart to give some initial ideas on what could be done. Then open it up to the group to add their ideas.

  Note that the individual or organization may not wish to use all the ideas under required capacity, but this gives them a menu of options to choose from when they create their own security plan.

- **Activity CC. Your priority risks.** In the virtual training, this activity is likely to be assigned as post-training work in small organizational groups. This is the chance for organizations to decide which risks they think are most important to address. The risk assessment formula can be used to make this decision. After they have decided on the three most important risks to address, they should develop a security plan for them. The security plan template will be shared in the email that goes out after the Day 4. See Annex I for an example.

  If you are conducting this workshop in person, it is ideal to give time for organizations to work on their security plans while everyone is together. Then, they can present them to other participants for feedback, further improving their final products.

- **Activity DD. Action planning**. This step allows organizations to convert their security plans into action plans. Once you have reviewed their security plans and provided feedback, have each IP fill out the table (shared in the email after the final session) and send it back to you by email. Then you can track their progress and help them stay on schedule. You can also use the information about required resources to highlight security-related needs in conversations with the donor.

  The speakers' notes for this slide also make the incredibly important point that if those who have been trained wish to share what they have learned with others, they first need to make substantial changes to the training itself. The training is designed to help organizational leaders make their organizations safer places to work. This is largely accomplished by creating protocols and policies for workers to follow and then sensitizing workers on these documents. Thus, if those who have been trained wish to share this training content with others, it should be done only after the organizational leaders have created the relevant policies. Then the training should be revised to reflect those policies/protocols and used to build workers' understanding of the policies and how the policies/protocols should influence their actions.

- **Activity EE.** Use the Google Forms you created in advance, from the content in Annex J and Annex L, to give participants the chance to evaluate the training and demonstrate their knowledge.
- **Activity FF. In your own words.** Using Menti.com, ask participants to enter a few words that describe how they are feeling at the end of the training. As desired, ask a representative from each organization to share a more in-depth response about the content of the training and how it will inform their thinking and actions going forward.

  After the final day's workshop is over, send an email to the group (a sample is in Annex I). The email should include the attachments Annex M (security plan) and Annex N (action plan).

Annex A: Instructions to complete the checklist

Who should complete the checklist?

The checklist should be completed by implementing partner members who will attend the security training. The checklist should be completed in a safe and private space where it is possible to speak openly. Because the checklist is designed to inform policies and procedures governing activities wherever program design, implementation, and monitoring occurs, the team completing the checklist should visit 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. For example, some sections should be filled out by lead agencies (such as principal recipients of The Global Fund or international nongovernmental organizations [INGOs] coordinating several implementing partners' activities) as well as organizations that are implementing activities (such as Global Fund subrecipients and USAID implementing partners). Other sections, such as D, which covers safety at physical locations, should only be completed by those who implement activities directly and should be done individually for each site instead of at an organizational level. This is further discussed in the box **How can collaborating organizations and regional networks work together to meaningfully complete the checklist?**

How can collaborating organizations and regional networks work together to meaningfully complete the checklist?

The rationale for having different organizations complete different sections of the checklist is that not all strategy types are relevant to each organization, and organizations working together can complement one another. Especially in the context of an umbrella organization and several implementing partners all working on the same objectives, the way an organization completes the checklist may be dependent on their collaborators' approaches to security. For example, if a lead organization has asked all implementing partners to direct journalists' questions to the Ministry of Health, then each implementing partner will simply mark questions such as "Does the organization have a designated member for talking to the media?" with "not applicable" because they do not need to have someone designated to speak to the media based on the approach used by the lead organization.

Regional networks may be unsure which components of the checklist to complete. Central leadership of such regional networks will likely benefit from completing the sections indicated as for "the organization leading the project" while their member agencies may wish to fill out the components indicated as for "individual organizations implementing activities." They can then look at their collective results to determine where the network would like to focus their energies to fill gaps as well as share good practices across organizations.

How should the checklist be completed?

For all those completing the various sections of the checklist, please read each question in Column B. If the question requires further clarification, refer to Column C. After each question put a "1" under either yes, no, somewhat, or not applicable 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 1 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 1 under "no."
- **Somewhat:** This answer indicates that the organization has used this strategy in the past but is not currently using it, or that the strategy is only partially employed. For example, under question 1—"Does the organization take actions to be visible to the public, portraying a positive image?"—if the organization only does public activities in some of the districts where it implements or previously had a publicity campaign that is no longer operational, they would put a 1 under "somewhat."
- **Not applicable:** This answer indicates that this strategy is not relevant or useful to the organization. For example, under question 1—"Does the organization take actions to be visible to the public, portraying a positive image?"—some organizations do not wish to be visible in any way because they feel that visibility may result in harm. In this case, avoiding public visibility is a well-thought-out choice, and they would choose "not applicable" because this strategy is not useful to them. Activities that are irrelevant, such as questions on outreach for an organization that only delivers services at a clinic, would also be marked as "not applicable."

In the column following the yes/no/somewhat/not applicable responses, there is room for the person(s) completing the checklist to explain their answer under "notes." See the box **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.

How can scores be interpreted?

Each “yes” answer awards a full point to the organization, “somewhat” awards a half point, “no” awards zero points. An answer of “not applicable” does not affect the score positively or negatively. Beyond each lettered section, A–G, there are cross-cutting scores for Emergency Preparedness, Digital Safety, and COVID-19. When you fill out the checklist, consider that this tool is designed for your own personal use and your scores will only be shared if you choose to make them available to others. See the box **Getting the most out of the checklist** for additional information.

Getting the most out of the checklist

This checklist is designed to be useful to implementers. If a strategy is not useful or relevant to your organization, marking it as “not applicable” will not impact your score and will allow you to focus only on those strategies that you think would be beneficial to employ. What you mark as “no” or “somewhat” is also not a reflection of a failure. Many of these important components of security have not been contemplated or funded in HIV programs. You can use low scores (which will result from selecting “no” and “somewhat”) to work with your funder and organization to highlight areas for growth while high scores may indicate that your organization could provide technical assistance or guidance to others embarking in this new area.

Your scores are presented as a graph on the second tab of the Excel document, “Responses Graph.”

Annex B: Sample in-person participants' agenda

Please note that the in-person participants' agenda is ***not*** accompanied by a corresponding in-person facilitators' agenda as the modifications made to host this training in person should be determined locally. This sample agenda is meant for illustrative purposes. It helps those contemplating an in-person event incorporate time for activities assigned as homework in the virtual training that could be given as small group work during in-person meetings. For example, in the virtual version, participants are asked to discuss the key recommendations as homework and then present their feedback on Day 2. In this agenda, time is built in for this activity to occur during the "Key terms and overarching recommendations" session instead of as homework.

Time	Session	Objectives
	DAY 1	
8:00	Welcome, introductions, and background	● Welcome all participants and introduce participants to one another. ● Come to a shared understanding of training content and goals as well as participants' involvement in the training. ● Identify implementer security as an important and new area of HIV programming.
8:45	Key terms and overarching recommendations	● Define security, risk, threat, capacity, and vulnerability, and discuss the key recommendations for security of implementers in KP programs.
10:15	Break	
10:45	Threat identification and assessment	● Identify threats and determine their seriousness.
12:30	Lunch	
1:30	Limiting an aggressor's capacity to harm	● Describe what can be done, and by whom, to limit an aggressor's ability to cause harm.
2:15	Digital security	● Describe the vulnerabilities inherent to digital platforms; identify risk-reduction strategies within each.
3:15	Review of our capacities and plan for skill sharing	● Review collective responses to the security assessments. ● Assign each implementing partner to a skill to be presented in the next session.
4:00	Closing	● Complete Day 1 evaluation

DAY 2		
8:00	Recap Day 1	● Review the content from Day 1
8:30	Group presentations	● Share a security strategy assigned to your CSO. ● Ask questions about all presented strategies to gain understanding of implementation, and pros and cons of the strategy.
10:00	Break	
10:30	Continue group presentations (as needed)	● Share a security strategy assigned to your CSO. ● Ask questions about all presented strategies to gain understanding of implementation, and pros and cons of the strategy.
11:00	Using what you've learned: security challenge case studies	● Brainstorm what your organization could do if faced with a variety of security challenges. ● Discuss whether the "possible solutions" after each scenario would be appropriate in the local context.
12:30	Lunch	
1:30	Risk assessment formula	● Become familiar with the formula for determining the likelihood that a given harm will occur.
2:00	Security planning	● Recognize the elements of a security plan and practice using the template to develop your own plans. ● Identify your top three risks and create a security plan for each by considering vulnerabilities, existing capacities, and needed capacities. ● Present your security plans to the group for feedback (optional, depending on time available)
3:45	Next steps	● Discuss opportunities for: immediate no and low-cost action, continued cross-CSO learning, linking security activities into ongoing violence prevention and response, and seeking international support. ● Identify action steps to finalize and build buy-in for security plans at each CSO.
4:15	Reflections and closing	● Share thoughts on and evaluate the workshop; provide closing reflections

Annex C: Facilitator's agenda for virtual training

Time	Session	Objectives	Materials
		DAY 1	
8:00	Welcome, introductions, and background	● Welcome all participants and introduce participants to one another. ● Come to a shared understanding of training content and goals as well as participants' involvement in the training. ● Identify implementer security as an important and new area of HIV programming.	● Slides ● Menti ● Handout: Instructions to complete checklist (Annex A)
8:45	Key terms and overarching recommendations	● Define security, risk, threat, capacity, and vulnerability, and discuss the key recommendations for security of implementers in KP programs.	● Slides ● Handout: Cheat sheet (Annex D)
9:15	Threat identification and assessment	● Identify threats and determine their seriousness.	● Slides ● Handout: Security incident log (Annex E)
9:55	Day 1 closing	● Evaluate the day.	● Slides ● Menti
		DAY 2	
8:00	Recap of Day 1 and HW #1	● Share HW #1 answers. ● Remember the topics covered on Day 1.	● Slides ● Menti
8:25	Limiting an aggressor's capacity to harm	● Describe what can be done, and by whom, to limit an aggressor's ability to cause harm.	● Handout: Cheat sheet (Annex D)
9:00	Digital security	● Describe the vulnerabilities inherent to digital platforms; identify risk reduction strategies within each.	● Slides
9:40	Review of our capacities and plan for skill sharing	● Review collective responses to the security assessments. ● Assign each implementing partner to a skill to be presented in the next session.	● Slides ● Excel checklists
9:55	Day 2 closing	● Complete Day 2 evaluation	● Slides ● Menti

DAY 3 - Special Session, Group Presentations			
As needed	Group presentations	● Share a security strategy assigned to your CSO. ● Ask questions about all presented strategies to gain understanding of implementation, pros, and cons of the strategy.	● Slides from CSOs
Time	**Session**	**Objectives**	**Materials**
DAY 4			
8:00	Day 2 recap and special session reflections	● Reflect on strategies presented during the special session ● Remember the topics covered on Day 2	● Slides ● Menti
8:10	Using what you've learned: security challenge case studies	● Brainstorm what your organization could do if faced with a variety of security challenges. ● Discuss whether the "possible solutions" after each scenario would be appropriate in the local context.	● Slides
8:45	Risk assessment formula	● Become familiar with the formula for determining the likelihood that a given harm will occur.	● Slides ● Handout: Cheat sheet (Annex D)
9:05	Security planning	● Recognize the elements of a security plan and practice using the template to develop your own plans. ● Identify your top three risks and create a security plan for each by considering vulnerabilities, existing capacities, and needed capacities.	● Slides ● Handout: Security plan template (Annex M)
9:35	Next steps	● Discuss opportunities for: immediate no and low-cost action, continued cross-CSO learning, linking security activities into ongoing violence prevention and response, and seeking international support. ● Identify action steps to finalize and build buy-in for security plans at each CSO.	● Slides ● Handout: Action planning template (Annex N)
9:50	Reflections and closing	● Share thoughts on and evaluate the workshop; provide closing reflections	● Slides ● Menti

Annex D: Security training cheat sheet

Overarching security recommendations

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 key population 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 programs for key populations should never be assumed or left to chance. Ideally, both should be contemplated from the proposal stage of a project in the risk assessment portion as “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 key populations.

As such, security activities should have specific budget line items. Such safeguards are not a luxury or added extra, but a necessity. When activities to promote safety and security 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 guidance—such as the World Health Organization guidelines and key population implementation tools—that prevention and action in response to violence against key populations is a *critical enabler* of effective responses to HIV.

Worker mental health is of particular importance to organizational security efforts and should be resourced and programmed for explicitly. Implementing activities for an HIV program brings with it a unique set of mental health strains. Beyond the violence and abuse that can be perpetrated against implementers for their work, they also meet daily with beneficiaries who have needs that often far exceed the capacity of the organization. Being unable to meet needs for basics such as safe housing and nutritional support takes a toll on workers' mental health, and organizations must make investments in worker mental health to avoid burnout and negative outcomes, such as substance abuse.

3. Make a safe workplace the employer's responsibility.

Many gaps must be addressed to ensure a safe and secure environment for key population 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 ensure the safety and security of their employees (e.g., guidelines provided by the International Labour Organization). 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.

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.

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.

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. 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 than 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. 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 key population members 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 key population 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, transgender, or cis male with more feminine gender expressions may be especially vulnerable to gender-based violence (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.

▶ **Age.** For example, there may be power dynamics within the organization that favor older or younger workers. A workers' 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 population groups.** For example, staff members working with specific groups (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 population members 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* key population programs.** For example, safety issues may be different when doing outreach with men who have sex with men at hot spots, in residences, or online.
- ***Multiple* vulnerabilities.** For example, workers that support individuals who belong to more than one group may be vulnerable to multiple safety and security challenges and require a unique set of responses. For instance, workers who interact with 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, psychological) and security strategies holistically.**

Safety and security challenges in key population 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. 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.

▶ **Flexible**—Having the potential to modify plans and adapt quickly and effectively, such as in response to a sudden change in the security environment.

10. **Be together, work in coalition, and learn from one another.**

Be aware of safety and security as a collective. While each key population 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.

Key definitions

- **Security:** the state of being free from risks or harm that come from intentional violence
- **Risk:** the probability that something harmful will happen
- **Threat**: indication/sign that someone wants to hurt, damage, punish us; these come from the outside
    - **Direct threat** – An indication that someone wants to inflict pain or damage me specifically, e.g., “I will attack you because you are a sex worker.”
    - **Indirect threat** – An indication that someone wants to inflict pain or damage a broader group of people that I am a part of, but ***not me/my organization specifically***, e.g., another sex worker feels threatened based on the above threat even if it was not made to him/her.

- **Security incident** – Situations that we see happening, but we are unsure if they are a threat or more of a coincidence, e.g., your computer is stolen. Is this targeting you to get information about what you are doing or to steal your contacts? Or is this just an opportunistic theft?

- **Capacity:** any resource (financial, ability, contacts, infrastructure, personality, etc.) that we can use to improve our security
- **Vulnerability:** anything that increases our exposure to those who want to hurt us

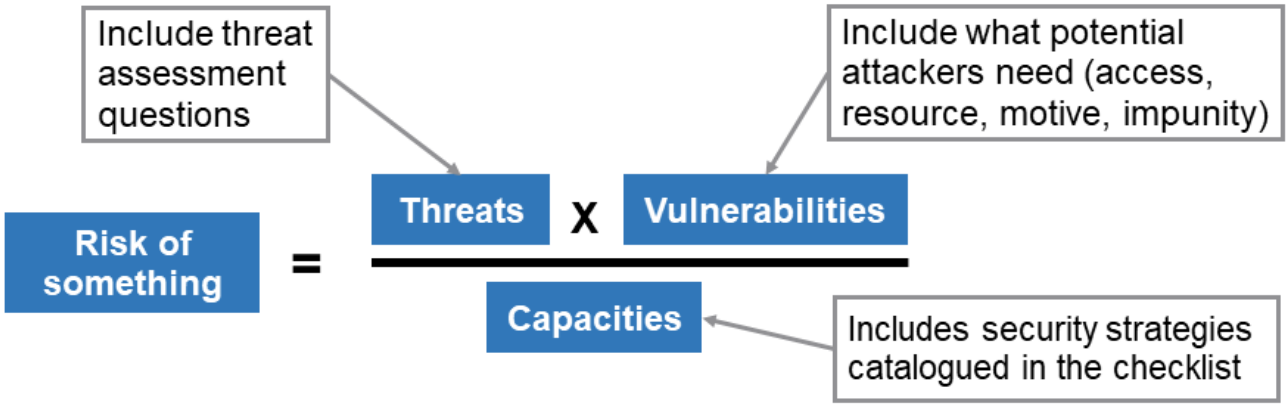
Questions to assess the danger of a threat

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

What does an attacker need to be successful?

- **Access:** to you physically or electronically
- **Resources:** anything that can be used to carry out the attack – information on the victim location, weaknesses; weapon; transport; money
- **Impunity**: a lack of consequences for the attacker, legal and/or social
- **Motive:** a reason to cause harm

Formula to calculate risk



Security protocol

- Security plans take time to implement. We need to come up with steps to take now to deal with issues when they occur. The solution to short-term needs is a security protocol.
- First, we need to come up with levels—green (normal), amber or orange (indications that an attack could be carried out), red (extreme likelihood of attack)—and then think about what to do as it relates to: staff, programs, and premises.

Here is a sample security protocol.

	Staff	Programs	Premises
Green	No restriction	No restriction	Normal security procedures
Amber	1. Staff deemed most at risk (defined/determined in advance) do not come to work or do not work in public spaces 2. Reminder sent to all staff about who they should inform in case of emergency 3. Alert trusted neighbors and allies of the situation ("hey, we think it's OK, but let us know if you see something strange") 4. Alert organizational lawyers	1. Extremely sensitive activities or those occurring in hostile environments (determined in advance) are put on hold 2. Non-sensitive activities continue as normal 3. Alert donors 4. Alert beneficiaries to the situation and ensure they follow any required security measures (e.g., we will no longer host large events until further notice)	1. Contract a short-term security guard for surveillance during office hours 2. Visitors must be pre-vetted to access office premises (no unannounced visitors) 3. Staff are reminded to check that no sensitive information is easily accessible (digital and physical) 4. Move contingency funds so they can be easily accessed (maybe on ATM cards, maybe within Western Union)
Red	1. Staff deemed "most at risk" will temporarily relocate (with staff and relocation sites defined in advance) 2. Other staff do not come to the office 3. Organizational allies are informed and mobilized 4. Organizational lawyers are alerted	1. Temporarily suspend all project activities 2. Inform organizational donors that projects have been suspended 3. Communicate suspensions to beneficiaries	1. Lock the office (staff responsible for locking office determined in advance) 2. Contract security guard for surveillance during and after office hours 3. No visitors allowed on premises

Annex E: Security incident log

Implementer security incident log			
	Question	**How to Answer**	**Response**
1	Security incident number	Begin with number 1 and continue; the numbering allows security incidents to be linked to one another (see question #14)	
2	Date of incident	Type as YEAR-MONTH-DAY (e.g., 2019-02-17 for February 17, 2019) to organize this security event log by date	
3	Time of incident	Specific time of day (if known), or more general (morning, afternoon, evening, night)	
4	Perpetrator	If known and safe to list, or use a more general term such as "law enforcement officer"	
5	Affected organization	Name of HIV program implementing partner (i.e., community-based organization's name)	
6	Target	Specific person or type of staff, physical space (e.g., name of a specific hot spot), website, database, etc. Do not name individuals here unless you have their permission to do so.	
7	Where incident occurred	Physical address, online, by phone, etc.	
8	Believed motivation of aggressor (if known)	For example: intimidation, to stop programming, to deflect attention from other local issues	
9	Description of security incident	For example: Facebook posts on project page said "[paste specific message here"]; or peer educators were arrested without charge when distributing condoms to a group of MSM during a mobile HIV testing event	
10	Programmatic consequences of security incident	For example: Implementing partner will conduct only online outreach until physical outreach is considered safe to conduct	
11	Description of actions taken to respond to security incident	For example: On YEAR-MONTH-DAY, implementing partner targeted in Facebook post decided that it is not safe to conduct outreach activities for a two-week period and implementing partner filed a complaint with the police. On YEAR-MONTH-DAY, local Ministry of Health officials held a meeting with power holders and local law enforcement; they discussed threats to the implementing partner and created a WhatsApp group that can be used to notify and activate allies immediately as needed. Please include dates of actions taken (and continue to update this row as actions are taken).	

Implementer security incident log			
	Question	**How to Answer**	**Response**
12	Was the security incident related to index testing?	Select one: Yes, No, or Unsure	
13	Was the security incident related to COVID-19?	Select one: Yes, No, or Unsure	
14	Which other security incidents is this related to? (if any)	Note whether this incident was related to other security incidents by listing other security incident numbers here.	
15	Incident resolution (if any)	For example: On YEAR-MONTH-DAY, peer educators were released from state custody and provided with mental health support.	

Annex F: Sample post-session 1 email

Dear team,

Thanks for your great participation today. Attached are:

1. Slides from today's session
2. The cheat sheet that will help you complete your homework and understand key concepts from throughout the training
3. The security incident log for use by your organization

You can find a recording of today's session here: PROVIDE URL

Please remember that you have been tasked with reviewing one of the overarching recommendations and sharing the following at the start of next session: (1) a summary of the recommendation, (2) how you are currently using the recommendation, and (3) how you could use the recommendation going forward.

We look forward to seeing you at Session 2 on X date at Z time!

Facilitators' names

Annex G: Sample post-session 2 email

Thanks for your great participation today. Attached are:

1. Slides from today's session

You can find a recording of today's session here: PROVIDE URL

Please remember that each CSO has been tasked with teaching a specific skill during our next session at X time on Y date. The assignments are described in the slides (provide slide numbers). If you would like me to share your slides on my screen so that you do not need to share your screen during our session (this could be especially important if you struggle with connectivity), please send them to me in advance.

We look forward to seeing you for our special session 3 on X date at Z time!

Facilitators' names

Annex H: Sample post-session 3 email

Thanks for your great participation today. Attached are:

1. Slides presented by all implementing partners

You can find a recording of today's session here: PROVIDE URL

We look forward to seeing you during our final session on X date at Z time!

Facilitators' names

Annex I: Sample post-session 4 email

Thank you to everyone for being part of this important workshop! We have all learned so much together. Attached to this email you will find:

1. The complete slide deck, including slides shared by CSOs during session 3
2. A security plan template
3. An action planning template
4. A one-pager on available emergency resources
5. Guidance on developing standard operating procedures on security for HIV program implementers working with key populations

You can find a recording of today's session here: PROVIDE URL

Please remember that all of you should submit your security plans for review to X person by Y date. We will send you feedback and also help you think about resource mobilization for activities that cannot be done with little or no cost.

Thank you again for your attention, participation, and energy. We look forward to supporting you as you move forward with implementer security.

Facilitators' names

Annex J: Post-test

This test can be entered into Google Forms to collect answers electronically. For information on using Google Forms, click here: https://support.google.com/docs/answer/6281888?co=GENIE.Platform%3DDesktop&hl=en.

We recommend making each of the questions below required. This can be done by selecting the “required” button in Google Forms.

1. Which of these phrases best describes “security”?
    a. Freedom from intentional harm
    b. Safety from medical errors, such as needle sticks
    c. Being prepared to face natural disasters, such as flooding
    d. All of the above

2. Why is it important for an organization to track security incidents (e.g., arrests of peers, attacks on the organization’s reputation on social media, threatening graffiti on a drop-in center)?
    a. The organization can identify trends, such as increasing attacks, and make plans that take these trends into account. For example, pausing outreach in certain areas.
    b. The organization has a record that can be shared with the donor to explain changes in performance.
    c. The organization knows which cadre of its workers is most at risk and can assign additional resources to protect them.
    d. All of the above

3. Select true or false for each statement below.
    - An organization is responsible for creating a secure environment for its workers.
    - It is sufficient for an organization to tell its workers to "use their best judgment" without giving specific guidance.
    - Online outreach workers should always share their full names (first and last).
    - Passwords should be used on all office and personal computers.
    - Staff burnout can be a consequence of security incidents.
    - Having a sexual harassment policy makes an organization more secure.
    - All organizations serving key population members should engage with the police.
    - Sharing a photo of yourself online may give an attacker information to use against you.
    - Working with religious leaders may help protect an organization.
    - Having a media spokesperson can protect an organization from harm.

4. A threat is a sign that someone wants to harm or punish another person. Which of the following questions helps you understand the seriousness of a threat to your program/organization?
    a. Who is making this threat?
    b. Is this a series of threats that has become more frequent or systematic over time?
    c. How serious do you feel the threat is?
    d. What is the objective of this threat?
    e. All of the above

5. Which of the following is correct?
    a. We should remove all vulnerabilities to limit the risks to our programs.
    b. Some vulnerabilities cannot be removed; the most important thing to do is be aware of vulnerabilities.
    c. Vulnerability is the same thing as weakness.

6. What do you need before you can develop a security plan?
    a. An understanding of the most serious threats to your organization.
    b. An understanding of your existing security capacities.
    c. An understanding of your current vulnerabilities.
    d. Funding to implement the plan.
    e. All of the above.
    f. A, B, and C.

Annex K: Post-test answer key

1. A
2. D
3. True or False (see each statement)
    - An organization is responsible for creating a secure environment for its workers. (TRUE)
    - It is sufficient for an organization to tell its workers to "use their best judgment" without giving specific guidance. (FALSE)
    - Online outreach workers should always share their full names (first and last). (FALSE)
    - Passwords should be used on all office and personal computers. (TRUE)
    - Staff burnout can be a consequence of security incidents. (TRUE)
    - Having a sexual harassment policy makes an organization more secure. (TRUE)
    - All organizations serving key population members should engage with the police. (FALSE)
    - Sharing a photo of yourself online may give an attacker information to use against you. (TRUE)
    - Working with religious leaders may help protect an organization. (TRUE)
    - Having a media spokesperson can help protect an organization from harm. (TRUE)
4. E
5. B
6. F

Annex L: Example evaluation

1. **The content of this training is interesting.**

   strongly disagree — strongly agree

   1 2 3 4 5

2. **The content of this training will help me to do my job.**

   strongly disagree — strongly agree

   1 2 3 4 5

3. **I can share what I learned today with others.**

   strongly disagree — strongly agree

   1 2 3 4 5

4. **I would recommend this training to others.**

   strongly disagree — strongly agree

   1 2 3 4 5

5. **The facilitator's speed is:**

   a. Too slow b. About right c. Too fast

6. **Please share any concerns you have about sharing this training with others.**

7. **I could successfully use the technology (e.g., Zoom, Teams, Mentimeter, Google Forms) employed in this training.**

   strongly disagree — strongly agree

   1 2 3 4 5

8. **Please share anything else you think is important for the facilitators to know.**

Annex M: Security plan

Risk of something:			
Threats	**Vulnerabilities**	**Existing capacity**	**Required capacity**

Annex N: Action plan

#	Top 10 capacities to build	Requires additional monetary resources? (Y/N)	When will capacity be fully built?	Main person(s) responsible
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				