JOURNEYING TOGETHER TOWARDS PROTECTION: TRAINING MEETINGS AND WORKSHOPS

> CHAPTERS 2.1, 2.2, 2.3 OF THE NEW PROTECTION MANUAL
FACILITATORS OUGHT TO MASTER THESE BEFORE READING AND APPLYING THIS CHAPTER OF THE FACILITATION GUIDE

In order to help facilitators interact effectively with human rights defenders, their organisations and communities, capacity building may be conceived of as a journey, which is illustrated in the graph below.

MEETING JOURNEY

As mentioned in the previous chapter, capacity building for protection is an iterative and mutual learning process involving a series of exchanges with partner organisations and communities, during which participants and facilitators alike experience "learning moments" of reflection and action. The aim is to reach a set of previously agreed objectives together, which should be aimed at improving the partners' security management skills without limiting their ability to continue working. The process (or cycle) starts with an **assessment** phase, followed by security management **workshop** sessions, then continues with a **follow-up** phase involving the adoption and implementation of security plans before returning again to an assessment phase (where are we now?) during which decisions are taken about the next steps to be taken.

PHASE 1 – PRE-TRAINING ASSESSMENT

The assessment phase allows the facilitator and the partner organisations or HRD communities to work together to identify participant expectations and needs, the facilitator´s capacities and skills, the expected outcomes of the security improvement plan, and the resources required to conduct the workshop and complete the overall process.

Furthermore, this initial step allows both the partner organisation or community and facilitators to establish the **objectives** and **priorities** for the first part of the journey, as well as to design the contents and timetable of the initial workshop and follow-up sessions.

ASSESSING NEEDS

Facilitators need to conduct an assessment of how security is dealt with within the partner organisation/community in order to identify its specific needs and define the contents and structure of the capacity building workshop. This assessment should be agreed with the partner's management or leadership. Capacities and vulnerabilities should also be assessed.

WHO TO WORK WITH :

Whenever possible, facilitators should seek to hold the first assessment meeting with the management or leaders of the organisation/community, or with the appointed Security Focal Point (SFP). It will be important for facilitators to gain a better understanding of the attitudes of decision-makers towards the capacity building process. Generally, they will themselves have both the ability and the will to push for organisational change (although in other cases the initiative might come from other parts of the organisation or community). It will be difficult to establish realistic objectives and reach lasting outcomes at the end of the process if management or leaders show little commitment to security management, if they only get involved to meet bureaucratic requirements, or if the SFP has little to no influence on the decision-making process.

While obtaining the involvement of managers or leaders is key for bringing about organisational change, staff may also need to change attitudes (e.g. in relation to risk analysis, assessment of threats and security incidents, or their views relating to free time and security). Thus, it is important that everybody who will be affected by the process participates in it. Facilitators should remind partners that security is everybody's concern!

It is impossible to overstate the importance of defining the objectives of the capacity building intervention jointly with the partner organisation/community. The main goal at this stage is to agree on realistic objectives that respond to the needs, characteristics and resources (economic and human) of the organisation/community and its HRD members. The workshop training sessions should be adapted to the culture, memory, and characteristics of the partner and the context in which it evolves as well. It is therefore important to identify the reasons why the organisation/community has requested a workshop.

Organisations or communities may be motivated to participate in a security workshop for a number of reasons: the desire to conduct an assessment of the organisation's/community's security management capacity; to learn how to assess and manage security; or to learn how to deal with (evaluate and follow up on) security issues in their day-to-day work. Past experience teaches that **this desire is often related to a concrete security situation or actual security incidents that the organisation faces**. Whether constituted by direct or indirect threats, emails or a hacked website, security incidents, or just the fact of having to face risks, these situations frequently lead organisations to rethink security issues and how they manage them. Thus, one of the main objectives of the capacity building intervention is to deal with these concrete security situations.

It is also crucial to identify the needs of the organisation or community in connection with security issues and practices, as these will help determine the specific objectives of the process. This analysis should be conducted with the directors/leaders. However, though unlikely, it is possible that these people will not be aware of the day-to-day reality and work of staff members. In this case, facilitators might decide to integrate an assessment component into the workshop cycle. This has the advantage of including the perspectives of all members of staff, and not only of management, right at the beginning of the process. Moreover, such an approach can strengthen the motivation and commitment of all participants towards the workshop objectives. Many organisations stress the importance of establishing horizontal working relationships in order to foster trust and cohesion. Be aware, though, that this takes time. In the end, the chosen method will depend on the global objective of the workshop and on the time available. Both approaches to this initial identification of objectives have advantages and disadvantages.

Please refer to the form "**Risk Assessment and Security Management for Human Rights Defenders**" in **Annex 1 of this chapter**. This provides basic guidelines for facilitators to help them conduct the assessment meeting with partner organisations/communities. Answers to the questions included in the form can shed some light on the wide array of risks HRDs in the partner organisations/communities face. Facilitators face the challenge of supporting them in developing capacities to manage these.

WRITTEN AGREEMENT

As it has been mentioned already, capacity building for protection and security is a process that requires serious commitment from the partner organisation/community to bring about the changes required to enhance the protection of HRDs. Likewise, facilitators should share their knowledge and experience on security and protection and accompany partners in the elaboration of security plans and during follow up to their implementation.

These commitments should be captured in a written agreement (or memorandum of understanding) signed by both parties. This serves as a baseline for monitoring and evaluating progress and, ultimately, the success of the process. See the form "**Agreement on Capacity Building for Security Management**" in **Annex 2 of this chapter**.

PHASE 2 – WORKSHOP TRAINING SESSIONS

The workshop sessions are structured meetings for capacity building, focused on raising the awareness of participant HRDs on security and protection issues as much as on transferring knowledge and skills to them. Furthermore, as the workshops are based on popular education principles, facilitators also learn from the experiences of participants.

CONTENTS

The success of a security and protection capacity building workshop is proportional to the extent that it responds to the needs of participants. For instance, if an organisation has very strong context analysis skills, the facilitator might decide to skip the section on Assessing your Environment and pass directly the Risk Equation. The facilitator might also want to rearrange the order in which the **New Protection Manual** and this Guide address the different themes, adapting them to the needs of the organisations or communities they are working with. However, facilitators should make sure that each session builds on what has come before in order to ensure the workshop's pertinence and coherence.

TIPS ABOUT WORKSHOP SESSIONS

- → **Estimated duration:** past experience teaches that awareness raising sessions can require 2-6 hours and training sessions, 2-3 days to complete. Ultimately, however, the duration of the workshops will depend on the agreed objectives and the content to be covered.
- → **Composition of participants:** again, there are no fixed criteria. However, facilitators should encourage organisations/communities to strike a balance between the numbers of managers/leaders and staff/members. This also applies also to training sessions with one or several organisations/communities.

VENUE

Once the contents of the workshop have been defined, the venue should be agreed. Two elements should be considered when choosing a venue: **available space** and the **security of participants**. The room should be large enough to allow participants to feel comfortable and to carry out learning activities, including group work and role plays. The venue should be in a location that participants and facilitators feel safe in, allowing the workshop to proceed without any concerns and in an atmosphere of confidence.

While workshops in rural areas can take place in community buildings that are habitually used to hold meetings, it might be practical for organisations in urban settings to conduct the workshop in their offices. This has the advantage that the office is a well-known place, where people usually feel safe. Furthermore, it has no additional cost implications. However, there are some downsides to this choice, particularly if the office is small, if participants are distracted by their computers or keep responding to work issues, or if there is no safe, discreet place available to conduct the sessions – for example when the office space is shared with other organisations or there are frequent visitors. In such cases it might be advisable to hold the workshop in an external venue such as a conference room or the office another trusted organisation. Additionally, a change of venue might help to generate new dynamics and break with the everyday routines associated with the workplace. Facilitators, of course, need to take into account the specific risks associated with conducting workshops in external venues.

RESOURCES

Ideally, sessions should not involve more than 20 participants. If the number exceeds 30, facilitators should consider suggesting that partner organisations/communities work in small groups and use plenary sessions to permit feedback and discussion.

Although one facilitator can conduct the sessions, it can be an advantage to have two, as this can improve the dynamics of the workshops. Two facilitators working together can share responsibilities (leading different sessions, note-taking, etc.) and bring a diversity of views and experiences to the workshop, etc. If working with a colleague, facilitators need to prepare and rehearse the contents of the sessions and learning activities in advance.

Workshop exercises and activities should be tailored to the reality and cultural contexts of participants. The same applies to the objectives, structure and timeline. Therefore, facilitators should find out in advance about the fields of human rights participants work in, their educational backgrounds, ages, gender and origins (if relevant). Thus, facilitators should avoid using the same learning methods everywhere: a group of HRDs who are lawyers and paralegals might respond well to abstract conceptualisations and academic-style approaches using PowerPoint, while peasants with low levels of formal education may be more responsive to visual and context-related methods (see Chapter 2 on adult learning). Whatever their background, workshop participants never start from scratch. Although they might not use the concepts of the security manual they should have ideas about security and protection. **The challenge facing facilitators is to relate these concrete experiences to concepts of security and protection**.

ONE OR SEVERAL ORGANISATIONS IN THE SAME WORKSHOP

The methods and tools used to conduct workshops differ according to whether facilitators work with one or with several organisations. A number of issues can be identified that might affect the objectives of the training process, related to the identities of the organisations, and the contexts in which they work.

When working with participants from a single organisation or community, facilitators can capitalise on the fact they are working with a **homogeneous group** that has common concerns and expectations regarding security, faces the same threats and has the same vulnerabilities and capacities. Facilitators may thus favour drawing examples and exercises from their own experience. This can help speed up the capacity building process by allowing exercises and activities to become the basis of the security plan the organisation or community will subsequently develop.

When working with **heterogeneous groups** (with participants coming from different organisations), facilitators face different challenges, such as defining common objectives, dealing with disparate participant expectations, etc. Moreover, participants may not share the same concerns regarding their security, nor face the same threats or have the same capacities and vulnerabilities. Confidentiality of information might be another challenge. Not all organisations will be keen on sharing internal information. This can slow the process down. Thus, facilitators are required to generate group dynamics that favour common understanding, while channelling diversity. Equally important is the need to develop trust at the beginning of the process. In the annexes of this Guide you will find some ideas of activities that can be used to build trust. These can be adapted according to different contexts.

These challenges notwithstanding, workshops involving several different organisations can also confer advantages. Diversity among participants and the opportunity to share experiences frequently make the process richer and more dynamic. Coming from different backgrounds, each organisation brings its own identity, culture and perspectives on security issues. This diversity enables participants to share their own experiences. Each organisation will in turn benefit from this diversity, leading to a mutual learning process. Networks, solidarities and mutual support arrangements might even be born from such processes.

PARTICIPANT MOTIVATION

At the individual as much as at the organisational level - and whatever the objectives of the workshop - if participants lack the motivation to take security issues seriously, the process is bound to fail. This in part depends on the capacity of the facilitator to mobilise participants around common objectives and to encourage their active participation. It is equally important for facilitators to identify early signs of disengagement or failing motivation and to address them with management, leaders or designated contact person so that corrective measures can be adopted. Facilitators may use the "Personal Logbook" in **Annex 3 of this chapter** as a guide as to helping participants make the most of a training session.

WORKSHOPS IN URBAN AND RURAL ENVIRONMENTS

Technological requirements differ between rural and urban contexts as do the working environments of participating organisations or communities. Particularly when working in remote rural areas, facilitators should try to be self-sufficient. This means using flipcharts, markers and other similar materials rather than a laptop and projector.[1] More importantly, facilitators can be creative, using materials they find around them. In addition, print-outs of the information produced and other workshop outcomes should be provided as hand outs to participating grass-roots organisations and communities .

In urban contexts and rural areas with appropriate infrastructure and public services, facilitators should be able to use more technological tools, such as laptops, projectors, or an internet connection. However, they should be prepared to conduct the workshop without these, should they fail to work or the facilitators feel participants might react more positively to a more traditional way of delivering the sessions. Facilitators can also provide electronic copies of the workshop outcomes.

Facilitators should in any case enquire beforehand about the technology that is available in the workshop venue, and prepare accordingly. However, it is important to take into account that face-to-face exchanges and joint activities are what make workshops most useful.

This Guide, and the learning activities it contains, take this distinction between rural and urban contexts into account. When necessary, therefore, learning activities are adapted to one or other of these contexts. Something that works for urban organisations, might not work for rural communities and vice versa. For instance, it may not make sense to develop a formal security plan for a peasant community. Instead, facilitators might wish to focus on the design of concrete protection strategies and measures, which would then be put into practice in the day-to-day activities of the community. The methods employed might also be different. The relevant sections of the Guide specify whether learning activities are designed to be applied in both contexts or only in one.

1 Facilitators can use a laptop for note-taking purposes if it has enough battery power or there are adequate power sources; care should be taken to ensure data protection and encryption when travelling to remote areas.

This distinction between rural and urban workshops also has implications for content . Joint and collective action is much more important for remote rural organisations and communities, and it is because of this that the Guide highlights **protection networks for communities in rural areas**. This decision was made in response to several years of field experience working with communities and grassroots organisations in rural areas. These groups face daunting challenges to ensure their collective protection in the face of threats and risks stemming from their work in defence of their economic, social and cultural rights, including their rights to the territory where they live and work.[2]

Indeed, HRDs operate in relatively complex socio-institutional contexts, interacting with other grassroots organisations, NGOs, non-state actors and public institutions . All these actors can operate simultaneously at local, regional, national and/or international levels. Thus, this network of relationships between internal and external actors can contribute to generating a collective capacity to act (i.e. the protection of community members and the defence of territory).

IN SESSIONS ON PROTECTION NETWORKS FACILITATORS SHOULD FOCUS ON:

- → **Making communities aware of the benefits networking confers: helping them access or mobilise resources (internal and external) and generate protection (for individual members and the collective).**
- → **Providing tools that help communities understand the dispute over the territory better and how they function as a group.**
- → **Enhancing community capacities to defend their territory.**
- → **Strengthening the capacities of the HR movement to continue defending human rights.**

Facilitators can find additional materials on protection networks for rural area communities in **Chapter 5.8 of this Guide**.

2 PI is undertaking an applied research study on community protection networks. It builds on the ongoing experiences with rural area communities in Guatemala and other countries where PI has field protection offices. The outcome of this project, which is expected for late 2014, aims to inform current practice and enhance protection strategies for community-based HRDs.

WHAT MAKES A WORKSHOP SUCCESSFUL :

- > Commitment of organisation managers and/or community leaders.
- > Joint preparation with participating organisation(s).
- > Institutional as well as individual awareness of security issues.
- > Quality, diversity and dynamism of the methodology (videos, cards, role-play, etc.), and sharing of facilitators' own experiences to aid understanding of situations.
- > Rooted in participants' expectations and experiences.
- > (Whenever possible), two facilitators to conduct the workshop.
- > Context-related activities and exercises.
- > Security plan with clear and realistic objectives. (It is better to have a short but needs-focused security plan than an ambitious one that will not be implemented).
- > Concrete results and outcomes for participants.
- > A suitable venue.

PHASE 3 – FOLLOW-UP OF THE WORKSHOP SESSIONS

When dealing with complex topics, such as the organisational or community management of security, one-off workshop training events are rarely useful. If the capacity building process is going to be effective in helping bring about change and achieve sustainable outcomes, the workshop training sessions must be followed up after they have finished. In this third phase, facilitators and partners should meet a number of meetings times and possibly even organise further training if the need arises. As in the previous phases, the follow-up period has to be conducted jointly with the management or leadership of the organisation/community receiving the training. This is why **it is important to include an organisational commitment to conduct follow-up activities in the written agreement signed at the start of the process**. This being said, there is no barrier to convening meetings outside the pre-established agreement if requested by the partner or in response to "opportunities" that may arise. An example of this could be when the partner organisation calls the facilitator for advice following a fresh security incident.

Although there is no limit to the number of follow-up meetings that facilitators and partner organisations/communities may schedule, their number will depend principally on time and budget constraints. Moreover, it is important to strike a balance between the need for guidance from facilitators and empowering the partner to manage its own security plan. Despite these considerations, experience has shown that successful follow-up ought to be carried out in three steps.

The first step is the **workshop evaluation** during which the partner carries out an appraisal of the quality of the training and the performance of facilitators against its own expectations. This should be done immediately after the workshop, or over the next few days, while details are still fresh in the minds of participants. The evaluation should also help facilitators hone the pertinence of workshops. The "**Workshop Evaluation form**" in **Annex 4 of this chapter** can be used as a grid for such assessment.

The second step involves the **regular follow-up meetings**. These meetings, to be held regularly (every one or two months) for a given period of time (six months to two years, depending on circumstances), should serve to assess the implementation of the security plan and measures designed during the workshop sessions. They provide the opportunity for facilitators to troubleshoot and help partners overcome any hurdles they might encounter along the way. In **Annex 5 of this chapter** facilitators will find the "**Monthly Follow-Up Meetings**" table, designed to help them structure their dialogue with the management/leadership of the partner organisation/community. It is very important that partners understand that this step is not an evaluation of their progress implementing the security plan or lack thereof, but is focused primarily on needs and barriers. The meetings also provide the opportunity to learn from the experience of facilitators (e.g. "this has sometimes happened to other organisations, what about yours", etc.; on this, please refer also to Chapter 2.3 of the NPM on barriers and organisational processes). Experience shows that on too many occasions the task of drafting a security plan is perceived to be an onerous and daunting one by people in partner organisations/communities, but this is not actually the case. Facilitators should be clear on this, but remind the organisations/communities that there are no magic recipes (and be sure to reject requests such as "do you have a ready-made security plan we could use?").

The third and final step involves the **end of the collaboration or the beginning of a new cycle**. The previous step provides the basis for assessing what should be done next. Depending on the stage the partner organisation/community has reached regarding the adoption of the plan, and their levels of commitment, facilitators might decide to end the collaboration, begin a new cycle, or to go into more detail on particular themes. The "**Final Evaluation Form**" in **Annex 6 of this chapter** may be used as a guide.

ANNEX 1

PRE-TRAINING ASSESSMENT

> RISK ASSESSMENT AND SECURITY MANAGEMENT FOR HUMAN RIGHTS DEFENDERS

TO BE COMPLETED BY THE FACILITATOR IN CONSULTATION WITH THE HRD/ORGANISATION/COMMUNITY

NAME OF PERSON CONDUCTING THE ASSESSMENT:

DATE & VENUE:

RESPONDENTS (INCL. POSITION WITHIN THEIR ORGANISATION)

Note to facilitators: please take into account that for security reasons organisations might not be willing to put all the information requested on this form in writing. If this is the case, assurances should be given that it will be kept safe .

A. PROFILE

1. Name of the HRD/organisation/network; contact details & location.

2. For organisations & networks, indicate the type of organisation:

- ☐ Local NGO/Community-Based Organisation
- ☐ National NGO
- ☐ International NGO
- ☐ National Institution(e.g. National Human Rights Commission, Ombudsman)
- ☐ Academic/Research Institution
- ☐ Government
- ☐ Independent (not attached to any institution/organisation)
- ☐ Other/Specify

3. Does the participant have an office(s)?

- ☐ Yes
- ☐ No

4. Number of offices (including branches), location (country, and city/town) and number of staff.

5. Please indicate the principal target groups the defender/organisation/network works with/for:

- ☐ Human Rights Defenders
- ☐ Indigenous People
- ☐ Media
- ☐ Migrant Workers
- ☐ Policy & Decision makers
- ☐ Police/Military/Security Forces
- ☐ Internally displaced peoples/Refugees/Immigrants
- ☐ Women
- ☐ Prisoners
- ☐ Sexual Minorities
- ☐ Other/please specify

6. Please indicate the main human rights issues the defender/organisation/network currently addresses:

- ☐ Freedom of Information/Expression
- ☐ Freedom from Torture
- ☐ Labour Rights
- ☐ Access to Justice (due process, arbitrary arrest, etc.)
- ☐ Minority rights: ☐ Religious ☐ Ethnic ☐ Other :
- ☐ Refugee Rights
- ☐ Rights of Human Rights Defenders
- ☐ Rights of Women
- ☐ Rights of Children
- ☐ Good Governance
- ☐ Economic, social and cultural rights
- ☐ Other/please specify

7. Indicate up to three (3) main types of activities carried out:

- ☐ Research
- ☐ Capacity Building
- ☐ Publications
- ☐ Community Development
- ☐ Conflict Resolution
- ☐ Human Rights Education
- ☐ Anti-Corruption Campaigns
- ☐ Journalism
- ☐ Advocacy
- ☐ Monitoring
- ☐ Legal Aid
- ☐ Others

B. CONTEXTUAL INFORMATION

1. What are the *principal* human rights violations in the area/community?

2. What are the *principal factors* contributing to these violations?

3. Who are the *main perpetrators* of HR violations in the community/area?

4. How does the work of the defender affect them?

5. How have the *perpetrators* reacted to the work of HRDs?

6. Does your work have different implications for male and female staff? If yes, how?

C. CURRENT SECURITY MANAGEMENT PRACTICE OF HRD/ORGANISATION/NETWORK

1. What are the risks faced as a result of the HR work they carry out (think also about information and communications)? Why?

2. Have the participants experienced incidents related to their work that have jeopardised their security? If yes, please describe these incidents (When? What happened? Who was involved?)

3. Do the HRD/organisation/community analyse incidents – individually or - in the case of organisations and networks - jointly?

4. What security measures are currently being implemented? Which risks do they seek to address?

5. Does the organisation carry out active security planning? If yes, how?

D. MANAGEMENT OF DIGITAL OPERATIONS BY THE ORGANISATION/NETWORK/DEFENDER.

1. How are computers used ? (desktops, laptops, tablets, etc.)

2. Have there been any digital security incidents (SIs) e.g. emails or website hacked, targeted theft of computers etc.?

3. Does the HRD/organisation/community have IT support? If yes, who provides it?

4. What are the participants currently doing to protect digital information?

5. How are phones used for work-related tasks e.g. work e-mail accessed via the phone etc. ?

E. ASPECTS OF WELL-BEING TO BE CONSIDERED BY FACILITATOR DURING ASSESSMENT

1. From the information provided above, could there be possible cases of trauma as a result of events or experiences that have had a major impact on staff well-being? e.g. physical attack as a result of HR work, witnessing violent acts committed against others etc.?

2. Have HRDs shared information about past SIs or attacks that suggest a high level of risk likely to have resulted in stress among staff?

3. Are there indicators of high work load that could impact on physical and emotional well-being in terms of stress and exhaustion?

4. Does the organisation have policies and practices that recognise the well-being of employees, e.g. annual leave, time off in lieu for overtime or weekend work, availability of support services such as counselling (compulsory or on demand), etc.?

5. What is the general atmosphere among staff members – would it allow for open, discussions of stress and fear among staff?

6. Does management support the idea of including the issue of well-being in the capacity building process?

F. MOTIVATION & COMMITMENT

1. What is your motivation to participate in a capacity building process on security management?

2. Think of past capacity building initiatives you have attended. Considering those which were successful, what factors contributed to a successful organisational change process?

3. What change do you want to see as a result of participating in this capacity building process – at individual and organisational level?

4. Who needs to be involved to make this change happen?

G. PREPARATIONS FOR THE WORKSHOP TRAINING SESSIONS

1. How many people will participate in the workshop?

2. What is the composition of the participant group? (management/leadership, staff/members)

3. How many days will the workshop last?

4. Where will it take place? What technical facilities are available?

5. What should the objectives of the workshop be?

H. OTHER

Please indicate any others comments/remarks/questions:

ANNEX 2

MEMORANDUM OF UNDERSTANDING

> AGREEMENT ON CAPACITY-BUILDING FOR SECURITY MANAGEMENT

TO BE COMPLETED BY THE FACILITATOR IN CONSULTATION WITH THE HRD/ORGANISATION/COMMUNITY

AGREEMENTS WITH THE PARTNER

NAME OF NETWORK, ORGANISATION OR COMMUNITY:

DATE:

FACILITATOR:

COORDINATION OR MANAGEMENT STAFF:

SECURITY FOCAL POINT:

CONTACT PERSON(S):

AGREEMENTS:

AGREED RESPONSIBILITIES TO ENSURE FULFILMENT OF AGREEMENTS (DETAILED BELOW)

IMPLEMENTATION SCHEDULE

EXAMPLES OF PROGRESS INDICATORS

(These should be concrete milestones that reflect the depth and complexity of the desired change. They should respond to the questions "Who does what?" and "How"?)

Note: These examples are appropriate for a hypothetical urban workshop and are provided here by way of example)

1. The following actions are expected: these are easily achievable reactive actions, for example, Participate in a Workshop. (Between 4 and 8 indicators)

1. Everybody within the organisation participates in the risk analysis and security plan workshops.
2. Management and Security Focal Points to participate in follow-up meetings.
3. Any person who is required to use IT security tools will participate in the relevant session(s).
4. Everybody in the organisation should participate in the overall evaluation of security performance.
5. Individuals who require advice on a specific case have participated in a meeting where they have been able to receive advice.
6. Members of the organisation participate in the institutional context analysis.
7. ...
8. ...

2. It would be desirable to achieve: these actions indicate more active learning or greater commitment. (Between 8 and 12 indicators).

1. Members of the organisation are aware of the need to implement a security plan, and the measures it contains.
2. All members of the organisation report security incidents in the correct place (incident book, or report to the Security Focal Point)
3. Members of the organisation contribute proposals to improve the plan and its weak points.
4. Members of the organisation implement an average of 50% of the security plan and the measures it contains.
5. The organisation's management team and the Security Focal Points analyse Security Incidents and evaluate the associated threats, vulnerabilities and capacities.
6. The organisation's management team, or the Security Focal Points, inform the rest of the organisation of the results of the analysis of the incidents and gather their impressions and contributions.
7. The organisation's management team and the Security Focal Points prepare protocols defining actions to be taken in response to emergency situations.
8. ...
9. ...
10. ...

3. Ideally, the following will be achieved: these actions indicate real transformation and maximum achievement. They might require more time to fulfil than has been programmed for. (Between 3 and 6 indicators)

1. Full implementation of the entire security plan by all members of the organisation.
2. The organisation's management team and the Security Focal Points possess all the necessary information on risk; they analyse it, create protocols or measures in response, and present them to the rest of the organisation for agreement; they also ensure that context and risk analyses are carried out and security plans prepared, all of them regularly.
3. The organisation manages risk autonomously, only requiring advice or training as a result of its own analyses.
4. ...
5. ...

PROGRESS INDICATORS

1. The following actions are expected: these are easily achievable reactive actions, for example, Participate in a Workshop. (Between 4 and 8 indicators)

2. It would be desirable to achieve: these actions indicate more active learning or greater commitment. (Between 8 and 12 indicators).

3. Ideally, the following will be achieved: these actions indicate real transformation and maximum achievement. They might require more time to fulfil than has been programmed for. (Between 3 and 6 indicators)

FOLLOW-UP

The Facilitator agrees with the partner when and how the follow up activities/workshop/subsequent meeting(s) will be carried out:

Signature of person responsible (approved).

ANNEX 3

PERSONAL LOGBOOK

> TO MAKE THE MOST OF A TRAINING PROCESS:

A PERSONAL LOGBOOK IS A TOOL THAT ALLOWS PARTICIPANTS TO REFLECT (EITHER INDIVIDUALLY OR COLLECTIVELY) ON A LEARNING OR CAPACITY BUILDING PROCESS

You will find the logbook on the next page. Print out one copy for each participant with the number of sheets corresponding to the number of training days. Introduce the purpose of the personal logbook to participants on the first day of the training. Provide time at the end of each day or during the morning of the following day for participants to fill it in. The information in the logbook remains with participants.

Often, in a training process or workshop, participants have many different learning experiences. These tend to get mixed up and, therefore, to fade. This can happen quite quickly. It appears that halfway through a training course most people find it difficult to remember exactly what they learned during the first few days.

This personal logbook will help you benefit as much as possible from the training experience. In it you will be able to record the most important messages of each day. After each day (or the following morning) you will be given 10 to 15 minutes to reflect on the day's activities (or those of the previous day) and to note down the learning points that were most important to you.

At the end of the course the resulting overview will provide you with a summary of what you experienced and learned. That summary will help you to decide which learning points you want to use in your daily working practice.

→ **The first box** (see next page) allows you to note down the **observations** you have made during the day. What did you hear? What did you see? There are no wrong answers, so feel free to write down anything that comes to mind.

→ **The second question** focuses on how these observations made you feel. Sensory impressions are essential to learning and conscious efforts will be made to engage the senses during the training process in order to deepen learning. In your reflections, mention events you considered to have been **eye-openers** throughout the day: what made you enthusiastic, surprised you, amazed you, annoyed you, etc.?

→ **The third question** addresses the **meaning of your feelings**. Why were you amazed? Why was it an eye-opener? Why did you not agree with what was said or done? What does this tell you about your experiences with the topic of this workshop so far?

→ **The last question** focuses on the future and the workshop's impact on your work. What **have you learned** about yourself? What does this imply for you? What are you going to do **to change or to add** to your skills and behaviour? What does this imply for your future work/activities?

PERSONAL LOGBOOK

DAY .....

1. What have you observed today? What topics have we dealt with? What exercises have we done?

2. What were the eye-openers in today's sessions? What made me enthusiastic? What did I not agree with?

3. Why was I enthusiastic? Why did I not agree?

4. What have I learned about myself? What does this imply for my work? What am I going to change or add in to the way I work?

ANNEX 4

FIRST STEP – FOLLOW UP

> WORKSHOP EVALUATION FORM

1. Were your expectations about the training workshop met? If not, why not?

2. Were your knowledge and experience appreciated and actively incorporated in the training? If not, how could this be improved?

3. Was the content of the training well prepared? If not, what could be done differently?

4. Was the workshop easy to understand? If not, how could this be improved?

5. Do you feel empowered to work actively on your security management? If not, what further support do you need?

5. Do you feel empowered to share your knowledge with others? If not, what further support do you need?

7. So that we can improve as trainers, we would value your feedback on our skills. Please let us know what our strengths are and what we could improve.

NAME OF FACILITATOR :

Strengths :

Areas for improvement :

NAME OF FACILITATOR :

Strengths :

Areas for improvement :

NAME OF FACILITATOR :

Strengths :

Areas for improvement :

8. Were the logistics of the training adequate (travel, venue, etc.)?

THANK YOU !

ANNEX 5

SECOND STEP – FOLLOW UP

> MONTHLY FOLLOW-UP MEETINGS

ORGANISATION OR COMMUNITY:

DATE & VENUE:

PERSON RESPONSIBLE FOR FOLLOW-UP:

1. SECURITY INCIDENTS

1. Have you been registering and analysing security incidents?

2. Aggressions suffered:

2. SECURITY PLAN

1. Which were the most efficient security measures included in your security plan?

2. Have your vulnerabilities been reduced?

3. Have your capacities increased?

4. How well were the security measures implemented by members of the organisation?

5. Has there been resistance to the implementing security rules by members of the organisation?

6. What institutional difficulties have you had to face to advance the security plan?

7. How much of the security plan has been implemented?

8. When will you next assess your risks and review your security plan?

3. OTHER FACTORS

1. Context related elements:

2. General observations:

ANNEX 6

THIRD STEP – FOLLOW UP

> FINAL EVALUATION

The aspects presented in the form, below, should be used to document an HRD's, organisation's, or community's achievements following the capacity building process. The table contains a check list and space for a short narrative explanation of the decision that has been taken to finalise the process, alter its terms or initiate a new cycle. Space is also available to provide notes on the process of support that was provided.

To ensure a participatory approach, the partner organisation should be involved in the evaluation, preferably by participating in an evaluation session in which HRDs are able to discuss the process, progress and learning points. This will in part inform the answers to the questions below.

1. Reasons why one or both of the entities have decided to end the collaboration :

2. Overall assessment of the situation at the moment the collaboration ended:

3. Additional facilitator support that still might be needed based on the list presented in the table below:

4. Overall evaluation of the support process:

5. Aspects of security management – knowledge – attitude - behaviour :		
COPY LIST OF ACTIONS FROM MONITORING SHEET	**PERSON RESPONSIBLE**	**DESCRIBE THE SITUATION AFTER INTERVENTION**