



GUIDE FOR FACILITATORS

FOR THE **NEW PROTECTION MANUAL FOR HUMAN RIGHTS DEFENDERS**

MAURICIO ANGEL & ENRIQUE EGUREN (EDITORS)



Except where otherwise noted, this work is licensed under
<http://creativecommons.org/licenses/by-nc-nd/3.0/>

Published by: Protection International, Rue de la Linière 11, B-1060 Brussels, Belgium

Copyright © 2013 PROTECTION INTERNATIONAL

ISBN 978-2-930539-33-1

Editors: Mauricio Angel & Enrique Eguren

Contributors: Mauricio Angel, Enrique Eguren, Sylvain Lefebvre, Nora Rehmer

Translators: James Lupton (English), Thomas Lecloux (French), Valeria Luna (Spanish)

Design and layout: Quidam

Acknowledgements: To all PI teams in the field and head office, and particularly to Balzac Buzera, Elena Caal, Gitahi Githuku, Ben Kabagambe, Ivy Kihara, Alexandra Loaiza, Luisa Pérez, Tessa de Ryck, Cahyadi Satriya, Bee Pranom Somwong, Ilaria Tosello, Kheetanat Synth Wannaboworn, Arjan Van der Waal & Xabier Zabala.

Donors: American Jewish World Service; European Instrument for Democracy and Human Rights



European
Initiative for
Democracy and
Human Rights
EIDHR



TABLE OF CONTENTS

1. INTRODUCTION TO THE GUIDE FOR FACILITATORS	5
2. LEARNING PROCESSES AND CAPACITY DEVELOPMENT	7
POPULAR EDUCATION	7
LEARNING METHODOLOGIES: HOW ADULTS LEARN	8
THE TASK OF BUILDING PROTECTION CAPACITIES IS ALWAYS OPEN-ENDED	13
3. JOURNEYING TOGETHER TOWARDS PROTECTION: TRAINING MEETINGS AND WORKSHOPS	17
MEETING JOURNEY	17
PHASE 1 – PRE-TRAINING ASSESSMENT	18
PHASE 2 – WORKSHOP TRAINING SESSIONS	20
PHASE 3 – FOLLOW-UP OF THE WORKSHOP SESSIONS	24
ANNEX 1 - PRE-TRAINING ASSESSMENT	25
ANNEX 2 - MEMORANDUM OF UNDERSTANDING	29
ANNEX 3 - PERSONAL LOGBOOK	33
ANNEX 4 - FIRST STEP – FOLLOW UP: WORKSHOP EVALUATION FORM	37
ANNEX 5 - SECOND STEP – FOLLOW UP: MONTHLY FOLLOW-UP MEETINGS	39
ANNEX 6 - THIRD STEP – FOLLOW UP: FINAL EVALUATION	41
4. MONITORING PROGRESS	43
SUPPORTING HRDS IN THEIR PLANNING PROCESS	46
COLLECTING RELEVANT DATA THROUGH MONITORING	49
5. WORKSHOP SESSIONS	51
PREPARING THE WORKSHOP SESSIONS	51
1. ASSESSING YOUR ENVIRONMENT	53
2. RISK ANALYSIS	59
3. UNDERSTANDING AND ASSESSING THREATS	67
4. SECURITY INCIDENTS	75
5. PREVENTING AND REACTING TO AGGRESSIONS	81
6. DRAWING UP A COMPREHENSIVE SECURITY STRATEGY	87
7. PREPARING A SECURITY PLAN	93
8. PROTECTION NETWORKS FOR HRDS BASED IN RURAL AREA COMMUNITIES	99
9. ORGANISATIONAL SECURITY	109
10. INFORMATION MANAGEMENT AND DIGITAL SECURITY	117

INTRODUCTION TO THE GUIDE FOR FACILITATORS

This Guide for Facilitators is intended to serve as a tool for people who are interested in facilitating training processes to develop protection capacities in human rights defenders (HRDs), their organisations and communities. In preparing the Guide, PI's Policy, Research and Training Unit (PRTU) has received valuable support from colleagues who work in the Protection Desks in the different countries where the organisation operates. The Desks have shared their day to day experiences working with HRDs and grassroots organisations in urban and rural contexts. Equally, the Guide is rooted in the key concepts of the popular education movement, offering facilitators access to concepts that will allow them to stimulate interest among participants and offer a shared, non-hierarchical, training experience for HRDs.

This publication can be used within the framework of the capacity building work that PI carries out with the HRD organisations and communities it accompanies and as a resource to carry out a diagnostic of the security situations they face. It also contains support materials that will help them monitor and evaluate their progress implementing their security plans.

Similarly, this Guide for Facilitators contains a range of materials and advice that may be used to structure and prepare practical workshop sessions along the pathway set out in the **New Protection Manual for Human Rights Defenders** (henceforth, the NPM).¹ The Guide suggests different ways in which facilitators can transmit their knowledge, by contextualising the key contents of the NPM for different specific audiences. Thus, the Guide is designed to function as a "Toolbox" from which facilitators can choose elements to use when preparing their training sessions.

The Guide has at least six objectives:

1. To **systematise experiences of facilitation of capacity-development processes**, recognising their complexity and the need for multiple interventions .
2. To address aspects related to the **diversity of partner HRD organisations and communities** (learning patterns and experiences will be different in each case).
3. To provide **practical, participant-focused, methodological approaches** for facilitators that; to help learning and understanding among groups.
4. To provide facilitators with **tools to assess the learning needs of participants as well as monitoring tools to measure change** that occurs as a result of the capacity building provided.
5. To provide facilitators with a range of **materials and further reading** to enable them to contextualise the training they provide and to utilise partners' experiences actively as part of the learning process.
6. To simplify the content of PI's **New Protection Manual for Human Rights Defenders** and help facilitators use it effectively as resource material.

Far from seeking to impose a single approach that must be followed to the letter, the PRTU team hopes that the Guide will encourage facilitators to be creative when responding to the most frequent difficulties and challenges they face in their daily work with HRDs and grass roots organisations.

¹ Luis Enrique Eguren and Marie Caraj (2009). *New Protection Manual for Human Rights Defenders*. Protection International. Brussels.

THE NEW PROTECTION MANUAL AND THE DEVELOPMENT OF PROTECTION CAPACITIES: MAKING CONNECTIONS AND LEARNING TOGETHER

The NPM is the fruit of nearly three decades working with HRDs, evaluating the risks they face because of the work they do, and designing and implementing plans to improve their individual and organisational security. The NPM is intended to develop the capacities of HRDs to take responsibility – independently and in a sustainable manner – for their security and protection. In other words, it is meant to provide accompaniment to the HRDs as they themselves develop their roles as agents of change.

“Security and protection are complex areas. They are based around structured knowledge, but also influenced by individual attitudes and organisational behaviour. One of the key messages in this manual is to give the issue of security the time, space and energy it deserves, despite overloaded work agendas and the severe stress and fear all defenders and their organisations are under. This means going beyond people’s individual knowledge about security and moving towards an organisational culture in which security is inherent”.²

PI is aware that there is no magic formula that guarantees protection for HRDs, their organisations and their communities. Furthermore, each HRD is immersed in their own unique cultural, social and political context. Plus, risks change. Any attempt, therefore, to formulate a single security plan that may be applied in any situation is doomed to failure and it is extremely unlikely that a written text will be entirely valid for so many and so diverse a group of people, whose geographical, cultural and political contexts are so different.

This is why it is important to facilitate the kind of interaction that occurs in workshops or meetings and that create connections between what the NPM says and the lived experiences and needs of HRDs in the real world. This interaction occurs in two directions as might be supposed: from the facilitator to the participants and from the participants to the facilitator. This interaction can and should lead to a mutual learning process that is enriching for facilitators and participants alike.

This also explains why we consider this Guide to be a work in progress, open to improvement, change and development. The feedback received from the people who use it will be fundamental in ensuring that this is indeed the case, as it will enable us to enrich a document that is permanently available on line. We will endeavour to improve it permanently, adding complementary materials whenever we are able to. This Guide for Facilitators remains, in other words, in your expert hands.

² Ibid. pp. 10-11.

LEARNING PROCESSES AND CAPACITY DEVELOPMENT

This chapter addresses the three conceptual underpinnings of the training process in security management for HRDs: **popular education**, **adult learning methodologies** and **capacity development**. It provides guidance and suggestions to facilitators on how best to stimulate participants' understanding of security in the different meetings, encounters and workshop training sessions they will be involved in.

POPULAR EDUCATION

Popular education refers to a socio-pedagogical approach to emancipatory education or **an education for critical consciousness**¹, and it informs most of the contents of this Guide for Facilitators. Although the learning methods and techniques employed are similar to those used in adult learning (see Section «**Learning methodologies: How adults learn**» below), popular education seeks to construct an alternative educational approach that is consistent with rights, emancipation and social justice. Popular Education is popular because it prioritises working with the rural and urban poor, who are the majority in the Global South. It is a collective educational endeavour where teachers and students learn together. There are three parts to the process beginning, (a), with the **concrete experiences of the participants** followed (b), by **reflection on these experiences** which in turn lead, (c), to the **identification of actions to bring about positive change**.

Popular education traces its roots back to the 1960s and the literacy training programs of Brazilian educator and philosopher Paulo Freire. He taught his students to read and write by discussing basic problems they themselves were experiencing, such as lack of access to agricultural land. As the causes of their problems became clear, students analysed and discussed what joint action they could take to change their situation.

Freire coined the term “**consciousness-raising**” to describe the **process of action-reflection-action**, which led participants not only to acquire new literacy skills, but also to understand their own reality.

Popular education has certain principles, which have been applied in this Guide:

- The starting point is the **concrete experience of the individual HRD**.
- **Everyone teaches; everyone learns.**
- It involves **high levels of participation**.
- It leads to **action for change**: in this case, the promotion of a more secure practice in defence of human rights.
- It is a **collective effort**, focusing on shared rather than individual solutions to problems: similarly, defending human rights is usually a collective action.
- It stresses the **creation of new, place-specific knowledge**, rather than simply applying existing knowledge to new scenarios: security plans and practice should be created and owned by defenders, rather than adapted from pre-existing external “recipes”.
- It is an **ongoing process** that can be carried out at any time and in any place: the vision of capacity development inspiring this Guide is that security and protection for HRDs involves a journey.

¹ This chapter has been prepared by adapting A Popular Education Handbook, by Rick Arnold and Bev Burke (see http://www.popednews.org/downloads/A_Popular_Education_Handbook.pdf) and the website <http://www.practicingfreedom.org/offerings/popular-education>. Those interested in exploring popular education further should read Freire's seminal book “Pedagogy of the Oppressed”.

WHAT IS THE ROLE OF FACILITATORS AS POPULAR EDUCATORS IN PROTECTION?

The role of the popular education facilitator differs dramatically from the role of teachers in conventional education programs, in at least four ways:

- **Shared leadership:** everyone teaches and everyone learns.
- **Joint construction of knowledge:** the starting point is the prior experience of the participants.
- **There is no so-called “expert”:** instead, there is mutual respect for the knowledge and experience that all participants bring to the process.
- **Working hand in hand:** facilitators help participants develop ideas and skills for action while themselves also committing to act.

It is important to bear in mind, however, that facilitators are not participants and that the learning process is far from spontaneous. The role of the facilitator is to ensure that the process – what happens and how it happens – encourages learning and the development of leadership in the group. How an activity is discussed is important, as the ways in which a technique is decoded are crucial to the learning of the group. Facilitators must understand the likely needs of participants and their perceptions of the security issues they face beforehand. They should know a good deal about the situation themselves so they can assist participants to change the reality under scrutiny. How the process is handled will determine the role HRDs can play in shaping the content and design of the program as it develops.

> THEORY AND PRACTICE: NOT JUST A METHODOLOGY!

Popular education seeks to get to the «heart» of issues of power and privilege. It is often – although not always – the case that facilitators enjoy several advantages compared to the HRDs participating in the workshops (being an outsider, being the “expert”, etc.). If this is the case, facilitators should establish a common language and a shared framework, whether through dialogue, presentations, or interactive exercises. They should create an environment that permits all participants to be heard and to explore ways forward so that each member of the organisation (or community) has a role to play developing protection measures, ensuring security and owning the process.

LEARNING METHODOLOGIES: HOW ADULTS LEARN

WHY PEOPLE LEARN

When planning a learning process, it is crucial for facilitators to understand what motivates people to learn. At the core is a **need**; in situations where individual HRDs, human rights organisations, networks or communities have faced serious security incidents, threats or even attacks, the motivation for learning may be quite obvious: to be able to improve their security and reduce the risks they face. This aspect is examined as part of the **assessment** phase explained in the next chapter. Second, **relevance** and perceived **benefit** are crucial factors motivating learning. In other words, participants need to understand that security management tools are relevant to improving the current situation. An improved ability to manage security matters will be directly beneficial at individual and organisational level. Thus, facilitators must actively stimulate and respond to these factors during the **workshop** and **follow-up** phases if their work is to have an impact.

HOW PEOPLE LEARN

Facilitators face the challenge of finding ways to structure the new information they want to transmit in ways that build most effectively on what the participants already know. One way of doing this is by building on the different steps of David Kolb's experiential learning cycle.² The illustration below shows how facilitators can support participants to derive new understanding from a concrete experience :



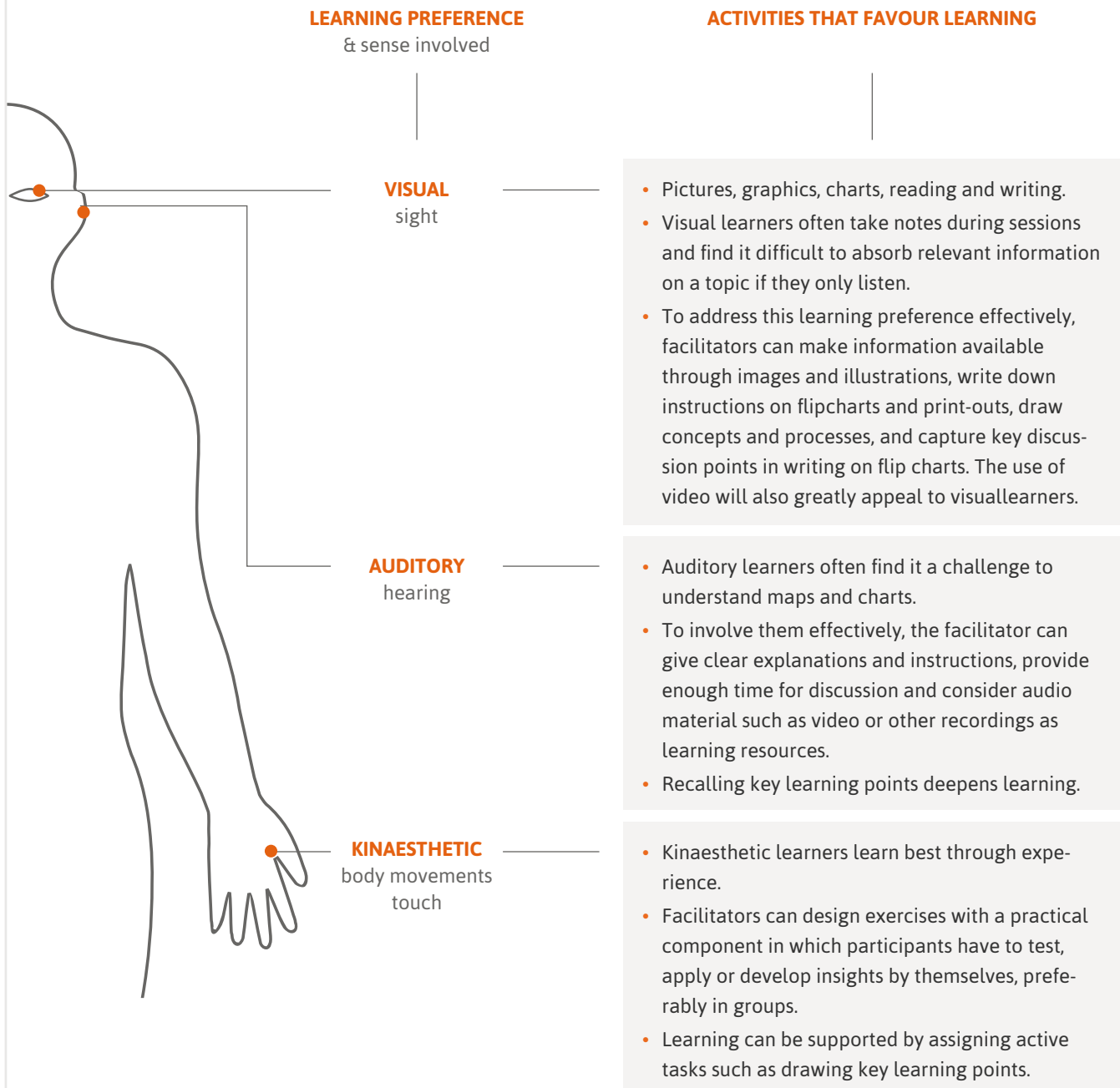
To further strengthen new ideas and the understanding of participants, facilitators should make regular reference to the insights gathered throughout the training, showing how different aspects interconnect and build upon each other. It is equally useful in later sessions to build on earlier exercises, using outcomes from previous assignments, exercises and discussions.

² Kolb, D and Fry, R. (1975). "Toward an Applied Theory of Experiential Learning". In C. Cooper (Ed.). *Theories of Group Process*. London. John Wiley. Experiential learning has since been further developed and widely discussed. A wide range of information on the topic can be found on the internet.

HOW TO REACH EVERY LEARNER

Human beings learn throughout their lives. Adult learners in particular have a rich set of knowledge and experiences. When facilitators build on this consciously they encourage and deepen learning. Yet it is important to recognise that people learn in different ways. Each person has a preferred manner of absorbing and processing new information more effectively.

An easy way to differentiate these learning preferences is by identifying which sense(s) individuals favour when processing information:



While participants will certainly use all their sensory organs in the course of a training session, one of is usually dominant. Furthermore, it is very likely that among a given group of participants all learning preferences will be represented. Facilitators face the challenge of addressing all of these and avoiding the pitfall of only addressing the preference that is closest to their own.

The more interactive the sessions, the more stimulus is provided for participants and their different learning preferences .

The following principles can help facilitators address the three areas of preference effectively in the sessions³:



³ AI SPA 2013, Barefoot Collective (2011). Designing and Facilitating Creative Learning Activities. A Companion Booklet to the Barefoot Guide on Learning Practices in Organisations and Social Change. See: <http://www.barefootguide.org/designing-and-facilitating-creative-learning-activities.html>


THE TARGET GROUP

HRDs are deeply committed individuals who rely on knowledge and personal experiences to carry out their work. They are embedded in complex networks and develop their activism in the process of making sense of their environment. They have a unique insight into the structure and functioning of their communities and are able to detect and influence social and political dynamics.

Facilitators face the challenge – which is also an opportunity - of recognising and using the vast resources that each individual participant brings to a training session, in order to:

- > **Help and deepen learning on an individual level;** and
- > **Support cross-fertilisation and learning from others' experiences.**

When facilitators recognise that they are not the only source of knowledge in a training context an atmosphere of exchange and mutual learning tends to develop, allowing new insights to be shaped and made relevant to the local context of participants.⁴

-  → **Facilitators are advised to design their sessions in ways that support the natural ways in which adults learn. The ability of human beings to acquire new knowledge and improve their practice is also shaped by their attitude towards learning. Helping participants achieve a positive attitude will facilitate the process of learning.**⁵
- **Build in regular elements of practice and sharing of experience.**
- **Be aware of different learning preferences. This will help you devise methods to ensure the active involvement of all participants in their training.**
- **Contextualise new information (i.e. relating it to what is already known and its benefit and relevance for participants). This will motivate participants.**
- **Repeating and regularly referring to previous learning points deepens learning.**

⁴ Hammond, Linda-Darling, K. Austin, S. Orcutt, J. Rosso (2001). *How People Learn, Introduction to Learning Theories*. Stanford University School of Education. See: <http://www.stanford.edu/class/ed269/hplintrochapter.pdf>

⁵ Ibid.

THE TASK OF BUILDING PROTECTION CAPACITIES IS ALWAYS OPEN-ENDED

Nowadays the free exercise of the right to defend human rights is internationally recognised. It is, however, frequently the case that men and women who work as human rights defenders (HRDs) face opposition to their work from the authorities or from other social actors. And on too many occasions this opposition takes the form of repression: HRDs are threatened, stigmatised and criminalised; they suffer from physical aggression and even murder.

This is why this Guide for Facilitators focuses on developing the capacity of HRDs to take care of their own security and protection. The Guide is intended to provide a structured reflection on the topic that identifies ways HRDs can work jointly, within an organisation or a community, to improve their levels of protection.

WHAT ARE PROTECTION CAPACITIES?

The term protection capacities refers to the ability of HRDs, social organisations and communities to continue working for human rights in a safe and sustainable manner, even when faced by the threats or aggressions they receive because of their human rights work.

Protection capacities also have to do with power: “the power to”, “the power to do”. That is, they involve increasing the power of HRDs to make decisions when they are confronted with different alternatives, and the power to take these decisions in safety.

IS IT POSSIBLE TO DEFINE WHAT THE DEVELOPMENT OF PROTECTION CAPACITIES ACTUALLY MEANS?

The development of protection capacities is based on the conviction that every individual, every organisation and every community has certain capacities that enable them to confront threats or acts of aggression. It is, though, frequently necessary to develop and improve these capacities, especially when the risks faced on a day-to-day basis are elevated. These capacities can be developed directly by those who are affected, but external support is frequently useful to help them carry the process out.

No one is born “fully formed”, ready, in the natural course of a life, to face death threats or direct physical attacks. This is why we say that people who defend human rights are ordinary people facing extraordinary situations.

The construction of protection capacities is in large part a collective or organisational process. This is clearly the case for civil society organisations, whether urban or rural, but it is true also of individuals, because human beings learn from each other and alongside others.

This is why we speak of the development of protection capacities at different levels:

- **The individual level:** the protection capacities of each person;
- **The organisational or community level:** the protection capacities of an organisation or a community; and
- **The inter-organisational or inter-community level:** the protection capacities of networks and alliances between organisations or communities.

People who are interested in facilitating the development of protection capacities need to understand three particularly influential factors and to ensure they understand them thoroughly:

- **The ways in which an organisation or a community understands both its context and what it hopes to achieve;**
- **The ways in which this organisation or community understands and interprets the risks it faces as a result of its actions to defend human rights;** and
- **The protection strategy or strategies that it is possible to put into practice .**

HOW ARE CAPACITIES DEVELOPED?

A series of logical steps should be followed when developing protection capacities: they constitute a repetitive process in which learning occurs through reflection and action:

- **Reflection:** Analyse which capacities are needed to achieve protection in different contexts and in the face of different risks, and understand the range of capacities that already exist.
- **Action:** Design and implement a protection plan and evaluate its results permanently, so that it can be modified in the light of emerging needs and what has been achieved.
- **Reflection:** Analyse the results of the actions that have been carried out and decide which capacities need to be developed, or which actions are required to improve protection levels.

And so on...

Nevertheless, it is very important that the facilitator should always bear the following in mind:

- **A repetitive process does not necessarily mean an “ordered” process (see below);** and
- **It cannot be assumed that everything that is done is adequate, or that a given practice is the product of systematic reflection. And even where reflection has been involved it is not always correctly oriented. In other words, there is always room to improve practice through reflection.**

In few words, individual or collective learning requires key moments of analysis and reflection, which can either be internal or be enjoyed with the support of others.

This is why this Guide to Facilitation understands the development of capacities as a process, and why the moments of analysis and reflection are key to the process.

What do these moments of analysis and reflection look like? There might be many, but in order to simplify things, we are going to refer the two that we think are most important:

- **“Protection workshops”;** and
- **“Meetings”** that in one way or another deal with protection matters.

To illustrate the point, these moments of reflection are like the “clearings” in a “forest” of work, of the commentaries, exchanges, complicities, uncertainties, fears and specific activities of HRDs who, if they are to develop protection capacities, must opt to engage in these moments of reflection.

There will be occasions when an organisation decides to improve its ability to protect itself by organising a protection workshop. But there will also be times when a community suffers a security problem and decides, in response, to meet to deal with the issue immediately and then, maybe, to organise a workshop facilitated by outsiders that it hopes will improve its protection capacities. There will be other times when an organisation suffers repeated security incidents and whose members meet after each incident but remain unable to translate their reflections into action. In other words, organisa-

tion might be engaged in a fragmentary sequence of ordered or disordered meetings and perhaps workshops (some planned, some improvised when the need or the opportunity arises) that might occur amid calm or submerged in the stress and fear of events. This is the complicated backdrop against which protection capacities can and should be developed.

THE IMPORTANCE OF POINT OF VIEW AND OF KNOWLEDGE ROOTED IN THE EXPERIENCE OF EACH INDIVIDUAL DEFENDER

The development of capacities is greatly dependent on the experiences and contexts which have marked the development of individuals and groups, because it is in relation to these that we construct our view of the world. It is important we understand that everything individuals do is imbued with meaning derived from their experiences. That is, their actions can be explained with reference to their personal narrative: what is happening (to me) and why I act as I do. In a risk situation it is impossible to separate the management of protection from the management of daily life. Nor can it be hoped that people will approach the risks they face rationally even if they are able to be rational in the ways they seek to examine and understand the whole range of information available to them.

Consequently, it is impossible to impose an external logic of security on the life story of an HRD. According to this point of view there is no such thing as an **objective** risk analysis (because it will always be **subjective**); and it is very difficult to arrive at an “overall” external approach to the subject of protection; those who are able to arrive at this “holistic” view of protection will not be able to achieve a deeply contextualised and culturally rooted perspective on HRDs. HRDs have a partial understanding, but an understanding nevertheless that is profoundly rooted in their realities. And it is from this this rootedness that they construct their protection, in a fragmentary but consistent way.

This is the point on which external facilitators should focus their own subjective viewpoints, alongside those of the HRDs, so that they may get to know and understand their (other) point of view. From this starting point it is possible to seek out the elements that are shared between the two perspectives and to begin to walk together along the same pathway.

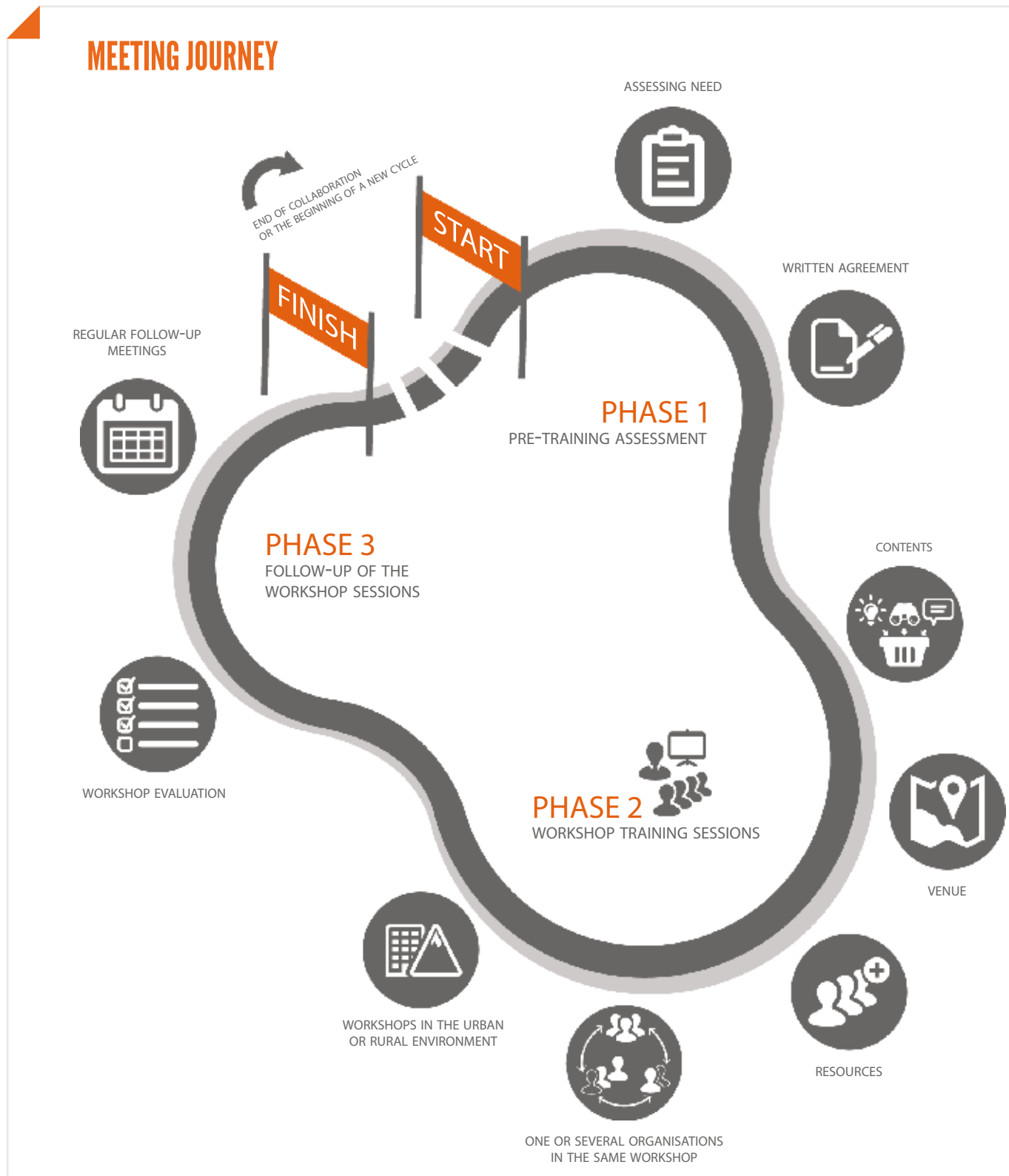
In other words, this Guide to Facilitation invites its readers to abandon any view that the development of protection capacities is “linear”, or that it can be created during one or two workshops whose “lessons” may be “applied immediately”. Very much to the contrary, this Guide promotes a view of the development of capacities as a process inscribed in a context and in a culture, and which follows a mutable and complex route that is subject to multiple influences and interactions. Let us meet each other, then, along the way.

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.



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.

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.

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:

- | | |
|---|--|
| <input type="checkbox"/> Research | <input type="checkbox"/> Anti-Corruption Campaigns |
| <input type="checkbox"/> Capacity Building | <input type="checkbox"/> Journalism |
| <input type="checkbox"/> Publications | <input type="checkbox"/> Advocacy |
| <input type="checkbox"/> Community Development | <input type="checkbox"/> Monitoring |
| <input type="checkbox"/> Conflict Resolution | <input type="checkbox"/> Legal Aid |
| <input type="checkbox"/> Human Rights Education | <input type="checkbox"/> 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 participants reacted to the work of HRDs?

6. Does your work have different implications for male and female staff differently? 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. ?

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. ...

EXAMPLES OF 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).

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?

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 !

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:

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:

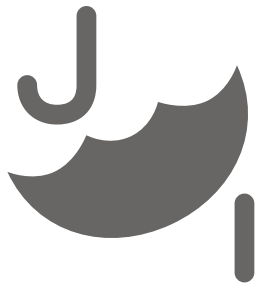
4. Overall evaluation of the support process:

MONITORING PROGRESS

> CHAPTERS 2.1, 2.2, 2.3 OF THE NEW PROTECTION MANUAL

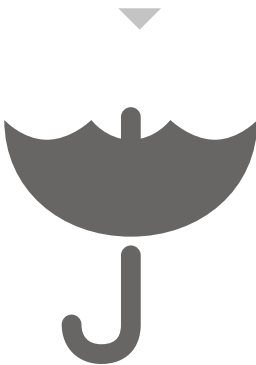
FACILITATORS OUGHT TO MASTER THESE BEFORE READING AND APPLYING THIS CHAPTER OF THE FACILITATION GUIDE

Change or action (whenever it may be needed) is the ultimate aim when supporting HRDs during a capacity building process designed to strengthen their security management. Successful change or action requires attitudinal and behavioural transformations at both individual and organisational levels. The illustration below explains the different levels of sustainable change that HRDs need to attain in order to ensure effective security management.



Straightforward-achievable changes

- Organisation staff/community members acquire knowledge about security management
- Some new security practices are put in place



Deeper changes

- Increased knowledge but, in particular, attitudinal change within the organisation/community and among all staff/members
- More structured security practices in place



Fundamental changes

- Development and implementation of policies and cultural change concerning security management within the organisation/community

However, some questions emerge from this: How do facilitators know that they are doing the right thing and that some progress is being achieved concerning security practices? How do they ensure that they are working toward the goals that HRDs themselves have set? How do facilitators know what works? And how do they account for their efforts?

Monitoring and evaluation (M&E) methods can assist in finding answers to these questions. Applying them in a participatory manner (i.e. involving the HRDs so that they feel ownership of the monitoring process) is crucial if facilitators are to understand the views of those who are currently responsible for the change process.

The essential purpose of monitoring is to gather information throughout the capacity building process, analyse it and feed the insights back in, in order to improve it. **Collecting the right data** will help in:

- **Planning:** how facilitators may best support HRDs over a period of time but also how to assist them in their own security planning: ensuring it is realistic, achievable and relevant and that participants feel ownership of it.
- **Improving implementation:** being able to see what is going well and where changes are needed (e.g. specific technical support to HRDs or changing the format of a training process).
- **Adjusting strategy:** supporting HRDs to review their strategy to ensure it meets their needs.
- **Learning:** understanding why a change has occurred and what it means for facilitators and for the HRDs working to improve their security management.
- **Accountability:** documenting the impact of facilitators' efforts in order to justify the resources used by them and the partner organisations or HRD communities.

Learning and change processes are not linear but the result of interactions and mutual influences between multiple factors and actors, both external and internal to the organisations/communities facilitators are working with. Therefore, if they focus solely on how their support contributes to bringing about change, facilitators run the risk of ignoring how other factors and actors contribute to it. Understanding this also helps facilitators learn about their own work.

But, what data is required and how much? To avoid monitoring turning into an end in itself, facilitators should ask themselves what information they require to effectively carry out their multiple roles of assessor, trainer, coach, guide, partner, sounding board, etc. Thus, it is crucial to make choices between “need to know” and “nice to know”.

The illustration below seeks to highlight the kind of information that can be useful to facilitators throughout the capacity building process and refers to some tools that are provided in this Guide and that can be used to capture and analyse it. Facilitators are encouraged to adapt these to their own needs and those of the HRDs they are working with.

MONITORING AND EVALUATION

	ELEMENTS	RELEVANT INFO GATHERED	USEFUL TOOLS / APPROACHES
ASSESSMENT	<ul style="list-style-type: none"> • Political context (actors & dynamics) • Risk profile • Organizational structure & dynamics • Current security management practices • HRDs reflect on current security management practices and desired change 	<ul style="list-style-type: none"> • Baseline of existing security management practices • Capacity building needs i.e. identifying areas of knowledge & skills transfer to inform training content • Organisational dynamics/ structures to be drawn on in change process 	<ul style="list-style-type: none"> • Assessment form • Security wheel • Training session plan
TRAINING	<ul style="list-style-type: none"> • Participants' log book • Daily evaluation of achievement of learning objectives & quality of facilitation • End of training evaluation: achievement of learning objectives & quality of facilitation • Facilitator debrief for learning 	<ul style="list-style-type: none"> • Risk situation • Key learning points for individual staff • Staff capacity and internal dynamics relevant to identifying change drivers/inhibitors • Effective/ineffective facilitation methods • Areas of improvement for facilitators • Lessons learnt for facilitator/institution 	<ul style="list-style-type: none"> • Participant log books • Daily evaluation exercises • End of training evaluation • Facilitator debrief
PLANNING SESSIONS	<ul style="list-style-type: none"> • Visioning: what change do we want to achieve in our security management? • Formulating action plans • Schedule for follow up meetings/actions with facilitator 	<ul style="list-style-type: none"> • What actions have been taken by whom with what effect? what has worked, what has not worked, and why? How will this influence our ongoing work? • What adjustments are needed to make/keep goals/actions relevant to organisation's needs 	<ul style="list-style-type: none"> • Action plan
FOLLOW-UP (MULTIPLE)	<ul style="list-style-type: none"> • Tailored technical support • Monitoring progress against the action plan • Facilitating review of goals/actions if necessary 	<ul style="list-style-type: none"> • What actions have been taken by whom with what effect? what has worked, what has not worked, and why? How will this influence our ongoing work? • What adjustments are needed to make/keep goals/actions relevant to organisation's needs 	<ul style="list-style-type: none"> • Monitoring template
MONITORING	<ul style="list-style-type: none"> • Description of current security management practice • Evidence of attitudinal change (anecdotal, observations, incident descriptions) • Comparison with baseline • Highlighting learning junctures 	<ul style="list-style-type: none"> • What has changed? • Intended or unintended? • How did change come about? – which /actors contributed, limited? • Individual and institutional change • Lessons learnt • Best/worst practices 	<ul style="list-style-type: none"> • Baseline (from Assessment form) • Monitoring template • Evaluation template

SUPPORTING HRDS IN THEIR PLANNING PROCESS

Training courses on security management are frequently organised following an initial assessment, when HRDs work together with a facilitator to identify the tools that might be required to enable them to analyse their security situation and develop risk reduction strategies. The training process is therefore a means of transferring relevant knowledge and skills to HRDs in the way that is most useful to them.

While training is only one part of a change process and not an end in itself, it is often an eye-opener for the HRDs with whom facilitators are working. Once they have understood that it is possible to influence risks and got an idea of the tools at their disposal to do so, it is now up to the HRDs themselves to decide in much more concrete terms what they want to change about the ways they manage their security and how exactly they intend to do it.

A key responsibility of facilitators involves supporting defenders to make relevant, realistic and achievable plans. Developing grand schemes that cannot be put into practice does nobody any good. Facilitators guide HRDs to adopt a step-by-step approach that takes into account the logical sequence of actions, timelines and responsibilities, and that anticipates possible challenges and identifies potential solutions. This creates an empowering learning experience and a tool that facilitators can use to monitor progress.

A **security plan** is like a **roadmap** that leads HRDs to their intended destination, but they need to know what they require to make sure their journey will be successful. First of all, though, HRDs need to be clear about where they actually want to go. Seemingly easy, it is often a challenge for defenders to formulate what exact change they want to achieve. After participating in a security management training process, defenders will usually have a better understanding of their current risks, capacities and vulnerabilities and a more critical view of their existing security management practices. To help HRDs formulate a goal, facilitators should ask them to describe their ideal way of managing their security. Facilitators should stress that it is important to consider the following aspects: behaviour, attitude, institutional change and the different roles of management, designated security focal points or working group, and other staff.

When working with an entire organisation, the result might look like this:

The program intends to identify security management as a priority for management with clearly defined roles and responsibilities for all staff. The Security Focal Points are knowledgeable about security management and transfer this knowledge to colleagues. They initiate risk assessments and are principally responsible for mapping the security measures, protocols and policies established as a result of the risk assessment, monitoring of implementation and regular reviews.

Management initiates and maintains a security-conscious working culture within the organisation and leads by example. It monitors the implementation of the security plan/security measures and compliance by staff, and supports an internal learning process that feeds into the organisational security management practice. Management identifies the resources required to mainstream security management and sensitises key partners on security management, in order to improve the organisation's protection network. Staff have a common understanding of security management and its application, and contribute to organisational change by complying with security management practices.

When an organisation begins to plan how to achieve its security goal, **it is crucial for facilitators to recognise organisational structures and dynamics as well as individual roles and capacities**. This can be done at the assessment and workshop stages. Within organisations, most staff have clearly assigned responsibilities. Management, program, and support staff have complementary roles. People’s positions are usually also an indicator of their level of influence over decision-making on a day-to-day basis as well as at the institutional level. However, networks, and communities and grassroots organisations in rural areas, may have different hierarchical structures. Thus, facilitators ought to be sensitive to interpersonal relations and profiles of individual staff/members to help them understand informal circles of influence. If they are aware of these aspects, facilitators will be able actively to draw them when supporting the change process. This is particularly important when assigning roles and responsibilities during planning if the overall change process is to be realistic.

Once the organisation has formulated its ideal security management goal, facilitators should support the process of defining the steps that need to be taken to achieve it. **One major challenge for the facilitator at this stage is encouraging participants to break down the steps into small achievable units**. Instead of setting complex tasks that require multiple interventions by many people if they are to be accomplished, breaking things down into smaller units of behaviour, actions or relations will clarify actions and make it easier to identify the resources that are required (time, capacity, materials etc.) to accomplish them.

EXAMPLE:

Instead of stating a general goal, as in **Table A (“bad practice”)**, the facilitator should help the group break the task down into manageable steps with clearly assigned responsibilities and timelines (see **Table B, “best practice”**). This format can help capture all the information required by obliging defenders to think through the answers to the following questions:

- **How** does this action contribute to our overall goal?
- **Who** is responsible for the action?
- **What** is the timeline of the action?

BAD PRACTICE: TABLE A

Action	Person Responsible	Timeline
Improve security management of the organisation	Security focal point	3 months

BEST PRACTICE: TABLE B

Action	Person Responsible	Timeline
Define the role of the Security Focal Point (SFP) clearly and ensure it is understood by all staff members	Management	Immediately
Create space to share security incidents (SIs) and analyse security situation jointly	Management	Immediately
Staff reports on, analyses and reacts to, SIs	All staff	Immediately

Identify existing security management practices	SFP	Within 2 weeks
Develop a budget for staff consultation on security management e.g. refreshments for meetings	Management	Within 1 week
Facilitate an organisational risk assessment exercise involving all staff members & jointly decide on priority areas	SFP & all staff	Within 1 month
Develop draft of day-to-day practices required to reduce identified risks	SFP	Within 2 months
Reflection session with all staff on draft security plan; assign responsibilities for implementation	Management, all staff Facilitated by SFP	Within three
Monitor implementation of security plan	SFP & management	Over the next 2 months
Review of security practices in consultation with all staff in the presence of facilitator; review action plan for next stage of process	SFP, management	After 6 months
Final version of the security plan	SFP	Within 2 weeks after review of security practices

Facilitators can enquire into which aspects the organisation feels it will require further support in drawing up their own work plan. They should agree with the organisation when progress will be checked and how (personal visit, phone, email, etc.). Both facilitators and the partner organisation/community should keep copies of the action plan and use it when monitoring progress during the follow-up phase.

In cases where the entire staff group of the organisation does not attend the planning meeting, facilitators should encourage participants to think about how they will ensure absent colleagues are aware of security management issues. This is vital if the processes agreed to improve organisational security practices are to be inclusive and owned by all.

COLLECTING RELEVANT DATA THROUGH MONITORING

An expansion of the above format can be used by the facilitator during subsequent encounters with the organisation during the follow-up phase, when progress in implementing the plan is monitored.

Action	Person responsible	Timeline	Change observed	Factors (contributing/limiting)	Follow up action to be taken (by whom)
Define the role of the Security Focal Point (SFP) clearly and ensure it is understood by all staff members	Management	Immediately	SFP appointed, TOR developed, approved by Board, announcement to all staff		None
Create space to share security incidents (SIs) and analyse security situation jointly	Management	Immediately	SIs have become agenda items on weekly staff meetings	Sensitive to the importance of SIs	Consider regular absence of field staff during these meetings: how will they participate in discussion of SIs?
Staff reports on, analyses and reacts to, SIs	All staff	Immediately	Information on SIs is shared during weekly staff meetings	Atmosphere of trust and respect within the team	Ditto Format to record SIs needs to be developed (SFP, within one week – share template with her/him) SFP now has authority to act on analysis of SIs – need to sort out decision making responsibilities (Management)
Identify existing security management practices	SFP	Within 2 weeks	Not yet done	SFP busy with other assignments	Management to make adjustments in workload of SFP to ensure effectiveness

It might be overambitious to think that every organisation will be able to achieve fundamental changes to its institutional approach to security management immediately after a training process. It may therefore be advisable to “**start small**” and let the organisation choose two priority risks and to establish an action plan that focuses on improving their capacities to manage them. Once progress has been made and the organisation-wide commitment to security has increased, the facilitator can provide support to help the organisation plan for deeper, more fundamental change over a longer period of time, using the same format.

Throughout their engagement with HRDs, facilitators are encouraged to stay in touch with them, be it through face-to-face meetings when feasible and necessary or by way of other – safe – means of communication. If facilitators encourage regular consultation and are responsive to enquiries and requests they will strengthen their relationship with HRDs, motivating them in their commitment. Providing advice by phone or email, sharing materials, or setting up discussion over Skype are all follow-up actions that facilitators should carry out as part of their contribution to the goals of the HRD organisation or community. During in-person follow-up sessions the facilitator should: **(a) assess progress** towards the action plan and **register information** (on why change has or has not happened) on the monitoring sheet; and **(b) provide whatever technical support might be required** to ensure the steps set out in the plan are carried out, and the overall goal achieved.

By building elements of monitoring into their interactions with HRDs, facilitators have the opportunity to help organisations pause and rethink their goals and strategies and to make adjustments where necessary. Capturing key points from this process can provide essential learning points for facilitators and improve future processes too.

At the end of the process – ideally established according to a pre-defined timeframe - facilitator and HRDs alike should assess whether the objectives have been met and synthesise the learning experience in a way that improves their future working methods.

HOW CAN FACILITATORS LEARN FROM THE PROCESS?

While accountability is often the first thing that comes to mind when mention is made of monitoring, it is the learning opportunities that are most precious to facilitators in their efforts continuously to improve the way they carry out their work. As mentioned above, if they are to learn from the monitoring process, facilitators need to set aside time and employ the resources and tools that will let them capture and analyse information.

Facilitators should ensure that the HRDs from the organisations and communities with which they are working are at the centre of the process. That is, they should play a key role in planning and implementing the process and give their views on progress and on the factors that contribute to success or make it harder to achieve.



BIBLIOGRAPHY

- > David A. Kolb & Ronald Fry (1975). "Toward an Applied Theory of Experiential Learning". In C. Cooper (Ed.). *Theories of Group Process*. John Wiley. London.
- > AI SPA 2013, Barefoot Collective (2011). *Designing and Facilitating Creative Learning Activities, A Companion Booklet to the Barefoot Guide on Learning Practices in organisations and social change*. See <http://www.barefootguide.org/designing-and-facilitating-creative-learning-activities.html>
- > Linda-Darling Hammond, Kim Austin, Suzanne Orcutt & Jim Rosso (2001). *How People Learn, Introduction to Learning Theories*. Stanford. Stanford University School of Education. See <http://www.stanford.edu/class/ed269/hplintrochapter.pdf>
- > Carol Dweck (2006). *Mindset: The new psychology of success*. New York. Random House.
- > Sarah Earl, Fred Carden & Terry Smutylo (2001). *Outcome Mapping. Building Learning and Reflection into Development Programs*. IDRC. See <http://web.idrc.ca/openebooks/959-3/>
- > Kaia Ambrose & Huib Huyse (2009). "Considerations for learning-oriented Monitoring and Evaluation with Outcome Mapping. OM Ideas". Outcome Mapping Learning Community. See <http://www.outcomemapping.ca>

PREPARING THE WORKSHOP SESSIONS

This chapter addresses the preparation and delivery of workshop sessions to develop protection capacities in partner HRD organisations and communities. The chapter is designed to help facilitators prepare the sessions using the New Protection Manual (NPM) as the principal resource. Facilitators should read this introductory part carefully before tackling the sections.

STRUCTURE

Every session is intended to build on previous ones. However, depending on the needs of the partner organisations/communities and on prior agreements facilitators may have reached with them, facilitators may not want to follow the exact order of the Guide. If this is the case, they should be aware that some learning activities will need to be adapted.

REFERENCE TO THE NPM CHAPTERS

Each chapter of this Guide refers to a relevant chapter – or chapters – of the **NPM**.

LEARNING OBJECTIVES

Facilitators will find the key objectives of each session under this heading (i.e. the main concepts and protection methods to be delivered).

KEY MESSAGES

These messages stress the core elements that participants should take out of the session; they are developed throughout the learning activities and in the Tips for Facilitators.

THE SESSION

This section contains suggested learning activities and a step-by-step guide to conducting each session. Facilitators should consider the timetable given as a rough guide. The intention is to provide them with ideas they can use to build their own session. The section includes a list of materials to help facilitators prepare, but they should be creative and use their own proposals. Finally, the section indicates the principal challenges facilitators are likely to encounter when delivering the session (e.g. questions from participants or aspects they might find challenging, etc.). This should help them anticipate difficulties and to prepare for them.

LEARNING ACTIVITIES

This section contains examples of learning activities (e.g. group discussions, role plays, etc.). Whenever possible, the activities have been designed to be used with homogeneous training groups, all of whom come from one organisation, as well as with mixed groups. Examples are applicable both to urban organisations and rural communities.

> **CHAPTER X.X** OF THE NPM
CHAPTER TITLE



LEARNING OBJECTIVES

- > Learning objective 1
- > Learning objective 2



KEY MESSAGES

- > Key message 1
- > Key message 2

THE SESSION

CHALLENGES THAT MAY ARISE DURING THE SESSION :

- Challenge 1
- Challenge 2



THE SESSION STEP BY STEP :

LEARNING ACTIVITIES



ACTIVITY 1



ACTIVITY 2

TIPS FOR FACILITATORS

These suggestions are intended to help facilitators understand how to conduct the learning activities and explain the key points of the session to participants.

 → Tip 1

→ Tip 2

→ Tip 3

ADDITIONAL RESOURCES

At the end of the section, there is a list of further resources that facilitators might wish to explore. These offer further insights into the topics addressed in the **NPM**, as well as additional ideas to create their own workshop.

- > Koenraad Van Brabant (2000). *Operational Security Management in Violent Environments. A Field Manual for Aid Agencies*. Overseas Development Institute. London.
- > Front Line Defenders (FLD) (2011). *Workbook on Security: Practical Steps for Human Rights Defenders at Risk*. Front Line. Dublin.
- > Comité Cerezo Mexico, Fray Francisco de Vitoria O.P., A.C. et al. (2010). *Manual de Introducción. La Seguridad en las Organizaciones Civiles y Sociales*. Mexico.
- > Colectivo ANSUR (2012). *Tejidos de Protección*.
- > Protection International & Udefegua (2009). *Cuidándonos: Guía de protección para defensores y defensoras de derechos humanos en áreas rurales*. Guatemala.



ADDITIONAL RESOURCES

- > Van Brabant. Op. Cit. Chapt (pp. 22-38).
- > FLD. Op. Cit. Chapter 6.
- > Comité Cerezo Mexico et a Cit. Chapter 2. (pp. 31-35).

OVERVIEW OF THE WORKSHOP

The sessions presented in this chapter share a common logic. They all have a similar structure, informed by the sequence of contents in a hypothetical ideal security workshop. However, facilitators are free to omit some sessions, such as those on context analysis or digital security, which, according to circumstances, might not always be necessary. Similarly, the focus of the session dedicated to security networks is largely rural, as it has become apparent that an objective defined in terms of creating a formal security plan is not always appropriate for work with communities or HRD organisations working in isolated regions.

INTEGRAL APPROACH

When speaking of protection and security it is important to maintain an integral approach that takes into account all relevant aspects (physical, digital and psycho-social). Note that digital security includes issues of storage, communication and information management and that each aspect covered is interrelated. However, this does not mean all can be dealt with at the same time. For this reason, facilitators need always to be aware of the integral nature of the training they are facilitating and to be aware at all times of which aspects it might be possible to include, and to decide whether to jointly with participants.

GENDER AND OTHER SOCIAL ISSUES

In the field of protection and security, as in other areas, it is very important to maintain a vision of gender and other social factors that carry with them the risk of exclusion (ethnicity, age, sexual diversity, etc.) and at the same time to follow an integrative and differential approach to identities. While this aspect is highlighted in each session it is important that facilitators apply this perspective critically throughout the whole training process.

1. ASSESSING YOUR ENVIRONMENT

> CHAPTER 1.1 OF THE NEW PROTECTION MANUAL
MAKING INFORMED DECISIONS ABOUT SECURITY AND PROTECTION



LEARNING OBJECTIVES

- > Understand why it is important to analyse the security implications of the work environment.
- > Use different methods to undertake context and stakeholder analysis.



KEY MESSAGES

- > All HRDs may face risks, but not all HRDs face the same risks.
- > The risks faced by HRDs depend on the political context (threats) and their own vulnerabilities and capacities.
- > The political context, and the threats, vulnerabilities and capacities are all dynamic. Risk is therefore also dynamic and may change at any time.

THE SESSION

⚠ CHALLENGES THAT MAY ARISE DURING THE SESSION :

- The methods introduced during the session are intended to capture the complexity of the environment in which the HRDs work and should be adjusted accordingly. Be aware that you will need to familiarise yourself with these working methods before the workshop. They are indeed not easy to grasp at first sight.
- The session requires the facilitator to have a basic understanding of the working context of the participants so that they can initiate the discussion with concrete examples. This information will have been gathered from the pre-training assessment (See [Chapter 3](#) of this guide and [Annex 1 – Pre-Training Assessment form](#)).
- To aid understanding, be as concrete as possible and adhere to workshop participants' own experiences.
- Take into account the specific protection needs of women HRDs (threats, vulnerabilities, capacities and the kind of incidents they are likely to face, etc.).
- Facilitators should consider the particularities of any other relevant social category when assessing risk (for example, indigenous populations, LGBTI defenders, disabled defenders, etc.).
- The composition of the group is important:
 - For homogeneous groups, examples and exercises should as much as possible be drawn from their context.

- For heterogeneous groups (with participants coming from different organisations) examples should capture some of the experiences of each group. Group exercises may need to be devised to explore theoretical examples in order to ensure a common understanding of the issues. Here, the facilitator has the challenge of providing sufficient background and contextual information to the participants for them to be able to carry out the exercises.



THE SESSION STEP BY STEP :

- The methods introduced during the session are intended to capture the complexity of the environment in which the HRDs work and should be adjusted accordingly. Be aware that you will need to familiarise yourself with these working methods before the workshop. They are indeed not easy to grasp at first sight.


Time	Acc. time	Activity	Tool / method / materials
5'		Introduction: <ul style="list-style-type: none"> • Welcome everybody and round of presentations; • State objectives and structure of the workshop; • Explain why it is important to analyse the working context. 	Have the points ready on a flipchart or PowerPoint slide
15'	20'	Lea Learning activity: <ul style="list-style-type: none"> • Discuss the following statement: "All HRDs face risks but not all HRDs face the same risks" • Optional activity if sufficient time is available: visualising the context (if this activity is included, facilitators should adjust the timetable). 	Flipchart Blank cards Markers
15'	35'	Learning activity: asking questions	List of relevant questions in the NPM Flipchart
10'	45'	Explanation of the force field analysis	Force field diagram Flipchart
30'	75'	Learning activity: force field analysis	Cards Masking tape
15'	90'	Explanation of actor/stakeholder analysis	Flip charts Stakeholder matrix
60'	15'	Learning activity: actor/stakeholder analysis	
10'	160'	Conclusions	

TIME KEEPING: CALCULATE 180' (3 HOURS), INCLUDING A 20' BREAK

LEARNING ACTIVITIES

DISCUSSING THE STATEMENT “ALL HRDS FACE RISKS BUT NOT ALL HRDS FACE THE SAME RISKS”

Present the statement to the group and write it up on a flipchart. Invite participants to respond to the statement and have them explain their reasoning. Highlight key elements from their contributions on the flipchart (e.g. the importance of the profile of the defender, geographical location, gender, resources at hand to manage risks, partner organisations etc.). These will be useful for other parts of the session.

-  → This activity usually yields good results and increases the activity level in the room as people discuss the statement and give examples from their own experience.
- The outcome of the discussion provides the entry point to explore why it is important to analyse one's working context. It is vital for participants to understand that they are part of a complex network of actors influenced by political decision-making and to realise that they do not undertake their human rights work in isolation.
- The discussions throughout this session are designed to help participants gain understanding of the issues and actors that impact on their work and on whom their work in turn has an impact. This understanding increases the ability of HRDs to make informed decisions on which security rules and procedures to apply.
- When guiding the discussion, it is crucial not only to reflect from a national/regional perspective, but also to understand dynamics in the particular local context in which participants are working.

VISUALISING THE CONTEXT (OPTIONAL ACTIVITY)

All participants are asked to identify and write down on cards elements of the political, social and economic context that are having an impact on their organisation's – or community's – security. Two or three cards per participant are enough. Each one of the participants should read out their cards and explain why they wrote what they did.

As facilitator you are responsible for organising the cards under different themes on a flipchart or on the wall (you will have to identify the themes that emerge during the session, e.g. political, economic or social context, or any other relevant theme). Finally, you should summarise the outcomes of the session. The cards are left there for the participants to refer to when necessary during the remaining workshop sessions.

METHOD 1 - ASKING QUESTIONS

This is one of the tools that helps defenders to understand and analyse their working environment better.

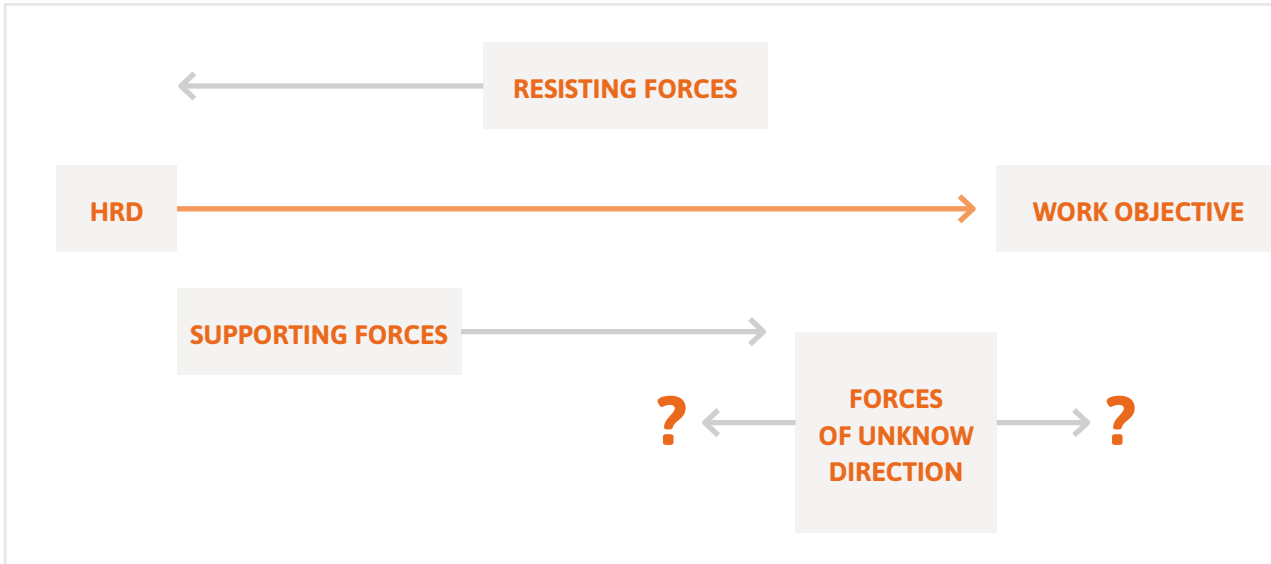
To show the importance of asking questions that will enable you to understand the working environment of participants, **formulate open questions** that encourage participants to find solutions while avoiding those that may lead to simple “yes” or “no” answers. If you are successful in this endeavour you will notice that the discussion will flow naturally. The questions asked will build upon each other, as an answer will lead to other questions.

You can use the list of useful questions in the relevant chapter of the NPM (pp.18-19) to help you. Where possible, develop your questions in reference to the context that is familiar to your participants.

METHOD 2 - FORCE FIELD ANALYSIS

This tool can help participants visualise the forces that support and hinder the work of HRDs. It is based on the assumption that security concerns arise from “resisting forces” and that a security strategy should taking advantage of the strength and influence of “supporting forces” that make it easier for HRDs to pursue their objectives.

To explain the tool, show the following illustration on a flip chart:



To aid comprehension among participants, use examples of work objectives and of stakeholders that are familiar from the participants’ working environment.

Distribute three cards to each participant and ask them to list forces that operate in their working environment. To visualise the analysis, ask them to come forward one by one and to group the cards on the flipchart according to whether they offer support, resistance or whether their effect is unknown; they should explain their choice. Use masking tape to stick the cards in place. Feel free to probe participants further on their choices should you feel them to be superficial (e.g. working on evictions and placing the Church as a supporting force without considering that it owns large extensions of land; or identifying the police as a supporting force, despite the fact it may be linked to illegal actors).

This will generate discussion and is likely to lead to further differentiation between stakeholders and the identification of sub-categories that assume different positions in relation to the work objectives pursued by HRDs (e.g. the media may be further divided into state-owned and private-owned media if they represent different positions).

Questions from participants are likely to arise in relation to the forces of unknown direction. On a case-by-case basis, participants might consider these to be supportive forces, arguing that they do not represent a concrete risk of harming the work of HRDs, or agree to monitor them regularly in order to gauge whether they change their position and come to function either as supporting or resisting forces. In certain circumstances efforts can be made to transform unknown forces into supportive ones, for example by educating them about the objectives pursued by HRDs. This relates to campaigning and advocacy activities.

METHOD 3 - STAKEHOLDERS ANALYSIS

This is the most complex of the three tools and adds an additional layer to the analysis, i.e. the interests of stakeholders in relation to a particular issue and the interrelation between the various stakeholders with which HRDs have contact. This is an important way of increasing the information available when making decisions about protection.

Ask participants to speak about what they understand by the term “stakeholder” and to agree on a definition. Then share with them the different categories of stakeholders as outlined in the **NPM (p. 20)**, summarising their commitments and duties towards the protection of HRDs). To contextualise, let participants name stakeholders from within their own working environment for each of the three categories.

Be aware that the strategies and actions of stakeholders are frequently confused. There is often a considerable gap between the duties of a stakeholder and their actual practice. This exercise is intended to illustrate and analyse the complexity of the context.

Share the four steps of the stakeholder analysis with the participants as outlined in the **NPM (p. 23)** and use local examples to aid understanding.

Create a stakeholders’ matrix to order and facilitate the systematisation of the vast amount of information the context analysis will generate. A lot of space is required for this exercise, so use a large section of the wall or floor (cover the space with flipcharts or divide it up using cards or other markers). Let participants choose a certain number of stakeholders from among the list generated during the force field analysis and help them place them in the matrix as shown in the relevant chapter of the NPM.

For each box that lies at the intersection between the columns and rows corresponding to the same stakeholder participants should fill in:

- the aims and interests of the stakeholder in protecting (or attacking) HRDs.
- stakeholder strategies in relation to the protection of (or aggression against) HRDs.
- stakeholder capacity to attack HRDs, or vulnerabilities in offering protection.
- stakeholder willingness to attack or protect HRDs (low/medium/high).

For the other boxes, i.e. where two different stakeholders intersect, participants should consider the relationships between the two in connection with protection issues and strategy.

Depending on the number of participants in the workshop and their roles, this exercise can involve the whole group (for smaller workshops) or pairs; each pair of participants is assigned two stakeholders and is asked to describe the characteristics of the stakeholders and their relationship to the other stakeholders in the matrix. At the end of the exercise the results should be brought together and overlapping, or absent, descriptions should be discussed in plenary.

At the end of the exercise, ask participants to identify concrete implications of the exercise for their work, and record these points. Possible responses could refer to: a lack of direct contact with stakeholders who have an interest in the protection of HRDs, or the existence of some stakeholders who may be interested in harming HRDs but might be susceptible to influence from supporting stakeholders and the fact that a strategy needs to be developed to exploit this fact.



- This is one of the most complex tools in the manual and participants usually struggle to put it into practice. In order to achieve concrete outcomes it will be necessary to provide good explanations and to accompany the participants closely in the process of analysis. You might want to prepare questions beforehand to feed into the discussion and analysis.
- For actor analysis activities, if you have a small number of participants (up to eight), there is no need to divide them into smaller groups. If you have a bigger group, it is recommended to do so. The workshop might then take longer, as all groups will carry out each one of the learning activities. You will need to adapt the timetable of the session accordingly.



GENERAL COMMENT

- Please note that the schedule proposed in the step-by-step guide to the session only includes one exercise per analysis method. There is no time to use all the learning activities during a single session. If you wish to employ them all, you need to rearrange the timetable. In addition, the different learning activities in this chapter all build upon each other and it is recommended that they be used consecutively.
- To aid understanding, be as concrete as possible and adhere as much as you can to participants' own experiences. Point participants to the interconnectedness of different stakeholders and how this may influence their risks.

CONCLUSION

Ask participants to identify key learning points. This also serves as a summary of the session that will help participants to process and structure the information they have received. As a facilitator you should link this to the previously established learning objectives, using the exercise as a way to evaluate whether they were achieved.

Ask participants about the methods they felt most comfortable with and why. Their answers should help you identify and return to contents that have not been fully understood or that were not clear.

Especially if exercises were based on the actual context familiar to participants, retain the most relevant of the flipcharts produced in the group work and brainstorming sessions. Where there is enough space and a secure environment, the flipcharts can be kept up on the wall of the meeting room as a reference and resource for coming sessions.

At the end of the session, you should have a better understanding of the context of the participants, an insight which should be used to inform subsequent sessions



ADDITIONAL RESOURCES

- > Van Brabant. Op. Cit. Chapter 3.2. (pp. 22-38).
- > FLD. Op. Cit. Chapter 6.
- > Comité Cerezo Mexico et al. Op. Cit. Chapter 2. (pp. 31-35).
- > Colectivo ANSUR. Op. Cit. (pp. 33-35).

2. RISK ANALYSIS

> CHAPTER 1.2 OF THE NEW PROTECTION MANUAL

ASSESSING RISK: THREATS, VULNERABILITIES AND CAPACITIES



LEARNING OBJECTIVES

- > Define the concepts of threat, vulnerability and capacity.
- > Conduct a risk analysis.
- > Take ownership of the concept of risk.



KEY MESSAGES

- > Risk is a dynamic concept, which varies over time and should be assessed periodically.
- > Risk is a subjective concept that is always dependent on the context, capacities and vulnerabilities of the individual defender and organisation. Perception and tolerance of risk may also vary from person to person and from organisation to organisation.
- > Risk is directly proportional to threat. In principle, if there is no threat, there is no risk (yet it is important to get ready in case threats should arise).

THE SESSION



CHALLENGES THAT MAY ARISE DURING THE SESSION :

- Participants sometimes find it hard to distinguish between threats and risks.
- Participants sometimes confuse elements of the context with vulnerabilities.
- English speaking participants sometimes request a differentiation between the concepts of safety and security. Safety can be defined as protection against accidental events; security is protection against intentional damage .
- Take into account the specific protection needs that women HRDs may have (in terms of threats, vulnerabilities and capacities, incidents, etc.).
- Take into account the particularities of any other relevant social category when assessing risk (for example, indigenous populations, LGBTI defenders, disabled defenders, etc.).

 THE SESSION STEP BY STEP :

Time	Acc. time	Activity	Tool / method / materials
5'		Introduction: <ul style="list-style-type: none"> Objectives and structure of the session; 	Have the points ready on a flipchart or PowerPoint slide
15'	20'	Define threat / vulnerability / capacity / risk (risk equation and risk scale). Oral presentation or projection of the video clip about risk analysis. Write down the definitions on flipchart and leave them visible.	Laptop/projector/ext. speakers for video clip about risk analysis Risk equation and/or scale drawn on flipchart
20'	40'	Get to know the concepts of risk, threat, vulnerability and capacity. <ul style="list-style-type: none"> Learning activity 1: Picture risks, threats, vulnerabilities and capacities 	Flipcharts Cards Marker pens Risk analysis illustration
75'	115'	Applying the concepts: <ul style="list-style-type: none"> Explanation of the exercise: Apply the risk analysis to your own organisation/community. Learning activity 2: List threats, vulnerabilities and capacities Learning activity 3: Joint risk assessment 	Chart 3: Information needed to assess a group's vulnerabilities and capacities" (NPM, pp. 32-35)
10'	125'	Conclusion	

TIME KEEPING: CALCULATE 180' (3 HOURS), INCLUDING A 20' BREAK

LEARNING ACTIVITIES

DEFINE THREAT / VULNERABILITY / CAPACITY / RISK

Based on the flipchart showing the risk equation (or scale), define risk, threat, capacity and vulnerability. Depending on the levels of understanding shown by your participants, you can choose either to present them with the definitions as provided in the manual or let the group brainstorm and to arrive jointly at the definitions. If you choose the latter option, be sure to draw out the following key issues that are central to their definition:

- **Risk:** a possible event, which may or may not occur, and which will result in harm or damage if it occurs.
- **Threat:** a declaration or indication of intention to inflict harm or damage.
- **Capacity:** strengths or resources that improve security.
- **Vulnerability:** any factor which makes it more likely for harm to materialise or that results in greater damage.

Alternatively you may choose to show the video explaining the risk equation using a laptop, speakers and projector. At the end of the video, let participants restate the key characteristics of each concept to ensure comprehension.

Once participants have no further questions, proceed to illustrate the concepts.

- Understanding risks is central to successful security management. Therefore this session is at the heart of the entire workshop and it is essential that participants should internalise the concepts before taking the subsequent sessions.
- Explain that risk needs to be unpacked. Otherwise, it can be perceived as too overwhelming a danger by some HRDs. When risk is unpacked, participants realise it is made up of many elements which they can work on separately to minimise risk.

UNDERSTANDING THE CONCEPTS OF RISK, THREAT, VULNERABILITY AND CAPACITY

DEPICTING RISK, THREAT, VULNERABILITY, AND CAPACITY

Choose which representation you feel most comfortable with and that is closest to your participants' experience and contexts:

→ ILLUSTRATION 1 :

Two children are in a small boat on a river, with an adult. The adult is much bigger than they are, and he has a big wooden stick. While one of the two children has a life jacket and can swim, the other has no life jacket, and cannot. The father of the children is watching from the bank of the river, in which crocodiles are swimming.

Instructions: while you tell the story to the participants, draw the scene on a flipchart (or hang a big printed version on the wall). Then ask the participants to identify the threats in the scene, and the vulnerabilities and capacities of the two children.

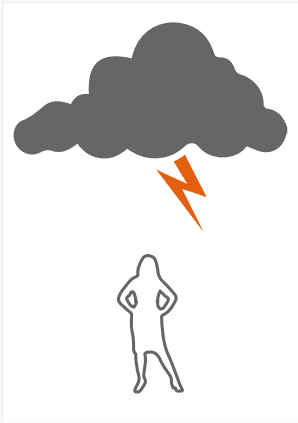


- **Threats:** The adult, threatening to harm the children; the river; the crocodile might eat the children.
- **Risks:** Of drowning; of being eaten by the crocodile; of being hit by the adult if they stay in the boat.
- **Vulnerabilities:** No life-jacket; not knowing how to swim; insufficient physical strength to deter the man with the stick.
- **Capacities:** Life jacket; knowing how to swim; the children's father is watching (if he can take action).

→ **ILLUSTRATION 2:**



Draw a threatening rain cloud on the flipchart. Ask participants what the risks resulting from this threat are and what their vulnerabilities and capacities would be. You can illustrate these in the following way:



THREAT
(RAIN)



RISK
(GETTING WET)



VULNERABILITY
(SHORTS, NO COAT)



CAPACITY
(BOOTS, UMBRELLA, COAT)

→ **ILLUSTRATION 3:**




Copy the illustration below onto a flipchart and put it on the wall (or use a laptop and projector if available). Start by asking the participants what they see in the drawing then to identify risks, threats, vulnerabilities, and capacities (although they might have started to do so when answering the first question, in which case you do not need to ask the questions).



- **Threats:** The two people threatening to push the rock.
- **Risk:** Being harmed or killed by the rock.
- **Vulnerabilities:** Being alone; Not being aware that some people are threatening her;
- **Capacities:** The people represent a community; they are less exposed to the risk than the woman, as they are on the other side of the river, sheltered by the forest and able to see the rock; they could warn the woman of the risk she is facing; the house is a capacity (it is possible to take shelter in it).

Go back to the risk formula (or scale) on the flipchart and show once more how the different components are interlinked: to reduce risk, HRDs need to reduce vulnerabilities deliberately, increase their capacities and try to reduce the threat (better still if the threatening actor stops threatening). Emphasise that vulnerabilities and capacities are internal variables, which defenders can work on.

-  The guide suggests you choose one of the three illustrations to further explain the components of risk. Should you prefer to present two, you need to adapt the timetable of the session.
- Irrespective of the illustration you use, guide participants to identify risks, threats, vulnerabilities and capacities by referring to the definition of these concepts you have developed earlier. Keep the illustrations and definitions pinned up for reference.
- Take into account that for the first and third cases, at least one of the principal threats is intentional. That is to say, the person who poses a threat has the potential to think twice and withdraw it, while in the second case rain is a natural hazard that you cannot “stop”.

APPLY THESE CONCEPTS

If all participants belong to the same organisation or network, you can employ the following learning activity. If the participants come from different organisations and do not share experiences or knowledge, use the example under the section “working with several groups”, below.

LIST THE THREATS, VULNERABILITIES AND CAPACITIES

Once they have understood the concepts of risk, threat, capacity and vulnerability, support participants in applying them to their own situation.

If you have enough participants (at least 12), form three groups. Distribute yellow cards (vulnerabilities) to the first group, blue cards (capacities) to the second group, and red cards (threats) to the third group (if you do not have coloured cards, please ensure that either the letter “T”, “V”, or “C” is clearly written down in a corner of the card, to identify to which category it belongs to). Ask participants to reflect on the work their organisation does.

Each group will spend time working on each of the three concepts, rotating their activities as follows: first round: 15 minutes; Second round: 10 minutes; Third round: 5 minutes. One person in each group acts as the focal point and therefore does not change groups. The focal points are responsible for ensuring the group writes down their organisation’s vulnerabilities, capacities and threats on the cards. As a guide, you can distribute – or project on a screen – Chart 3 (NPM, pp. 32-35).

For a group smaller than 12, all participants should work on the three concepts (vulnerabilities, capacities and threats) at the same time (for about 30’ altogether).

Take into account that a brainstormed idea might be identified as a capacity, but might also be a vulnerability (or vice-versa), depending on the approach and on the context. For example, an organisation must travel to a remote rural area and needs a car. Having a new four-wheel drive car may be a capacity because it will

be safer in terms of reliability/safety, but it might be a vulnerability if common criminals or armed actors are interested in taking “new” cars in the area. On the other hand, relying on public transport may make it more difficult to reach your destination on time, but be safer, as nothing is likely to happen to HRDs that would not be witnessed by other passengers. Therefore, please ensure that the vulnerabilities and capacities identified in the session include some level of detail (perhaps having two cards for the same factor – one as a vulnerability and one as capacity, and explaining why it could be either).

RELATE THREATS TO VULNERABILITIES AND CAPABILITIES

Take two minutes to place the cards where they belong on the risk equation or scale (which should be stuck on the wall). Ask the participants to look at the risk equation/ scale and initiate a discussion. This should help participants visualise the outcomes of the activity.

Then, ask the participants to choose the most concrete threats and to identify the vulnerabilities and capacities that are associated with them. If some vulnerabilities and capacities are related to more than one threat (which is likely), use new cards to create several copies of the same vulnerabilities and capacities, naming the risk associated with each one. You may wish to use the following table:

Activity	Tool / method / materials	Capacities	Risk
List one threat	List vulnerabilities linked to this threat	List capacities linked to this threat	Name the risk associated to this threat
...
...
...

If there are confusions between risk and threat, go back to the illustration you chose at the beginning of the session to help participants in their identification. Encourage debate between all the participants (15 minutes maximum).

WORKING WITH SEVERAL GROUPS

If you have a group of participants drawn from different organisations, with differing experiences and areas of work, you may want to develop a generic exercise participants to practice applying the concepts. One such exercise could be a case study, such as the following, which you should adapt as much as possible to their context:

Two journalists are working in a country torn by civil conflict. One of them is seasoned professional, but the other is quite young (although he has received training in security and protection). They are driving in a car on a secondary road, in an area where military clashes have been reported. The car is not bullet proof. The road surface is in very poor condition and liable to subsidence. There is no police or army presence along the road. The two journalists have told their support network about their trip. They have close ties with Reporters Without Borders and belong to an important national media concern. They are heading towards a community whose members have received death threats from both paramilitary and guerrilla groups. In order to reach the community, they have to go through a zone controlled by paramilitaries, which have links with the Government. When they get to one of the several paramilitary checkpoints, one of the guards tells them in a very ambiguous way: “alright, go ahead, but be careful”.

Then, follow the steps described above (i.e. List threats, vulnerabilities and capacities; and relate threats to vulnerabilities and capacities).

- Adapt case studies to the context of your participants and prepare questions to stimulate discussion.
- If participants confuse elements of context with vulnerabilities, use concrete examples or images to illustrate the difference. Stress also that vulnerabilities are internal to the organisation. If participants confuse elements of context with vulnerabilities, ask the question: “Within such and such a context, what are your vulnerabilities?”
- If participants find it hard to distinguish between threats and risks, use concrete examples or images to illustrate the concepts. It is useful to remind participants of the definition of these concepts. Risk refers to possible events, however uncertain, that may result in harm. A threat is the possibility that someone will harm somebody else’s physical or moral integrity or property through purposeful and often violent action. Thus a risk is the potential harm associated with a threat, given the organisation or community’s vulnerabilities and capacities (hence the utility of the risk analysis).
- The difference between threats and vulnerabilities: a common mistake is identifying “poverty”, “lack of funds” or “misinformation” as threats. It may be more practical to reformulate these as vulnerabilities, i.e. “lack of access to funds” or “lack of access to basic livelihoods” or “lack of access to reliable information”. This is so because this way of wording these vulnerabilities provides a hint about how to transform them into capacities. At the end of the day, risk analysis is a tool for designing a tailored security plan, and we need entry points to begin its elaboration.
- Aggressions go beyond threat, in the sense that harm has already been done. There can be a risk of becoming the target of aggression. The aggression itself might have been preceded by threats (e.g. “if you don’t mind your own business, we will take care of you”), but the threat is different both from the risk and the aggression.
- Participants might feel overwhelmed and ask what to do with the results of the risk analysis. They might want to determine their risk level and come to an agreement about how to respond to it. Be aware, though, that this might lead to endless discussions. Instead, tell them that risk management involves acting in response to threats, vulnerabilities and capacities and that this will be addressed in a more concrete way in subsequent chapters, especially [5.6](#), [5.7](#) and [5.8](#). The activities conducted in this session will then be used in future sessions. So you should keep the results of this session!

CONCLUSION

In plenary you should work with the group to summarise the insights gained during the discussions.

Key elements to draw out are:

- Risk varies depending on the level of threat, but also on one's capacities and vulnerabilities;
- Risk can differ for different actors in the same situation due to different capacities and vulnerabilities ("All HRDs face risks but not all HRDs face the same risks");
- Risk is dynamic and influenced by context – it needs to be re-evaluated periodically;
- Threats are external variables that defenders have limited influence over, but the likelihood of them materialising or having negative impacts on HRDs can be reduced by increasing capacities and reducing vulnerabilities.



ADDITIONAL RESOURCES

- > Van Brabant. Op. Cit. Chapter 3.2. (pp. 22-38).
- > FLD. Op. Cit. Chapter 6.
- > Comité Cerezo Mexico et al. Op. Cit. Chapter 2. (pp. 31-35).
- > Colectivo ANSUR. Op. Cit. (pp. 33-35).

3. UNDERSTANDING AND ASSESSING THREATS



> CHAPTER 1.3 OF THE NEW PROTECTION MANUAL
UNDERSTANDING AND ASSESSING THREATS



LEARNING OBJECTIVES

- > Identify the threats faced by HRDs.
- > Assess the likelihood of threats being carried out, using the five steps described in the NPM.



KEY MESSAGES

- > It is important to distinguish between direct threats (targeted and incidental) and indirect threats.
- > HRDs need to be able to identify patterns, sources and objectives of threats.
- > It is vital to handle the concept of “posing” a threat.
- > Threats always have a psychological effect.

THE SESSION

⚠ CHALLENGES THAT MAY ARISE DURING THE SESSION :

- A reliable threat analysis is only possible when the facts surrounding it have been clearly identified.
- Participants may struggle to identify concrete security measures to be taken on the basis of hypothetical cases, i.e. the conclusions of the threat analysis.
- Participants may argue that they do not have enough information to assess threats.
- Participants may confuse threats with security incidents.
- Participants may talk about potential threats, by which they will actually refer to risks. You will need to clarify the distinction between threat and risk (see Tips for Facilitators in section 5.2. above).
- Take into account the specific protection needs that women HRDs may have (in terms of threats, vulnerabilities and capacities, incidents, etc.).
- Take into account the particularities of any other relevant social category when assessing risk (for example, indigenous populations, LGBTI defenders, disabled defenders, etc.).

 **THE SESSION STEP BY STEP :**

Time	Acc. time	Activity	Tool / method / materials
05'		Introduction: <ul style="list-style-type: none"> Objectives and structure of the session. 	Have the points ready on a flipchart or PowerPoint slide.
40'	45'	What is a threat? <ul style="list-style-type: none"> Explain different types of threat. Identify threats. Explain the difference between "making" and "posing" a threat. 	Flipchart or PowerPoint slide with statements on "making vs. posing a threat". Blank flipchart. Markers. Cards. Masking tape.
60'	105'	How to assess a threat? <ul style="list-style-type: none"> Explain the five steps involved in assessing threats. Learning activity: threat analysis. 	Flipchart (or slide) with the five steps Print-outs of cases to distribute among participants.
15'	120'	Conclusion	

TIME KEEPING: CALCULATE 140' (2 HOURS 20 MINUTES), INCLUDING A 20' BREAK

LEARNING ACTIVITIES

WHAT IS A THREAT?

EXPLAIN THE DIFFERENT TYPES OF THREAT (SEE NPM, PP.39-40):

- Direct (targeting) threat: "Stop messing around or you will end up like your colleague".
- Indirect threats (related to the HRD's work): a partner organisation has just received a death threat; during a press conference a senior Government official accused my organisation of being a bunch of guerrilla collaborators.
- Incidental threats resulting from one's presence in a conflict area.

IDENTIFY THREATS

Ask participants to write down one threat they have received or heard of in the past, on a card. On a flipchart or blackboard, draw two columns, one headed "Direct Threats", and the other "Indirect Threats". Ask participants to determine whether their threat is indirect or direct and to stick it up in the corresponding column using masking tape. Ask participants why they placed their card in one column instead of the other, and engage them in a discussion about the nature of the threat on each card. This will help you to highlight the distinction between indirect and direct threats.

Briefly introduce the concept of security incidents if you find that participants confuse them with threats (See below, Tips for Facilitators).

- Participants might mistake threats for security incidents. It is important to stress that “all threats are security incidents, but not all security incidents are threats”. Threats and security incidents may have different objectives. At a minimum, an intentionally provoked security incident aims to gather information about defenders. Threats are meant to scare defenders and pressure them to abandon their work.
- Participants might talk about potential threats. But most of the time, what they will be talking about are risks. You will need to point out the difference between risks and threats and insist on the fact that a threat has to be something real and concrete. For instance, they might refer to the threat of being attacked. You should explain that this is a risk (i.e. it might happen) but that it is different from a threat, (e.g. “You will end up like your colleague if you carry on like that”). Note that in this case the would-be perpetrator clearly delivered the message that the HRD might suffer the same fate of her/his colleague who was killed or attacked.).

MAKING AND POSING A THREAT

Put up a flipchart with the following statements or project them, and discuss with the group:

- Some people who **make** threats ultimately **pose** a threat.
- Many people who **make** threats **do not pose** a threat.
- Some people who **never make** threats **do pose** a threat.

Draw out the following key elements from the discussion (some examples are provided in the **NPM**):

- A threat is only credible if it suggests that the person behind may (reasonably) be believed to have the capacity to do harm. Sometimes perpetrators try to hide their lack of capacity to act by instilling fear in HRDs. But on other occasions threats by potentially capable perpetrators have a more effective psychological component.
- To react appropriately, you need to know whether the threat can be fulfilled.

- Weighing the capacity of the potential perpetrator (the source of the threat) is important to understand whether someone actually poses a real threat. When issuing threats against HRDs, only some individuals have the intention or capacity to commit a violent act. However, some individuals can represent a serious threat without ever articulating it.
- Point out that the impact of a threat, and an individual’s reaction to it, will differ a) if the victim is reasonably sure that it is unlikely to be carried out and b) if they believe it has some basis in reality. It is very important for the psychosocial well-being of HRDs to be able to assess the feasibility of a threat.

HOW TO ASSESS A THREAT?

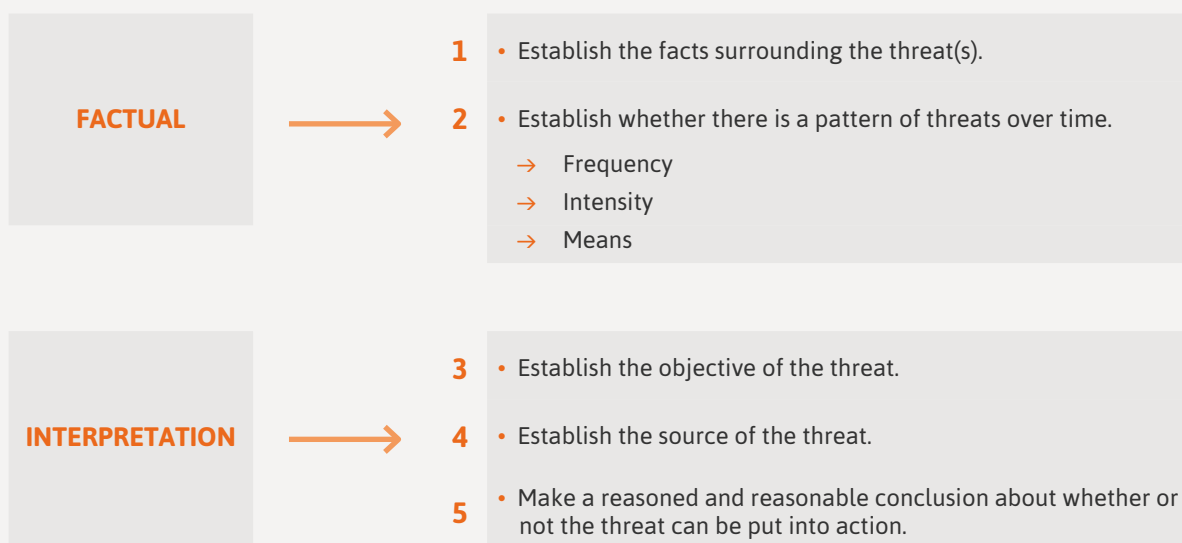
EXPLAIN THE FIVE STEPS INVOLVED IN ASSESSING THREATS

Follow the guidelines given in **NPM (pp. 41-42)**. Write the steps on a flipchart, or project them.

- The five steps are designed to guide this analysis and to ensure that the conclusions are based on a credible interpretation.
It is important to identify the facts surrounding the threats clearly if an HRD is to be able to conduct a good analysis. Indicate that the process has two phases: Phase 1 (regrouping steps 1 and 2) helps identify the facts and patterns surrounding the threats in something close to chronological order.

At this initial stage it is better not to interpret the facts, as they might point to several different causes. The proper analysis and interpretation of the facts is carried out during Phase 2 (steps 3 to 5).


- For Step 2, which involves establishing the pattern, point participants to the elements of frequency (how often have threats occurred, have they been more frequent recently, etc.?), intensity (have the threats become more severe?) and the means employed.
- The analysis evolves over time. It starts with concrete facts, which are then interpreted, before a judgement is formulated. That is, a reasonable conclusion is drawn concerning the likelihood of the threat, based on a clear identification and interpretation of the facts. Hence it is important to follow each of the steps in due order. However, the conclusions reached (step 5) are almost always hypotheses; this is so because all the information needed to reach an undeniable interpretation will never be available. Notwithstanding this, stress that when it comes to designing security measures HRDs should always take action on the basis of the worst-case scenario suggested by the conclusion they have reached. This is not a method for “guessing what might happen”, but for taking informed decisions about what to do when faced by direct threats.



THREAT ANALYSIS

Ask participants to apply the five steps using two or three fictitious cases based on real situations. Print out the examples below and distribute copies to groups of participants. Alternatively, you can use real-life examples drawn from participants' experience or contexts. If you do this, take into account that the emotional aspect of the exercise might be stronger. If the number of participants permits, divide them into small groups (about four or five people each group is ideal).

Participants should then apply the five steps for assessing threats to two different cases or, alternatively, each group can assess one case and present its analysis in the plenary.

-  → Participants might argue that they do not have enough information and that it is difficult to take concrete security measures based on hypothetical cases. However, not having enough information is information in itself. You know that you do not know. Security measures will therefore have to be designed on the basis of this lack of information and on an analysis of the worst case scenario.
- When discussing the result of the group's work on threat analysis, give guidance to ensure all facts are gathered and all possible interpretations have been taken into account. This can be a quite complex and time intensive but is a useful exercise. Some pointers are provided below to facilitate discussion

→ **CASE 1: THREAT AGAINST A FEMALE LAWYER**

A young female lawyer, with very little experience, is hired by the victim's family in a murder case where the defendant is an army officer. For a whole week after the first public hearing of the case, the lawyer receives phone calls at night, during which the caller does not speak and hangs up after a while. Several months pass and due to the sensitive nature of the case, the lawyer, although still working independently, decides to look for support from a human rights NGO. Together, the lawyer and the NGO organise a press conference to explain the case and the progress that has been made. The following night, the phone calls begin again, but this time a voice insults the lawyer ("bitch", "slut", "pig") for a few seconds and then hangs up. A few months later there is another public hearing, preceded by some media coverage over the previous days. The lawyer answers questions from the media inside the court building. One evening in the days prior to the delivery of the judgment, the lawyer receives a phone call from a man, who says: "I was next to you in court today. Next time we are so close together, you will not be so lucky". The lawyer is so scared that the following day she asks for an urgent meeting with the NGO supporting her, in order to analyse the threats.



- **Facts:** an army officer is accused of murder; first public hearing of the case; no military court; victims' lawyer receives first phone calls a week after the public hearing without caller talking; press conference; phone calls insulting the lawyer at night; second public hearing; public declarations of the lawyer on TV; last threatening phone call.
- **Patterns:** phone calls; threats received after public appearances; the "intensity" of the threats increases in a gradual but clear manner (but "intensity" is not equal to capacity to act).
- **Objective:** it was never stated! But it seems to be that the lawyer should stop working on the case.
- **Source:** the information we have indicates that the threats might come from someone who is somehow linked to the case but does not have access to information on the legal proceedings. The threats might come either from actors within the security forces who do not want the army officer to be condemned but can't run the risk of declaring it publicly, or from the army officer's family. From the pattern of the threats we can make an educated guess that whoever is making them does not have access to confidential information on the case. The author of the threats seems to get his/her information only from the media and the public appearances of the lawyer.
- **Conclusion:** we can consider this threat not to be real. The author does not pose a threat, as s/he has not demonstrated any capacity to take action on her/his threats.

→ **CASE 2: THREAT AGAINST A RURAL ACTIVIST**

→ A woman activist, with extensive organisational experience, moves with her family to a rural area. After a few months, she begins helping her neighbours to strengthen the community's internal organisation to help them in their struggle for land rights. The community aims to occupy some land over which they are in dispute with a cattle rancher. Some weeks later, a senior police officer meets the woman's husband and warns him: "If you can't keep your wife at home, then make sure you control her." A few days later, the activist finds a handmade invitation to her own funeral stuck to her front door. Not long afterwards, when they return home one day, she and her husband find the front door open and broken furniture inside the house. When they wake up the next morning, they find that all their chickens have been slaughtered and that someone has left a hand-written note which reads: «You should leave your home after reading this note. Don't bother to make a fuss about it with your friends in the capital. If you decide not to leave, you will end up like your chickens. Signed: Army of the People. God, Order, Fatherland".

- **Facts:** the woman activist moves to the rural region with her family and helps people to defend their land; does the police officer give unsolicited advice or issue a threat to the husband?; first threat (invitation to her funeral); break-in to the woman's house; chickens slaughtered, property destroyed and death threat made.
- **Patterns:** there is a clear increase in the intensity of the threat in this case, from verbal to physical actions that could expose the WHRD to being attacked by the perpetrator. Note the use of symbols and the references to death as well, which are meant to scare the victim and accompany the increase in the intensity of the threat.
- **Objective:** that the woman stop her activities and leave the area.
- **Source:** in this case, it is possible to identify several possible authors, either armed thugs linked to cattle ranchers, cattle ranchers themselves, or state officials who wish to use the lands. Although it may not be clear who is behind the threats, the perpetrators have demonstrated a clear capacity to act. Note that it is not possible to say for sure whether the police officer is threatening or just doing a favour to the husband. In a sexist society, he might just be warning him that his wife's activities might get them into trouble, either because the policeman has heard something or because he is linked to the authors of the threats. It is very ambiguous, and this is why it is important not to assume that things are as they appear to be at first sight.
- **Conclusion:** the threat is real and the next step is likely to be physical harm to the activist or her family.

→ CASE 3: THREAT TARGETING A HRD'S FAMILY MEMBER

Two HRDs go to a small town on one of the regular visits they make every other month to gather information about human rights abuses. IDPs generally come down from their camp to meet with the HRDs on a previously agreed date. These visits generally last for about three days. During the first day of the visit, one IDP tells the HRDs "People have been asking about you". The HRDs decide to carry on with their work. One of the two receives a phone call on his mobile from his young daughter, Lea. The girl is quite worried because she has received an anonymous call saying that her dad has been found poisoned. At the same moment, an IDP approaches the HRDs and hands over a note that reads:

08.30: Lea at school;

13.00: Lea at home;

15.00: Lea volley ball;

17.00: Lea ????????

- **Facts:** HRDs collect information about HR abuses; IDP tells the HRDs that "people have been asking about you"; phone call from Lea (daughter) in distress after receiving bad news about her father; HRD (the father) receives note (with information of his daughter's routine).
- **Patterns:** It appears that the HRDs and their families have been tailed for a while, both in the village, close to the camp, and at home. Both Lea and the HRD have received the same kind of message.
- **Objective:** that the HRDs stop collecting information about IDP-related human rights abuses.
- **Source:** The source is clearly related to people whose interests are affected by the HRDs' activities. With the information at hand, it is hard to tell who they really are. They could be members of militias involved in HR abuses. They have shown some capacity and willingness to act (they have managed to find out where the HRDs live, their phone numbers, and their whereabouts) and they seem to know how to make sure that the HRDs get their messages.
- **Conclusion:** This threat can be considered as a warning; action will be needed to reduce vulnerabilities and increase capacities.

CONCLUSION

Close the session by having participants restate the key learning points.

Relocate this session within the whole security management process by reminding participants of the importance of understanding the context when analysing threats (refer to the concepts discussed in [Chapter 5.1](#) above).

Remind participants of the importance of analysing threats if they are to be able to make good use of the risk equation ([Chapter 5.2](#) above)



ADDITIONAL RESOURCES

- > Van Brabant. Op. Cit. Chapter 3.2. (pp. 22-38).
- > FLD. Op. Cit. Chapter 6.
- > Comité Cerezo Mexico et al. Op. Cit. Chapter 2. (pp. 31-35).

4. SECURITY INCIDENTS

> CHAPTER 1.4 OF THE NEW PROTECTION MANUAL
SECURITY INCIDENTS: DEFINITION AND ANALYSIS



LEARNING OBJECTIVES

- > Learn to notice, identify and assess security incidents.
- > Learn to react to security incidents.



KEY MESSAGES

- > All threats are security incidents, but not all security incidents are threats.
- > Security incidents represent ‘the minimum unit’ of security measurement and indicate resistance to, or pressure on, the work of HRDs: they might be considered to constitute a sort of “feedback” which can help improve HRDs’ security management.
- > Security incidents should be registered, shared, and assessed and, when relevant, proper action needs to be taken.

THE SESSION

CHALLENGES THAT MAY ARISE DURING THE SESSION :

- Participants may mistake threats for security incidents.
- Participants may find it hard to react to security incidents when they only have a few elements to assess them.
- Taking into account the specific protection needs that women HRDs may have (in terms of threats, vulnerabilities and capacities, incidents, etc.).
- Taking into account the particularities of any other relevant social category when assessing risk (for example, indigenous populations, LGBTI defenders, disabled defenders, etc.).

 THE SESSION STEP BY STEP :


Time	Acc. time	Activity	Tool / method / materials
10'		Introduction: <ul style="list-style-type: none"> Objectives and structure of the session 	Have the points ready on a flipchart or PowerPoint slide.
50'	60'	Identifying security incidents. <ul style="list-style-type: none"> Explain the distinction between threats and security incidents (NPM, pp. 45-46). Case analysis. Identifying security incidents in your own environment (optional activity: adjust the timetable if you do it). 	Print-outs of cases to be distributed to participants. Flipchart. Markers.
50'	110'	Assess and react to security incidents. <ul style="list-style-type: none"> Explain the three steps for dealing with security incidents. Role-play. 	The three steps printed out on paper or written down on flipchart/PowerPoint slide. Sample security incidents for the role-play.
10'	120'	Conclusion	

LEARNING ACTIVITIES

IDENTIFYING SECURITY INCIDENTS

 CASE ANALYSIS

Choose one of the following activities (case analysis 1 or 2) or both (in which case you might not want to go through all five examples of case analysis 1).

-  → Participants might confuse threats with security incidents. See Tips for Facilitators – Identifying threats ([Chapter 5.3](#), above).
- This exercise will be useful only in highly insecure contexts in which HRDs are at clear risk and willing to share some information on the topic (it might even be useful to collect information about real incidents for reporting purposes, if participants agree). Otherwise there may not be enough incidents to be shared, and the timeline will not be useful in illustrating the point. If you are not working in a context similar to this one, you may skip this exercise and proceed to the next.

→ **CASE ANALYSIS 1**

Participants work in groups and each group receives a sheet containing the following situations to analyse. Later, discuss the results in the plenary.

Choose the correct answer for each situation and explain your choice:

- A.** It is a security incident.
 - B.** It is a threat.
 - C.** It is just a theft (mobile phones are frequently stolen).
-
- 1.1** *I am at the bus stop, waiting for the bus and talking on my mobile phone. A man approaches me from behind, takes my mobile phone and runs away through the crowd. I recall he had been looking at me some minutes earlier. I also noticed that there were other people talking on mobile phones but that he targeted me. Now I am worried because I stored people's numbers on the phone.*
 - 1.2** *I am walking to my office. At some point I look across the street and realise that someone is staring at me. Suddenly, the man mimics shooting at me with his hand in the shape of a gun. I carry on walking and reach my office without any problem.*
 - 1.3** *I am about to enter my office when I realise that the door is open and that the office has been broken into during the night. The office is a mess. A few computers have been stolen, but some files related to sensitive cases are still on the desks.*
 - 1.4** *My office has been broken into. In the middle of the mess, I find this note: "Next time, we'll take it to the next stage".*
 - 1.5** *I am walking in the street. I cross the street at the next corner. A motorbike going very fast almost knocks me over. There are two men on the bike. The one sitting on the pillion seat seems very upset and tells me to look out when crossing the street and that next time they won't stop.*



→ To help you ensure discussions remain focused on key elements for understanding the distinction between threat and security incident, consider the following model answers to case 1.1. You can build on these for the other four situations:

- If a group chooses answer a): With the information we have, could we not consider this to be a case of simple theft? In truth, you can't be sure whether it is a simple theft or a security incident. As it could be a targeted action, the theft should be classified as a security incident. You have to take all necessary measures to mitigate the risk caused by the theft of private phone numbers and the possible misuse of the phone (in case the thief sells it on the black market or impersonates you for any illegal purpose). If it is just a theft, it is unlikely that anything serious will happen. But when in doubt, you have to react according to the worst-case scenario as this allows you to take better security measures to face the eventual consequences of the theft. So the answer is correct, but for different reasons.
- If a group chooses answer b): See above: Identifying security incidents and threats.
- If a group chooses answer c): Again, the question is whether it is a simple theft or a security incident. You could consider this event as a simple theft, but how can you be sure that, even if the phone was taken without violence or physical harm being caused, it was not an intentional theft associated with the victim's work as an HRD? As you can't be sure (and note, no other mobile phone user near you was mugged), it could well be intentional targeted action, and this is why the theft has to be considered a security incident. As for answer a) it is important to take all necessary measures to mitigate the risk caused by the theft of private phone numbers and the possible misuse of the phone.

→ **CASE ANALYSIS 2****Read the case with participants and discuss it in the plenary :**

A, B, C and D work at the same HR NGO. They are writing a report about police brutality, which will be launched publicly in two weeks' time. On Monday, A goes home from work and notices someone standing opposite the office smiling at her. She dismisses the incident and assumes the person is just being friendly.

The next day, B has lunch in a café next to the office and a man comes in after him, sitting down at a table which is very close to his, even though the café is empty. B dismisses the incident.

On Wednesday evening, C leaves the office for home. A man stops her outside the office and asks for directions. The man also asks her whether she works there and what kind of work she does. C gives the man evasive answers and goes home. She dismisses the incident and doesn't think about it anymore.

On Friday, D, who likes a drink, goes from the office straight to a nearby bar. After five beers he starts a long chat with a friendly stranger in the bar. At some point D asks the stranger to keep an eye on his bag while he goes to the toilet. When D comes back, the stranger is gone. His bag is still there, with the barman, so D thinks there is no problem. When he gets home a few hours later D realises that his office keys are not in his bag. He wonders if he left them in the office and, being tipsy, decides to bother with that the next day. In the morning he receives a phone call, telling him that someone broke into the office last night.



→ If you want to add a bit of humour, give this answer as a joke: "No, the moral of the story is not that you shouldn't have a drink!" Then listen to their answers. Later, explain that even though it is not up to facilitators to tell people not to drink, it is important when dealing with security to realise that drinking or doing drugs can increase risk as, for example, it lowers levels of alertness and makes people careless. The lesson, of course, is that security incidents need to be shared and analysed. In this case, many security incidents had occurred but they were not discussed, so D did not realise that he was vulnerable and at risk when he went to that bar, even though his behaviour there was careless.

→ Assessing and reacting to security incidents (the role-play)

- The idea is that participants should follow the three basic steps for dealing with security incidents. Only guide the role play necessary. The first formal step consists in registering the incident (which participants might skip). Then the analysis should identify the facts surrounding the security incident, its possible authors and sources (which aspect of the organisation's or HRD's work is related to this incident), and its objectives (to gather information, but for what purpose?). Finally, participants need to decide on how to react to the incident: security measures to be adopted, implications for the security plan, actions to be undertaken, etc.
- If necessary, remind participants that they also need to take care of the victim of the incident.
- Conclude the role-play by asking the participants to identify the key points of the role-play.

IDENTIFYING SECURITY INCIDENTS

After the exercise with cases 1 or 2, ask participants to reflect on incidents that might have occurred in their own working environments and that remained unnoticed or that they did not attach much importance to. Underline that it is important to take into account every single incident, no matter how insignificant it may seem. Minor security incidents are often linked to each other and may pave the way for aggressions or more serious security incidents. Be sure to manage the emotions that may be linked to this exercise and ensure that no one is blamed for not reacting or reporting an incident or threat.

Next, distribute cards (red, yellow and green) and ask participants to write down any security incidents that may have occurred within the past year (one incident per card). Serious incidents (which are not necessarily threats) go on the red cards, medium intensity incidents on the yellow ones, and low intensity incidents on the green. Tell participants they need to be concise. They will have time to explain the incidents in more detail during the plenary session.

Use several flipcharts to draw a timeline on the wall representing the year. Write down each month of the year along the line. Ask participants to place the cards with their security incidents along the same line as they remember them occurring. As the participants explain the details of their security incidents, the facilitator should try to guide them in the identification and classification they have given each incident.

At the end of the exercise, support the group in summarising the insights gained regarding the links between different incidents, the information gathered on the interests and intentions of the potential aggressor, and the importance of recording and analysing security incidents.



ASSESS AND REACT TO SECURITY INCIDENTS

Guide participants through the three steps for assessing and reacting to security incidents, as outlined in [NPM \(Chapter 1.4, pp. 47-50\)](#) (you can prepare a presentation or write the steps on a flipchart). Then work on this topic with a role-play.

→ ROLE-PLAY (30 MINUTES)

Story:

A member of your organisation is walking in the street when she notices someone following her. She changes pavement and keeps walking. The man following her does the same. She then turns left and starts walking quicker. She does not see the man anymore and decides to go to the office to drop off a few documents. She is unsure about whether she was actually being followed, so she mentions nothing to her colleagues. When she leaves the office to go back home, having hardly reached the next block, she notices the same man, sitting in a white van with no number plates. She decides to go back to the office immediately and inform her colleagues. All staff members present in the office gather to discuss the incident and decide how to react.

Actions:

Tell participants to simulate a meeting and apply the three steps for dealing with security incidents

Roles:

One person is the witness of the security incident. The other participants play the role of staff members.

CONCLUSION

Close the session by asking participants to recall the key learning points of the session.

Insist on the key messages by coming back to examples or problems that arose during the session.

Replace the session in the context of the security management process. Remind participants of the importance of security incidents (see key messages).

Although security incidents are not necessarily integrated in the risk equation, they must be considered as an indicator of the impact of the defenders' work and their security. Thus, security measures need to be adapted to the security incidents suffered by the organisation.



ADDITIONAL RESOURCES

- > Van Brabant. Op. Cit. Chapter 3.2. (pp. 22-38).
- > FLD. Op. Cit. Chapter 6.
- > Comité Cerezo Mexico et al. Op. Cit. Chapter 2. (pp. 31-35).

5. PREVENTING AND REACTING TO AGGRESSIONS



> CHAPTER 1.5 OF THE NEW PROTECTION MANUAL
PREVENTING AND REACTING TO AGGRESSIONS



LEARNING OBJECTIVES

- > Assess the likelihood of different kinds of aggression taking place.
- > Critically reflect on how to prevent and react to aggressions.



KEY MESSAGES

- > An aggression is the culmination of a process that probably included security incidents, possibly even threats. Thus, in general, it is not an unexpected event. An aggression is the product of three interacting factors:
 - The party who takes violent action and uses violent means to attain her/his goals;
 - Background and triggers that lead the aggressor to see violence as an option; and
 - A suitable setting.
- > Aggressions require adequate resources and capacities and an enabling environment if they are to be carried out. Therefore, the prevention of attacks must address political cost and focus on reducing the physical exposure of the HRDs.
- > Aggressions take time and resources to prepare. It is therefore vital for defenders to detect and analyse any signs that might indicate a possible aggression. These include:
 - Assessing risks ([NPM, Chapter 1.2](#)).
 - Assessing the likelihood of a threat ([NPM, Chapter 1.3](#)).
 - Analysing and reacting to security incidents ([NPM, Chapter 1.4](#)).

THE SESSION

⚠️ CHALLENGES THAT MAY ARISE DURING THE SESSION :

- The session can be emotionally charged if based on real-life cases.
- Participants might find it hard to clearly separate the three interacting factors leading to aggressions.
- Taking into account the specific protection needs that women HRDs may have (in terms of threats, vulnerabilities and capacities, incidents, etc.). Taking into account the particularities of any other relevant social category when assessing risk (for example, indigenous populations, LGBTBI defenders, disabled defenders, etc.).

 THE SESSION STEP BY STEP :

Time	Acc. time	Activity	Tool / method / materials
10'		Introduction: <ul style="list-style-type: none"> Objectives and structure of the session 	Have the points ready on a flipchart (or PowerPoint slide).
20'	30'	Explanation of aggressions <ul style="list-style-type: none"> Aggressions as the product of three interacting factors. Who is behind aggressions? 	The three factors written down on a flipchart (or PowerPoint slide).
45'	75'	Establishing the feasibility of aggressions <ul style="list-style-type: none"> Learning activity: Assess the probability of aggressions 	Tables to establish the feasibility of aggressions (NPM Chapter 1.5). Video about the killing of Marisela Escobedo (http://www.youtube.com/watch?v=QNygrEKedsw).
30'	105'	Preventing a direct/indirect aggression. <ul style="list-style-type: none"> Case analysis: you can either use a real-life case chosen by participants, or use the case proposed below Exercise: planning as the aggressor 	Cases printed out on paper Contextual information about the case analysis;
10'	115'	Conclusion	
TIME KEEPING: CALCULATE 135' (2 HOURS, 15 MINUTES), INCLUDING A 20' BREAK			

LEARNING ACTIVITIES

EXPLANATION OF AGGRESSIONS

Refer to [Chapter 1.5. of the NPM](#) to explain why and how aggressions occur. See also the Tips for Facilitators below. Two main points will guide your explanation:

- Aggressions as the product of three interacting factors (p.53).
- Who is behind aggressions? (pp.53-55)



- Violent aggressions against HRDs have the purpose of causing them to abandon their work by inflicting harm – either directly or indirectly, e.g. by targeting family members. This has not only a physical but also an emotional dimension that needs to be acknowledged.
- When introducing the concept of aggression, underline that violence is not only an act but also a process. A violent aggression against a defender does not come out of the blue. Careful analysis of aggressions often shows that they are the climax of conflicts, disputes, threats and security incidents, which can be traced over time. So the good news is that by being observant, analysing and reacting to security incidents, and putting security measures in place, defenders can significantly reduce the risk of a violent aggression, i.e. they should not feel helpless.


- Outline the three interacting factors that make up an aggression and give examples to help participants absorb them. If possible, choose an example drawn from the participants' experience. Otherwise, you may use the following example:
- **Example:** The work of a WHRD has touched on the interests of a wealthy businessman who engages in large-scale farming and has illegally evicted farmers from their lands. The WHRD has evidence of this. To silence her, the potential aggressor needs to gather information on her behaviour, routines and vulnerabilities. This requires an investment of time and resources. The potential aggressor must take a conscious decision that an aggression against the defender, intended to stop her work, outweighs the possible repercussions this action might have, e.g. prosecution and conviction in the courts. Contexts with high levels of impunity make it less costly for a potential aggressor to carry out a threat, as there may be little or no risk of repercussions for her/his actions. In addition, s/he needs to find a suitable setting to carry out the aggression with limited risks for her/him to be discovered or stopped. S/he will therefore spend time planning the aggression in order to limit eventual negative consequences.

ESTABLISHING THE FEASIBILITY OF AGGRESSIONS

ASSESS THE PROBABILITY OF AGGRESSIONS

Divide participants into three groups, one per theme. Ask them to apply the three tables given in [NPM \(pp.56-58\)](#), "Establishing the probability of an aggression", either to their own environments or to another setting they are familiar with.

Share and discuss the results in plenary (be aware of any sensitivities if there may be trust issues among participants).

-  → To prevent aggressions, it is necessary to be able to analyse the likelihood of their happening. To help participants acquire this capacity, use the tables provided in [NPM \(pp.56-58\)](#). These will help participants to identify the different factors that interact in the development of aggressions and to ponder their relative importance in evaluating the likelihood of different types of aggression occurring (common crime, incidental aggressions and direct aggressions).

EXPLANATION OF AGGRESSIONS

Remind participants that to prevent an aggression it is crucial to:

- Persuade a potential aggressor or a person making threats that an aggression will involve them in unacceptable costs and consequences;
- Reduce the likelihood of aggressions occurring.

Choose one of the exercises below (useful for assessing the probability of aggressions).

For both exercises, divide the participants into small groups (four to five people) for about half an hour, after which each group will present the results of its discussions; then engage participants in a general discussion, in plenary, for about 15 minutes.

EXERCISE 1 - CASE ANALYSIS: THE KILLING OF MARISELA ESCOBEDO (MEXICAN WHRD)

(This video can only be screened if the facilitator has access to the Internet, or if the clip has been downloaded beforehand).

Following the disappearance of her daughter Rubi Frayre in August 2008 (she was found dead in June 2009), Marisela Escobedo had dedicated her life to seeking justice for her daughter. In December 2010, an armed man approached Marisela and shot her while she was participating in a pacifist demonstration opposite the Government Palace, in the city of Chihuahua. A security camera placed on top of the State Government building recorded the killing – which has since become a painful and yet unique testimony. Although the video is in Spanish and there are no subtitles, it is a useful and easy-to-understand visual resource. Some basic facts: Marisela was camping in the park as part of the protest, and at the time of the attack was sitting with a friend at a table on the pavement (on the right-hand side of the screen), opposite the main gate of the State Government building. A white car approaches; a gunman steps out of the car and attacks both Marisela and the person who is with her. Marisela tries to escape and runs across the road towards the State Government building (from right to left), but the gunman shoots her as she reaches the pavement (on the left of the frame). After that, he runs back to the car and leaves the scene.

Ask participants to read the contextual information about this case (which you have printed out on paper), and then show them the video. To analyse this case, ask participants to follow the three conditions necessary to carry out an attack and how each of them could have been influenced to prevent an attack:

- A. The thinking and behaviour patterns used by the individual or individuals who carried out the action.
- B. Why did the attacker imagine that he could “achieve an objective” or “solve a problem” by carrying out the attack? (What is the likely motive for the attack, the nature of the problem, how it was carried out, etc.).
- C. What context or circumstances made the attack possible (describing the place where it happened, how it was carried out, etc.).



- The example is based on a real-life case, but the facilitator might use another case (in written form) if it is relevant and adequate.
- Restate that, to prevent an aggression, it is crucial to: Persuade a potential aggressor or a person making threats that if they commit an aggression the costs and consequences will be unacceptable to them; Reduce the likelihood that an aggression will occur.



EXERCISE 2 – PLANNING AS THE AGGRESSORS

Ask participants to develop an attack plan against an HRD. Knowing how aggressors think is one of the best ways to prevent the possibility of an attack (facilitators can also read section “Surveillance and Counter-surveillance” (NPM, pp.60-62) to guide them in this exercise):

- A. Imagine a scene in which an HRD travels from home to the office every day. The HRD had previously received a death threat; his attackers plan to simulate a mugging, beat him up and, by these means, try to force him to stop working as an HRD. The attackers, who are two individuals paid by a local police officer, do not want to be identified in case they get arrested (draw a plan for the route if possible, etc.).
- B. Imagine the rest of the background information, such as the house the defender lives in, the distance from home to the office, whether s/he uses any transport, whether the attack will take place during her/his free time, etc.
- C. Imagine what you would have to do, in order to prevent such an attack from happening, without having any prior information about it. In other words, what security measures should be adopted to enable an HRD to lower/eliminate the risk of such an attack?

- The second case can prove to be very stimulating, as it requires participants to adopt the point of view of perpetrators. But the exercise should be implemented with great care, as requesting participants to assume this role might cause tensions, or lead participants to overplay their roles. Avoid the exercise if you do not feel comfortable with the group.
- In order to prevent direct aggressions and better understand their logic, it can be useful to put oneself in the shoes of aggressors. This should help participants to get a better understanding of the thinking, behaviours and strategies that aggressors adopt. Aggressions against defenders are often the product of processes of thought and behaviour that we can understand and learn from, even if they are illegitimate. Most people who attack defenders see violence as a “useful” means to reach a goal or “to solve a problem”.

CONCLUSION

Conclude the session by having participants recall the key learning points.



ADDITIONAL RESOURCES

- > Van Brabant. Op. Cit. Chapter 3.2. (pp. 22-38).

6. DRAWING UP A COMPREHENSIVE SECURITY STRATEGY



> CHAPTER 1.6 OF THE NEW PROTECTION MANUAL

DRAWING UP A GLOBAL SECURITY STRATEGY



LEARNING OBJECTIVES

- > Recognise and analyse the protection strategies and tactics HRDs already use.
- > Define a global strategy to protect the HRD workspace.



KEY MESSAGES

- > HRDs and their organisations do not start from scratch when it comes to security issues. Invariably they already have ad-hoc deterrence and protection strategies to handle risks and threats.
- > Not all strategies are able to cover all eventualities as they inevitably have gaps. Every single strategy (ad hoc or formal) needs to satisfy at least the “RASER” criteria: Responsiveness, Adaptability, Sustainability, Effectiveness, and Reversibility.
- > A global security strategy aims to expand and maintain the HRD workspace (working on two axes: tolerance/acceptance of the work carried out by HRDs; and deterrence/persuasion of potential aggressors).

THE SESSION

⚠ CHALLENGES THAT MAY ARISE DURING THE SESSION :

- This is a highly conceptual or “theoretical, western-style” module. If you are working with grass-root HRDs, who have direct experience but limited formal, conventional education, you might prefer to skip this session and go to [Chapter 5.8](#).
- Recognising and analysing ad hoc deterrence strategies and tactics already in place.
- Respecting ad hoc strategies linked to cultural or religious beliefs, while stressing the need to adopt more targeted security and protection measures.
- Getting participants to clearly understand the concept of “the HRD workspace”.
- Taking into account the specific protection needs that women HRDs and any other relevant social category of HRDs (for example, indigenous populations, LGBTI defenders, disabled defenders, etc.) may have in terms of strategies, security norms, etc., both for routine protocols and emergency procedures.

 **THE SESSION STEP BY STEP :**

Time	Acc. time	Activity	Tool / method / materials
10'		Introduction <ul style="list-style-type: none"> Objectives and structure of the session 	Have the points ready on a flipchart (or PowerPoint slide) Use PI videos "Protection strategies" and "Security and protection objectives" for background info
30'	40'	Ad-hoc deterrence strategies and tactics <ul style="list-style-type: none"> Identify security strategies and tactics. Dealing with risk after carrying out an assessment 	Flipchart with RASER criteria of effective security strategy
30'	70'	The HRD socio-political workspace <ul style="list-style-type: none"> Definition of the HRD socio-political workspace Security and the HRD workspace 	Flipchart with the illustration of the two axes of the HRD workspace (NPM, p.69)
40'	110'	Expanding the HRD workspace (global security strategy)	Markers Cards
10'	120'	Conclusion	

TIME KEEPING: CALCULATE 140' (2 HOURS AND 20 MINUTES), INCLUDING A 20' BREAK

LEARNING ACTIVITIES


AD-HOC DETERRENCE STRATEGIES AND TACTICS, AND DEALING WITH RISK

After introducing the main concepts (see Tips for Facilitators, below), help participants identify the ad hoc deterrence strategies and tactics they use in their daily life.

Once you have listed the ad hoc strategies on a flip chart, introduce the six ways of dealing with risk ("accept, reduce, share, ..."; **NPM, p.67**) in order to categorise the participants' ad-hoc strategies.

Depending on the time available, you may choose to analyse one or several of these strategies according to the RASER criteria (see RASER criteria for "analysing deterrence strategy"; **NPM, p.66**). Highlight to participants the potential harm that may stem from any of the strategies falling short of one or more elements of the criteria.

Conclude the activity by pointing out that when HRDs are threatened, stress levels rise and HRDs feel the need to act quickly. However, analysing strategies according to the five criteria will help them choose effective strategies based on a long-term perspective.

-  → Base your introduction to the topic on the ideas covered in the NPM. The PI videos "Protection Strategies" and "Security and Protection Objectives" can be useful for preparing the introduction.
- Individual HRDs, organisations and communities facing threats appeal to different ad hoc strategies

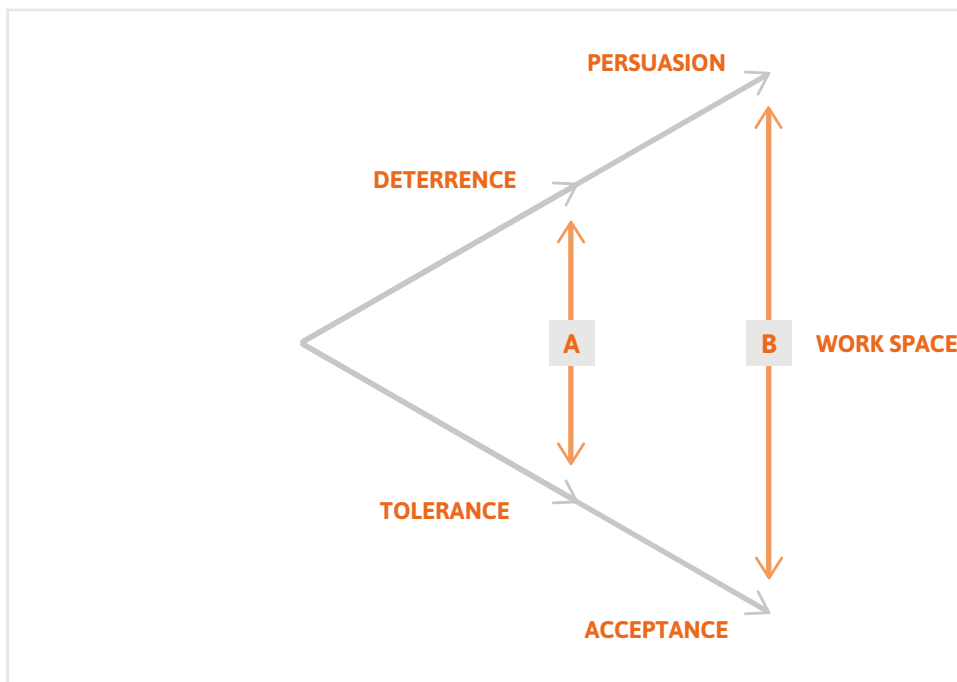
to deal with perceived risks. These strategies will vary according to several factors: environment (rural, urban); type of threat; available social, financial and legal resources; previous experiences; individual subjective perceptions of risk; etc. For a list of ad hoc strategies adopted by HRDs, with examples, see **NPM (pp.65-66)**.

- Remind participants that most ad hoc strategies can be implemented immediately and are intended to achieve a short-term objective. As such, they are more akin to tactics than comprehensive response strategies.
- As ad hoc strategies are deeply subjective, they might not respond to real needs at the individual or organisational level. Thus, HRDs must take care to ensure that they do not harm the wider group, especially if the strategies used cannot be reversed. You should point out the need to develop a long-term perspective on security strategies. In particular, if a security strategy is to be effective it should fulfil the RASER criteria.
- To sum-up, when reflecting on security and protection, HRDs need to take into account both their own as well as other people’s ad-hoc security strategies. However, it is key to strengthen the ones that are efficient while limiting the impact of those that may cause damage to other HRD colleagues.

THE HRD SOCIO-POLITICAL WORKSPACE

Introduce the concept of “the HRD socio-political workspace (**NPM, pp.68-70**). In particular, base your presentation on the definition that appears in the **NPM (p.68)**: “the variety of possible actions the defender can take at an acceptable (level of) personal risk”. In other words, the limits of the socio-political workspace are defined by what an HRD considers to be acceptable or unacceptable consequences of her/his work. You may use, or adapt, the example given in the NPM to explain this idea.

Move on to explain the global security strategy (**NPM, pp.70-73**). For this, use a flipchart with the relevant illustration taken from the NPM to explain the two axes of the HRD workspace (tolerance/acceptance & deterrence persuasion) .



Conclude the section by explaining to participants that a global security strategy should include an advocacy dimension: actions in such a strategy should contribute to raising the political cost of attacks against HRDs and reducing the levels of impunity for potential aggressors.

- The interests of powerful actors (e.g. government, security forces, opposition armed groups, multinational corporations, etc.) may be negatively affected by the daily activities of HRDs. However, it is important to remember that hostile power holders are complex actors: this means that they are not monolithic in their hostility against HRDs (e.g. some elements in the security forces may be committed to protecting defenders while others may be behind threats and aggressions).
- If asked how the “acceptability” of risk can be measured, you should remind participants that it varies greatly between individuals and organisations (e.g. X reached their threshold after receiving one threatening phone call while Y only reached hers after her son was killed) The threshold also changes over time (e.g. two years ago, I did not care if I went to prison, but now I do). Thus, security strategies should expand and sustain the HRD workspace so that they can continue to be able to operate.
- The illustration of the socio-political workspace (NPM) should help you explain that HRDs might work in a very reduced space, represented by situation “a”, or in a broader space – situation “b”. Ideally, the global security strategy should aim at moving HRDs from “a” to “b” by increasing tolerance, acceptance, deterrence and persuasion.
- On the advocacy dimension of the global security strategy: it is key for HRDs to understand their position (workspace) and how to strengthen it (occupying the workspace) by influencing stakeholders and hostile actors.

ACTIVITY: EXPANDING THE HRD WORKSPACE (GLOBAL SECURITY STRATEGY)

The aim of the global security strategy is to expand the workspace by increasing all four of its parameters: tolerance, acceptance, deterrence and persuasion.

Divide participants into four groups (carry out the activity in the plenary if there are fewer than eight participants). Each group will be in charge of proposing a set of actions (min. 1, max. 3) intended to increase one of the parameters. Ask the groups to write down one action per card.

If the plenary group is homogenous, encourage participants to carry out the exercise for their own organisation/community. If it is heterogeneous or there is reluctance to do use a real case, propose a fictitious example (see Tips for Facilitators, below). Troubleshoot any misunderstandings about the exercise.

Return to plenary after 20 minutes of group discussion and use the remaining 20 minutes to ask groups to stick the cards with actions on the wall, grouped around each of the parameters. Let the groups briefly explain the reasons why they believe such actions could help gain tolerance and acceptance from potential aggressors or deter and persuade them. Encourage discussion between groups.

- **Fictitious case:** You work for an environmental NGO that reports on the pollution of a village’s water supply by a paper mill owned by a multinational corporation. The local management – which is also linked to powerful local political bosses – is overtly hostile to the reports published by the NGO. In a field visit two days ago, village leaders told you that there is a rumour that a local politician is planning to hire thugs to teach a “good lesson” to those environmentalists who “put local jobs at risk with their unfounded accusations”.
- When troubleshooting possible misunderstandings during the exercise, refer to the indications given for each workspace parameter in **NPM (pp.70-72)**.

CONCLUSION

Have participants recall the key elements of the session and clarify questions or concerns. Remind participants that a global security strategy does not invalidate ad hoc deterrence strategies and tactics already in place. The idea is to reinforce those that are effective, while trying to limit potentially harmful ones.

Relate this session to sessions 5.1 to 5.5 and explain how it builds on them. Stress the fact that HRDs will only be able to increase their workspace effectively if they have a clear understanding of: their working environment, the identity of the aggressors and their own capacities and vulnerabilities.

End by reminding participants that a global security strategy is intended to expand and maintain the HRD workspace (working on the axes of tolerance–acceptance and deterrence–persuasion). Support your remarks by showing the illustration of the two axes of the workspace again ([NPM, p.69](#)).

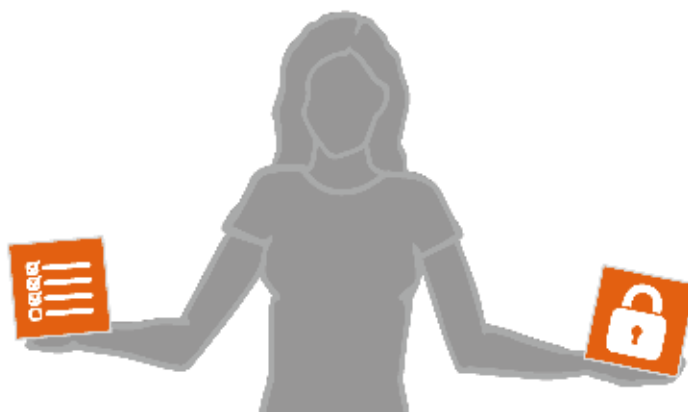


ADDITIONAL RESOURCES

- > Van Brabant. Op. Cit. Chapter 3.2. (pp. 22-38).
- > FLD. Op. Cit. Chapter 6.

7. PREPARING A SECURITY PLAN

> CHAPTER 1.7 OF THE NEW PROTECTION MANUAL
PREPARING A SECURITY PLAN



LEARNING OBJECTIVES

- > Participants identify their own security and protection objectives.
- > Design a security plan.



KEY MESSAGES

- > A security plan helps to decrease vulnerabilities and increase capacities so that threats are addressed – or made less likely, thereby reducing risk. It is preferable to have a simple security plan that defenders will implement than a complex one that they probably will not.
- > A good risk analysis leads to the identification of the main threats, vulnerabilities and capacities, in order to emphasise what is most important in the security plan. In case HRDs do not have much time or many resources, this will allow them to ensure that resources are allocated to priority security issues.

THE SESSION



CHALLENGES THAT MAY ARISE DURING THE SESSION :

- Drafting a realistic and simple security plan, focusing on priority issues.
- Getting participants to accept the plan and indicating to them how to start implementing it in the short and medium term. Taking into account the specific protection needs that women HRDs and any other relevant social category of HRDs (for example, indigenous populations, LGBTI defenders, disabled defenders, etc.) may have in terms of strategies, security norms, etc., both for routine protocols and emergency procedures.

 THE SESSION STEP BY STEP :

Time	Acc. time	Activity	Tool / method / materials
20'		Introduction: <ul style="list-style-type: none"> • Objectives and structure of the session • Objectives of security measures 	Have the points ready on a flipchart (or PowerPoint slide)
90'	110'	Drafting a security plan	Results of risk analysis carried out in session 5.2 Flipcharts from session 5.2 Flipcharts Markers Table templates for designing a security plan (can be either projected from a laptop or prepared on flipcharts)
10'	120'	Conclusion	

TIME KEEPING: CALCULATE 140' (2 HOURS AND 20 MINUTES), INCLUDING A 20' BREAK

LEARNING ACTIVITIES

 OBJECTIVE OF SECURITY MEASURES

To introduce this session, state the three general objectives that a security plan should contain:

- Someone stops doing something, i.e. the aggressor does not threaten or attack HRDs.
- Someone does what s/he has to do, i.e. the legitimate authority prevents aggressors from harming human rights defenders.
- HRDs become less vulnerable and increase their protection capacity.

Use examples drawn from the participants' own experience to illustrate these three objectives. Then remind participants of the risk equation (See [NPM](#) and [Chapter 5.2. of this Guide](#)). Point out that the first two objectives refer to threats and the last one to vulnerabilities and capacities. You should also stress the fact that the first two objectives are linked to their capacities. Indeed, the measures they take will increase their capacity to deter or dissuade potential aggressors.

 DRAFTING A SECURITY PLAN

Developing a full security plan is a complex activity that requires considerable time. In this exercise, you will just focus on how to design a simple security plan based on the priorities established by an organisation's risk analysis.

HOW TO WORK :

This work is based on the risk analysis carried out previously. When training a homogenous group, refer back to the results of the risk assessment exercise from [Chapter 5.2.](#) (see the Tips for Facilitators if working with mixed groups). Make sure you have the flipcharts from this exercise at hand to facilitate the process.

- Select the most specific threats:** Participants choose the most serious threats or the ones most closely related to their principal vulnerabilities, because they face greater risks from these threats (See [NPM, Chapter 1.2](#) for hints and clues). (10 minutes)
- Re-assess vulnerabilities:** Give participants a few minutes to re-assess the vulnerabilities they have previously associated with selected threats. Make adjustments where you think this is necessary. You should focus in particular on these associated vulnerabilities when planning actions to reduce the risk that the selected threats will materialise. And remember, not all vulnerabilities are associated with every threat. (10 minutes)
- Re-assess capacities:** Ask participants to carry out the same exercise for the list of capacities they previously associated with the selected threats. (10 minutes)
- Turn vulnerabilities into “objectives” in the security plan:** see table below for guidance (the example does not claim to be exhaustive). (30 minutes)

Threat	Objective	Vulnerability (related to the threat)	Objective
“Break-in – other offices have been broken into”.	<p>“To reduce the possibility of a break-in at our office”.</p> <p>“To reduce the negative impact of a break-in at our office should it occur”.</p>	“We have sensitive information stored on the office computers”.	<p>“Even if a break-in occurs we prevent:</p> <ul style="list-style-type: none"> the loss of information stored on the computers and; unauthorised people from accessing that information”.

- Develop each objective:** Write down actions that could be taken to achieve the objective. Draw the attention of participants to the fact that security measures should include preventive actions and reactive measures. Those objectives and actions will constitute an outline of the security plan (30 minutes). For example:

Objective	Actions
“To reduce the possibilities of a break-in at our office”.	<ul style="list-style-type: none"> Together with other organisations, issue a public statement denouncing the number of break-ins experienced by organisations, and demanding that the government put measures in place to stem them. Put pressure on the relevant authorities (police and legal) to investigate the motives behind the break-in and who was responsible, and to bring them to justice.
<p>“Even if a break-in occurs we will not lose the information stored in the computers and other people will not have access to that information”.</p> <p>Note: This objective relies on organisations having the support, through networking, of external IT teams.</p>	<ul style="list-style-type: none"> To set up a computer network with a central server. To regularly make backups/copies of the central server hard drive and keep the copy in a safe or protected place, external to the office. To install a secure and simple encryption program for the central server, so that even if the hardware is stolen, the information stored in it cannot be used.

6. List all actions to be taken in the form of a plan: For this, project the table presented below onto a screen. Use the example provided or use one derived from the group's own experiences. Alternatively, write key elements on a flipchart to guide participants later on in their group work. Ask participants to form groups of 4-5 people and assign an equal set of selected threats to each group. Each group is to develop security measures for every threat that is assigned. To make this a realistic/operational plan, emphasise that it is important to give each action a deadline, and to assign responsibilities. Later, each group should present its results in the plenary, and the proposed actions should be discussed in plenary. At the end of the exercise, they will have the outline of their security plan.

The more time you have to spend on this exercise, the more concrete a plan can be produced, which the organisation can begin to work on immediately after the training.

The following table illustrates further elaboration of the plan using the same example:

Objectives					
Comprehensive (related to threats)	Specific (related to vulnerabilities)	Security measures	Responsibilities	Costs	Timetable
"To reduce the possibilities of a break-in at our office"	"Even if a break-in occurs we prevent: <ul style="list-style-type: none"> • loss of information stored on the computers and; • unauthorised people from accessing that information" 	Classify which information is sensitive to take additional steps to protect from unauthorised access	Programme officers and management	\$0	Within 3 months
		Build a computer network with one central server at the office – the latter must not be easily accessible to outsiders	IT officer/ external IT consultant	\$0	Within 3 months
		Buy external hard drive	Finance officer	\$200	Within 2 weeks
		Make backups/copies of the central server hard drive once every week	Information/ communications officer	\$0	Every month
		Keep a copy of the back up in a safe or safe place (external to the office).	Programme Manager	\$0	Every six months
	Identify, learn how to use and use a simple encryption program	Information/ communications officer	\$0 (if using open software)	Within 2 months	

Internal training on the encryption program & strong passwords	All	\$0	Within a month
Install encryption program for the central server and the backup, so that even if both are stolen, the stored information cannot be accessed	Information/communications officer	\$0 (if using open software)	Within 2 weeks
Together with other organisations, issue a public statement denouncing the number of break-ins experienced by organisations, and demanding that the government put in place measures to stem them	Information/communications officer	\$0	Within a month
Put pressure on the relevant authorities (police and legal) to investigate the motives behind the break-in and who was responsible, and to bring them to justice.	Advocacy Officer	\$0	Immediate

 → **Share the following insights with defenders about initiating the process of preparing a security plan:**

- **A security plan is only useful, if implemented:** Having a security plan does not automatically reduce risks. Plans need to be shared, explained and implemented to have an impact on the security of defenders.
- **Security management is a dynamic process that evolves, and requires regular evaluation:** Risks are dynamic, as they depend on an environment that is ever-changing; a good plan today may no longer be appropriate in six months' time. If the situation evolves, defenders should review their analysis and plan. Security management should be understood as a permanent process, based on the analysis of changing threats, vulnerabilities and capacities, as well as the socio-political context.
- **Security plans must be realistic if they are to be effective:** An effective security plan must take into account a realistic timeframe and the organisation's capacities. If the plan is too ambitious or demanding, it runs the risk of being shelved. Your role as facilitator is to ask questions that help defenders to assess whether their planned actions are realistic and achievable.
- **Security plans should encompass a reactive and a preventive dimension.**

→ **Difficulties when carrying out the activity on drafting a security plan:**

- You may be working with a large list of threats and vulnerabilities and this creates difficulties. Once you have selected the threats, only the vulnerabilities directly related to them should be selected. This will make the exercise easier. It will also allow the plan to target priority security issues. See NPM Chapter 1.7. for concrete examples.
- If you have a mixed group, you will need to make up an example or divide participants into groups

(each group corresponding to one organisation). An easy way would be to build on the activity conducted in Chapter 5.2. of this guide. Bear in mind that if there is a lack of trust between participants, it may be difficult to share details about risk analysis and about real security plans (hence the utility of working on fictitious examples). However, each organisation should do its homework so that it can define its own security plan following the workshop.

- Participants might mistake objectives for actions. This should not be a problem as long as they manage to define relevant and concrete security measures. So, do not waste too much time on conceptual clarifications. Your efforts should instead be focused on reaching concrete outcomes.

CONCLUSION

- > Ask participants to recall the key learning points.
- > Remind them of the importance of integrating the previous activities covered in the sessions on security management (context analysis, risk assessment, threat and security incidents analysis) into the design of the security plan.
- > Remind participants that reading the relevant chapter of the NPM will be useful for the details of the work ahead.



ADDITIONAL RESOURCES

- > Van Brabant. Op. Cit. Chapter 3.2. (pp. 22-38).
- > FLD. Op. Cit. Chapter 6.

8. PROTECTION NETWORKS FOR HRDS BASED IN RURAL AREA COMMUNITIES

> PI & UDEFEGUA (2009). CUIDÁNDONOS: GUÍA DE PROTECCIÓN PARA DEFENSORES Y DEFENSORAS DE DERECHOS HUMANOS EN ÁREAS RURALES. GUATEMALA. PP. 89-113

THIS SESSION IS DESIGNED EXCLUSIVELY FOR GRASSROOTS COMMUNITIES AND ORGANISATIONS. IT BUILDS ON CHAPTERS 5.1 TO 5.5. AND PROVIDES AN INTRODUCTION TO COLLECTIVE SECURITY AND SECURITY MANAGEMENT FOR THESE HRD POPULATIONS



LEARNING OBJECTIVES

- > Strengthen collective capacities to deal with the risks faced by HRDs working with communities in rural areas.
- > Understand the dynamics of protection networks.



KEY MESSAGES

- > Collective security management in remote areas where inhabitants are scattered over large territories requires organisation and coordination.
- > Sharing the risk is easier if community bonds are strong.

THE SESSION



CHALLENGES THAT MAY ARISE DURING THE SESSION :

- Building on the work of previous sessions, especially those dealt with in Chapters [5.2](#) and [5.6](#) of this Guide.
- Finding sufficient space to conduct the session. Make sure that a sizeable room with plenty of wall space is available as you will need to display a large number of cards, flipcharts and other relevant materials.
- Adjusting protection strategies in remote areas to the protection network approach.
- Adapting the contents and concepts of the session to participants with low-level formal education; including some who are illiterate.
- Taking into account the specific protection needs that women HRDs and any other relevant social category of HRDs (for example, indigenous populations, LGBTI defenders, disabled defenders, etc.) may have in terms of strategies, security norms, etc., both for routine protocols and emergency procedures.

 THE SESSION STEP BY STEP :

Time	Acc. time	Activity	Tool / method / materials
10'		Introduction: <ul style="list-style-type: none"> Objectives and structure of the session 	Have the points ready on a flipchart*
60'	70'	Security strategies and security measures <ul style="list-style-type: none"> Review of risk analysis (15') What is a security measure? What is a security strategy? (15') Activity 1: Designing security strategies (30') 	Flipchart with risk scale Flipchart with RASER criteria of effective security strategy. Flipchart with table of Security Measures (see below) Blank flipcharts and markers. Use PI videos "Protection strategies" and "Security and protection objectives" for background info
140	210'	Protection networks. <ul style="list-style-type: none"> Activity 2: Walking together exercise (30') Explain protection networks (30') First collective reflection on protection networks (10') Activity 3: Social networks and fishing nets (20') Activity 4: Story(ies) about communities (15') and final collective reflection on the story(ies) (35') 	Telephone Table Enlarged picture of protection network Stickers/cards with the different elements of the protection network (arrows, Objective; Protection network committee; Analysis and Early Warning Commission; Our community; Other community; National Human Rights Institutions; National/ International support organisations; International institutions) Enlarged picture of a fishing net Print-outs of the stories
10'	220'	Conclusion	
TIME KEEPING: CALCULATE 240' (4 HOURS), INCLUDING A 20' BREAK			

* Laptop, projector and external speakers are optional although you may have difficulty in accessing power sources in remote areas.

LEARNING ACTIVITIES


RISK, SECURITY MEASURES AND STRATEGIES

REVIEW OF RISK ANALYSIS

Base this part of the session on the risk analysis that the participants carried out previously (see [chapter 5.2](#) of this Guide). Remind participants of the results of the risk analysis by hanging the risk scale and the results of their previous work on this topic on the wall. Explain that security measures should be designed according to the results of the risk scale.

WHAT IS A SECURITY MEASURE? WHAT IS A SECURITY STRATEGY?

The idea here is to provide participants with some examples of security strategies and security measures, adapted to community and individual needs. Hence, your intervention should be based on the methods and activities described in [Chapter 5.6](#) of this Guide. In particular, point to the need to develop security strategies that allow HRDs to deal with risk while continuing to work and get on with their lives in a safe environment. Move on to present the six security strategies for dealing with risk ([NPM, p. 67, and Guía Cuidándonos \[not available in English\] pp. 15-22](#)).

-  → One good approach to ensure a useful discussion when you explain the six strategies for dealing with risk is to ask participants whether they have used one of them in the past themselves. Although they might not have recognised them as such at the time, they might now realise that their reaction to a situation they faced in fact involved one of the strategies examined in this session. Depending on the time available, choose one or more of these ad hoc strategies and analyse them according to the RASER criteria.
- You can also provide concrete examples of security strategies that appear in *Guía Cuidándonos* (pp. 104-111).
- Conclude the activity by pointing out that when HRDs are threatened, stress-levels rise and HRDs feel the need to act quickly. However, analysing strategies according to the five criteria will help them choose effective strategies based on a long-term perspective.

ACTIVITY: DESIGNING SECURITY STRATEGIES

Form as many groups as required to analyse the threats and security incidents that were identified previously (usually between two and four). Groups need to be more or less equal in size.

Each group analyses one threat or security incident (to simplify matters, you may group threats or security incidents that share similar patterns) and tries to come up with security strategies to address them. Give blank flipchart papers to each group and ask participants to copy the “Security Measures” table below and to fill it in for the case they have been assigned.

Specific threats/ security incident or patterns	Vulnerabilities	Capacities	Measures	Responsibilities	Timetable
...
...

After the groups have finished filling in the tables, bring the participants together in plenary and ask representatives from each group to stick their flipcharts up on the wall and present their work. Encourage the other groups to ask questions or to comment on the results. On the basis of the discussion, participants should either accept the security measures or propose new ones. Insist on the need to define priorities, assign responsibilities and agree on a realistic timetable.

PROTECTION NETWORKS

Before introducing the concept of protection networks, introduce the following exercise :

ACTIVITY 2: WALKING TOGETHER EXERCISE


This activity helps participants realise how difficult it is to walk together. Organisation and leadership are instrumental to good coordination.

Place a phone on a table in the centre of the room and ask participants to form two groups (of equal size).

Each group gathers separately, 10-metres apart from each other and from the phone. Tell each group that every participant must touch and hold the ear of a second participant and the knee of a third, forming a human knot. Then tell each group to move towards the phone, without letting go of each other, so they can make an emergency call.

If the groups let go without reaching the phone, give them another opportunity. Tell them to think about how they might be able to reach the phone without breaking the knot. The activity ends when one of the groups reaches the phone or when both let go for a second time. Pay attention to the difficulties that arise during their attempts to move as a group.

To sum the exercise up, engage the group in a collective reflection: ask participants how they felt during the activity and why they did or did not manage to reach the phone. If the groups do not mention it, explain that the knot symbolised a network. This knot makes it difficult to walk together (bring up some of the difficulties you observed). However, if they get organised and create a leadership model that brings them together, they will be able to move together, reach the phone to call for help.

 → Consider this activity as an energiser, but also relate it to security issues. Stress the importance of community cohesion for the management of security.

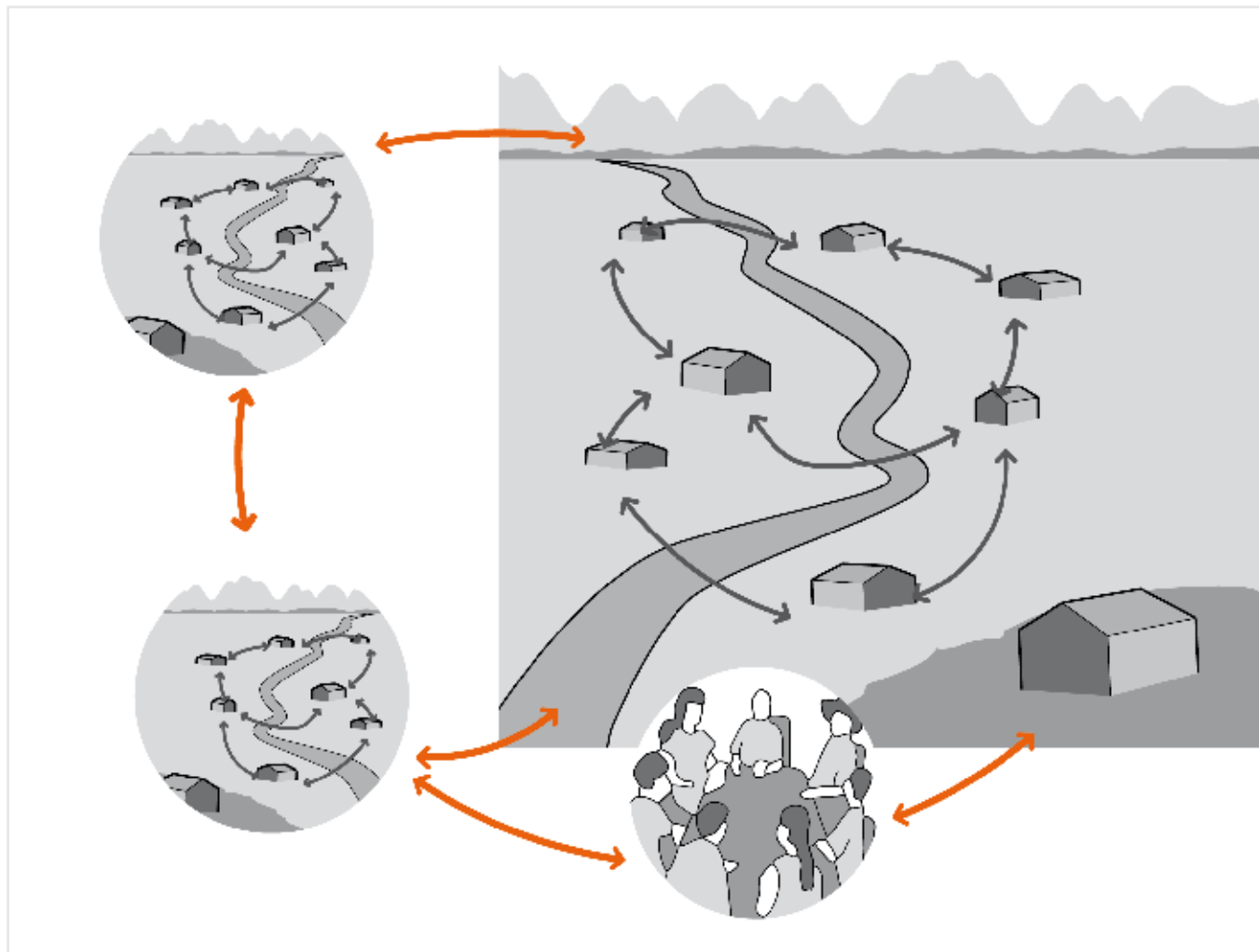
EXPLAIN HOW PROTECTION NETWORKS WORK (CUADERNO CUIDÁNDONOS P. 89-113).

Hang the enlarged picture, below, on the wall to illustrate the concept of protection networks.

Use the picture to describe how an ideal protection network would look. Place the cards/stickers with the different elements composing a protection network on and around the picture as you mention them (use the illustration in [Guía Cuidándonos, p.97](#), for further guidance).

Explain what a protection network is (see the relevant Tip for Facilitators for guidance). The **objective** of protection networks is to protect HRDs working with communities/grass-roots organisations and to defend their territories (place the sticker covering the objective of protection networks on the picture).

Every community creates its own **protection network committee** (place the corresponding sticker by the big house in the bottom right hand corner of the large green area). The committee is responsible for the coordination and decision-making on matters of security and protection. It ensures that security measures are respected and monitors security and protection issues.



It is crucial to develop and maintain regular high quality communication with other organisations to ensure the protection of the community. This includes other communities, National Human Rights Institutions, national and international organisations and international bodies (place the corresponding stickers on the picture: the other communities are represented by the small green areas to the left of the main community; the other organisations should be placed at the ends of the red arrows).

Some members of the protection network committee should be appointed as liaison officers with these other organisations. Once the protection network is extended to other organisations, it should be possible to create a second coordination committee gathering all the actors who support the community. This is called the **Analysis and Early Warning Commission** (place the corresponding sticker by the circle with the people involved in a meeting). This commission is made up of a community representative (who is also a member of the protection network committee), and members of other communities and organisations. These persons should have good analytical skills and enjoy the trust of the community.

Three stages can be distinguished in the security management process of protection networks: **a)** information; **b)** analysis; **c)** decision-making. These stages should be followed at all three levels of security management: **1)** the individual level; **2)** the community level; and **3)** in external coordination with other organisations or communities.

→ **A. INFORMATION:**

The community should make conscious efforts to gather information about what is happening in its territory and share it within the community, using effective channels of communication (refer to the blue arrows in the illustration).

→ **B. ANALYSIS:**

Based on this information the community should reach its own conclusions about the risk faced. This is the risk analysis stage. Remind participants of the context and risk analysis methods seen in the sessions based on chapters 5.1 and 5.2 of this Guide.

→ **C. DECISION-MAKING:**

Decisions on security measures should be made on the basis of the risk analysis. At the **individual** level, each community member should pay attention to the environment (remind participants of the session based on [Chapter 5.4](#)) and analyse the risks they face. All the information gathered should be communicated to the protection network committee. At the **community** level, each member is responsible for gathering information about threats and security incidents suffered by the community. This level is crucial, as this is where control over the territory is asserted. Again, the information gathered should be shared with the protection network committee, which will analyse it and take the necessary collective measures to protect the community and organise a response if needed. Finally, at the **external** level, the information gathered should be communicated to the Analysis and Early Warning Commission. This body carries out the global analysis and decides on the security measures and actions to be taken, if required. The community representative on the Commission communicates the analysis, information and alerts to the community.



- The aim of protection networks is to protect HRDs working in rural communities and their workspace. The concept is based on the idea that protection, if it is to be effective, must originate in the community and/or grass-roots organisation themselves in order to ensure that all the efforts and activities that they carry out are brought together. Protection strategies and measures aimed at ensuring the safety of inhabitants/members are thus embedded in the defence of their territory, which is defined in political and geographical terms.
- Protection networks may be described as collective efforts/responses within the community, and between the community and other external organisations, to respond to the risks – and repression – they face as a result of their actions in the defence of their human rights.
- Effective organisation is at the heart of protection networks.

FIRST COLLECTIVE REFLECTION ON PROTECTION NETWORKS

After this rather conceptual section on protection networks, participants should be encouraged to discuss and reflect on protection networks, explaining the concepts again if necessary. Facilitators may use real life experiences to illustrate the explanations (the [Guía Cuidándonos](#) includes a number of cases from Latin America).



The discussion might arrive at the following conclusions:

Protection networks are useful for:

- Get to know and analyse the information that communities require to protect their territory.
- Share this information.
- Be able to develop judgements and take decisions to protect the community.
- Seek alliances with others who share the same goals.
- Carry out joint actions.
- Resist.

Once the discussion seems complete, move on to the following activities, which can help you further illustrate the concept of protection networks:

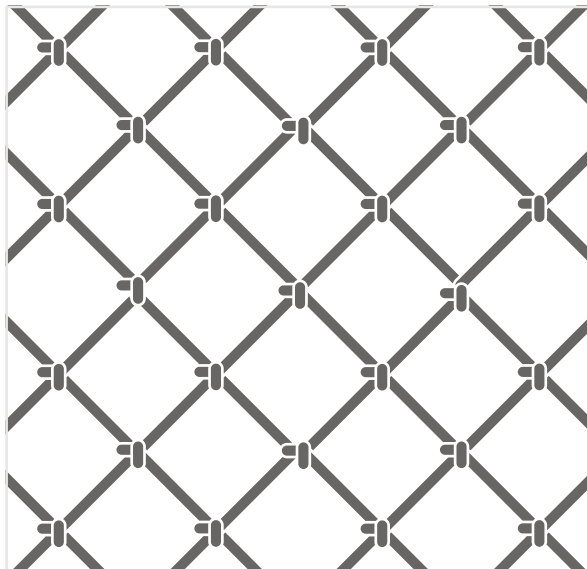
 **ACTIVITY 3: COMPARISON BETWEEN SOCIAL NETWORKS AND FISHING NETS**

It is not always easy to explain exactly what is meant by networks. While it is true that the concept is intuitive – which helps when it comes to explaining them – the very familiarity of the idea makes it more difficult to go more deeply into the question. To simplify the matter it can be helpful to compare networks with fishing nets.

→ **INTRODUCE THE ACTIVITY AS FOLLOWS:**


We have seen that protection networks are made up of individuals and organisations that maintain regular contact between themselves to share information, take decisions and act on protection matters that are of interest to their members. Networks do not always announce themselves as such. When we speak of networks we are referring to all the interactions between individuals and organisations – interactions that can take place in many different ways and at a variety of levels.

→ **ENCOURAGE THE PARTICIPANTS TO ENGAGE IN DISCUSSION:**



Stick a large illustration of a fishing net on the wall. Ask the participants what is most important: the **threads** or the **knots**?

Listen to the answers and note down them down without saying anything. Then, initiate a comparison between fishing nets and social networks. Ask participants if what they have said about fishing nets applies also to social networks. At this point feel free to point out any aspects that the participants have missed (See Tips for Facilitators).

-  → The answer to the question about what is more important, the threads or the knots: the logical answer is: both. Without knots, threads are just threads and there is no net. On the other hand it is impossible to tie a knot if you don't have thread. It could also be said that nets vary according to how far apart the knots are or, put differently, how large the mesh is. If the knots are too far apart the net is no good for fishing because all the fish can escape. In the social sphere, to pursue the comparison, it could be said that if there are only a few people or organisations in a network (few threads) and they don't maintain much contact (few knots) then the social network will not be very strong.
- Elements that will help draw conclusions from the discussion: just as a strong net means you can fish more successfully, a strong, well structured, network will be better able to work together. If you have to catch big fish then you will need a strong net. A weak net will break easily. The same is true of communities: if the opponent is big and strong a small, weak, community will not be able to confront it and will break before it achieves its objectives. But just as different communities can come together to make themselves strong so you can making a fishing net using different threads, or increase the number of knots to make it stronger and catch bigger fish.


 **ACTIVITY 4: STORY(IES) ABOUT COMMUNITIES**

This activity is intended to help participants understand **1)** the weaknesses and strengths of protection networks and **2)** how protection networks contribute to making communities stronger. The guide contains a fictional account of a situation commonly faced by communities (see [Annex of this Chapter](#) below). However, facilitators are encouraged to be creative and to make their own stories up, adapting them to local experiences and contexts. But they are also advised to be very careful to avoid any possibility that participants might feel allusions have been made that could interfere with the development of the workshop.

If you decide to use only one story you should distribute copies and ask one of the participants to read it aloud. If you use two stories divide the participants into two groups. Each group should meet and one person should read one of the stories out loud after which the groups discuss a series of questions posed by the facilitator. After the group work is over, each group should read its story out loud to the plenary and feedback on its discussion, giving the members of the other group the opportunity to express their views. The session ends when both plenary discussions are complete.

Use the following questions to guide these reflections (See Tips for Facilitators):

- Which aspects of a protection network is this story relevant to?
- How might a protection network have been useful to the community in this story?

- 
- Which aspects of a protection network is this story relevant to? Among others the following could be mentioned: the community had no access to information about the plans to build the highway; it had no contacts in the local town to inform them of their opposition; they believed it would be enough just to send a written communication; when they met together once the excavators had arrived they did not work together; the few who did act were detained; the community made no preparations for the return of the excavators; they had no early warning system; they had no contacts they could inform that the excavators had returned, etc.

- How might a protection network have been useful to the community in this story? Find out more about the construction project; analyse the situation; define protection measures; decide on representatives to deal with the problem; coordinate their actions; establish an early warning system; establish prior contact with individuals or communities who might be allies (for example the priest or the community 15 km away); etc.

CONCLUSION

- > Ask the participants to restate the key elements of the session and clarify questions or concerns.
- > Show participants how a comprehensive security strategy builds on insights drawn from the previous sessions and stages of the security management process.
- > Ask participants whether they think protection networks are useful in helping them deal with the risks they face.



ADDITIONAL RESOURCES

- > Van Brabant. Op. Cit. Chapter 3.2. (pp. 22-38).
- > FLD. Op. Cit. Chapter 6.

STORY: VALLEY COMMUNITY VS. HIGHWAY

This is the story of a small community of some 200 families who lived in a mountainous area at the entry to a valley a few kilometres away from the settlement. Historically, this area had been crossed by the routes that linked the mountainous regions to the valley; indeed, there is still an old dirt track there.

One day the mayor of the community was notified that the regional government was planning to construct a highway that would pass through the middle of the community. This would require the compulsory purchase of lands in the centre of the community, equivalent to half its territory. The inhabitants of the community were seriously worried by the news. They would lose their lands and the money received in compensation would not be enough to enable them to start their lives again elsewhere. Furthermore, they were unwilling to leave a place that had been in the hands of their families for generations. Those living higher up in the mountains realised that the highway would affect the community in many ways and that their lives would never be the same again. The community decided, therefore, to oppose the construction of the road. There was also an alternative route available that would take the highway around the mountains and along an uninhabited valley. But this would be more expensive and would take longer to construct, reducing profits for the construction firm.

The mayor, who had been in post for many years, began to represent the interests of the community and organised a meeting with some of the inhabitants to discuss what to do. Everyone was very angry and they decided to prepare a note of protest and send it to the regional government. After six months no progress had been made. By this time some families had received an official letter informing them that they had to leave their properties in exchange for an unspecified compensation payment.

One day, the inhabitants saw that two large mechanical excavators and five lorries had arrived, protected by a group of security guards from a private security firm. This was how they realised that work was about to begin and that their letter of protest had been ignored. The entire community met together urgently and 10 or so of the angriest amongst them proposed confronting the workers and forcing them to leave. The rest of the community vacillated because they were afraid of the security guards and because it was first time they had ever faced a situation like this. The angry group decided they could not waste any time and they decided to stand in the way of the machines. There was a fight with the security guards during which three of the inhabitants and two of the guards were injured. In the end, the machinery and the guards left the community, much to the celebration of its inhabitants. After two further weeks during which nothing else happened the community began to recover its air of calm.

Early one morning, the machines returned but this time they were escorted by 40 security personnel armed with pistols and accompanied by dogs. The excavators got down to work immediately. The community had not considered how it might react to this situation. The mayor and some of the individuals who had led the action the last time were not there because they were members of a small cooperative and were in town on business. As the machines began to work the security guards walked around the community detaining several of the people who had attacked them on the previous occasion (they were accompanied by one of the guards who had been attacked, who pointed these people out). When a group of women went up to the guards and asked where they were taking the men, they answered simply that they were going to teach them a lesson. Nobody knew what to do until someone thought of telling the priest whom they had seen yesterday on his way to another community some 15 km away. But no one was sure whether the priest had already left for another community further to the north. At dusk the excavators left, along with the guards. That same evening the members of the community formed a small commission which set off for the nearest town, intending to speak to the police and find out where their neighbours had been taken. The mayor returned at nightfall and once he had been told about what had happened, he called a meeting for first thing the next morning.

9. ORGANISATIONAL SECURITY

- > **CHAPTER 1.8** OF THE NEW PROTECTION MANUAL
IMPROVING SECURITY AT WORK AND AT HOME
- > **CHAPTER 2.1** OF THE NEW PROTECTION MANUAL
ASSESSING ORGANISATIONAL SECURITY PERFORMANCE: THE SECURITY WHEEL
- > **CHAPTER 2.2** OF THE NEW PROTECTION MANUAL
MAKING SURE SECURITY RULES AND PROCEDURES ARE FOLLOWED
- > **CHAPTER 3.1** OF THE NEW PROTECTION MANUAL
REDUCING THE RISKS ASSOCIATED WITH OFFICE SEARCHES AND/OR A BREAK INS



LEARNING OBJECTIVES

- > Assess the overall security management of an organisation (or community).
- > Improve compliance with security rules within the organisation.



KEY MESSAGES

- > To assess your security, you need a two-fold approach: self-assessment and assessment of how others perceive you.
- > Security is everybody's business.
- > Developing an organisational security culture is fundamental for the respect of security rules and protocols.
- > Rules are observed only if they are understood and if everyone feels ownership of them.
- > Successful security management requires time and resources.

THE SESSION

CHALLENGES THAT MAY ARISE DURING THE SESSION :

- The emergence of complexities and sensitivities associated with the dynamics of organisations.
- Complex information and concepts.
- Taking into account the specific protection needs that women HRDs and any other relevant social category of HRDs (for example, indigenous populations, LGBTI defenders, disabled defenders, etc.) may have in terms of strategies, security norms, etc., both for routine protocols and emergency procedures.
- This session only applies to urban organisations. If you are working with grassroots or community-based organisations in rural areas, we recommend you focus exclusively on the **Observation of rules and security protocols** section below while ignoring the case analysis. The discussion of the statement works well for such a session, but you should take into account the characteristics and needs of these organisations (See [Chapter 5.8](#) of this guide and [Guía Cuidándonos](#)).

 THE SESSION STEP BY STEP :

Time	Acc. time	Activity	Tool / method / materials
15'		Introduction: <ul style="list-style-type: none"> The learning journey 	Have the points ready on a flipchart (or PowerPoint slide) Enlarged print-out of the capacity-building journey on protection (Chapter 3)
65'	80'	Security wheel <ul style="list-style-type: none"> Explanation Activity 1: Filling in the Security Wheel 	Enlarged drawing of Security Wheel (or slide)
60'	140'	Observation of rules and security protocols <ul style="list-style-type: none"> Discussion of the statement Explanation of security rules Activity 2: Case analysis 	Print-outs of cases (below). Flipcharts Markers
75	215'	Improve security at home and at the office <ul style="list-style-type: none"> Explanation Activity 3: Analyse the security of participants' offices or homes Activity 4: Role play 	Table "Checklist: Office Security Review" (NPM, Chapter 3.1). Example of a search warrant (can be fictional but should be realistic) Locally applicable laws governing legal searches (if possible) Flipchart Markers
15	230'	Conclusion	

TIME KEEPING: CALCULATE 270' (4 HOURS AND 30 MINUTES), INCLUDING TWO 20' BREAKS

LEARNING ACTIVITIES

INTRODUCTION: THE LEARNING JOURNEY

Show participants a map of the journey they have been on so far. For this you should bring a print-out of the illustration of the capacity-building journey on protection ([Chapter 3 of this Guide](#)) and put it up on a wall, or project it. The tools covered in the training sessions are represented by symbols that appear along the path of the journey. Make sure that everyone feels confident in using the tools, and allow some time for clarifications if required.

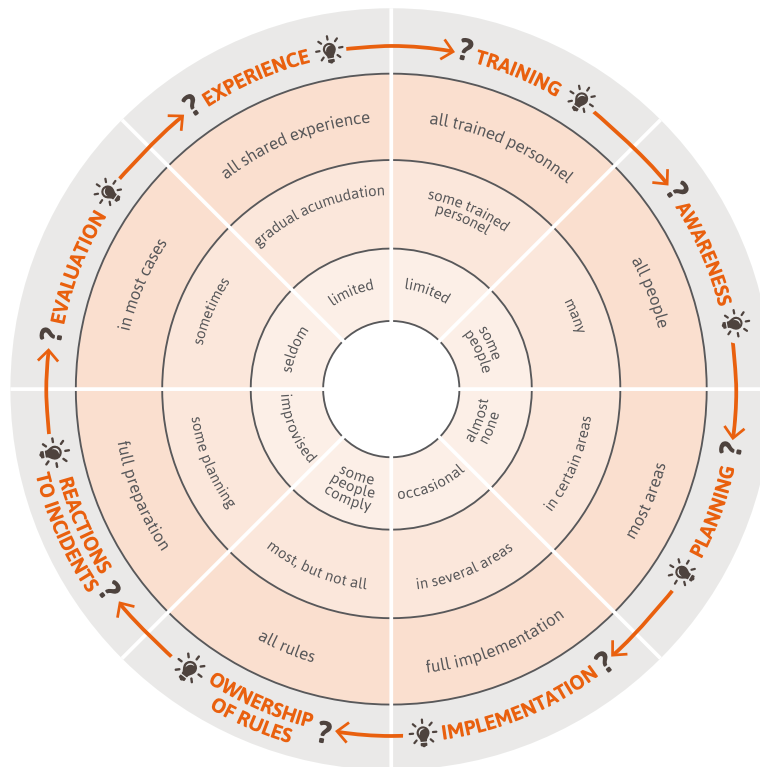
Next, shift the discussion onto the organisational aspects of security management, i.e. how organisations work, how decisions are taken and how change occurs. Remind participants that successful security management is about changing attitudes and behaviour. While the training may have already achieved a certain degree of attitudinal change, it is their behaviour as individuals and how the organisation operates on a daily basis, that need to be consciously worked on.

Remind participants that the existence of a security plan does not automatically ensure security or protection. Invite participants to express their views on this, as it will help you steer the discussion in the right direction. Facilitators should point out that security requires ownership of the whole process, starting with an assessment of the current levels of organisational security, identifying where improvements could be made, implementing security plans, and eventually conducting a regular monitoring and evaluation process.

THE SECURITY WHEEL

EXPLANATION

Introduce the Security Wheel by putting it up on a flipchart or projecting it. Explain the eight components, or dimensions, of the wheel (**NPM 2.1, pp. 132-133**). Once participants are familiar with the tool, explain the “step by step analysis of the Security Wheel”, i.e. the questions that need to be asked in order to determine the degree to which security components are currently met and any improvements that might be required or advisable (**NPM 2.1, pp. 134-138**). The logic behind the Security Wheel is that it should be as round as possible so that, if an actual wheel, it could roll easily. Translated into terms of security management, this means that it is not helpful to score well in one area but badly in others. All areas should be even.



ACTIVITY 1: FILLING IN THE SECURITY WHEEL

Ask participants to apply the analysis to their own organisations. Divide participants into groups if necessary (in this case, several security wheels will be produced for the same organisation. After all groups are finished, they should compare the different security wheels. Conclude the activity by engaging participants in a plenary discussion on the results of the exercise.

- When working with a homogenous group (assuming you have not divided the participants into smaller groups for this exercise), discuss the meaning of each dimension (spoke) of the wheel (**NPM 2.1**) in plenary; otherwise provide instructions before group work begins. The area of each spoke should be shaded, successively, according to the current status of organisational practice. There is likely to be some disagreement and discussion around what percentage of each section should be shaded. Help the group to achieve consensus by emphasizing that the wheel is a tool designed to illustrate the current state of the organisation, as a starting point for organisational change. Finally, recommend that participants review the wheel in six-months' time in order to assess their progress.
- If participants have been divided into groups, ask those who work at the same organisation to work together. Then put all the results on the wall and discuss the following general points: the group(s) is (are) likely to obtain a wheel whose spokes have different areas shaded. This helps to identify the types of action that need prioritising to improve the organisation's protection and security.

DISCUSS THE FOLLOWING STATEMENT

→ **“The security of our organisation is only as strong as our weakest link.”**

Read this statement to participants and present it on a flipchart too and encourage a discussion in plenary. The statement is based on the logic that if potential aggressors want to obtain more information on, or even harm, HRDs, they will probably try to find the weakest link that they will then act upon, for example, getting close to someone who likes to get drunk on Saturday nights. Similarly, if someone is interested in scaring the staff of an organisation, they will probably target someone who is generally careless about her/his security. Similarly, a careful person might be attacked because a careless person has left the door open. The point is that one careless person can put the whole organisation at risk.

EXPLANATION OF SECURITY RULES

Prepare and deliver a brief presentation on how security rules should be defined and supervised ([NPM 2.2](#)). This will provide the basis for the case analysis.

ACTIVITY 2: CASE ANALYSIS: HOW GOOD ARE THE RULES?

You can carry out this activity, which asks to participants to analyse three security rules of a fictional organisation, either in plenary or by dividing participants into three groups. Distribute one security rule (see below) to each participant or the group and ask them to analyse them according to the following criteria: practicality, sustainability, inclusivity and effectiveness. Note that the phrasing of the rules is intentionally convoluted, as the aim is to provoke discussion among participants about whether they are adequate and to identify improvements.

Allow participants to work for 10 minutes and then ask the plenary – or the groups if participants have been divided up – to report their analysis of the rules and then encourage a discussion in plenary (see Tips for Facilitators). If you wish, you may use examples taken from the organisation’s own security rules (but be careful, as this may create tensions).

→ **RULE 1:**

Before initiating verification of a presumed human rights violation, you should check the relevant parts of the security manual to make sure everything is being done according to the rules. If you are not familiar with the security manual because you are new to the job you should ask for help from your workmates or your direct supervisor.

→ **Positive aspects:**

- The rule refers to a security manual, which means, at least, that the organisation has one. As a rule, everybody should be aware of its existence.
- It implies that someone is responsible for security issues, i.e. the direct supervisor, to whom new staff can ask security-related questions. However, having to ask could be a barrier. If the organisation has an open consultative culture (meaning that people - and above all management - show a certain willingness to help), this should not be a problem.

→ **Negative aspects:**

- New staff should not have to take on such tasks. If they are required to, they should be properly trained and supervised.
- The security manual should be easily accessible, which does not seem to be the case here.
- Staff should know which parts of the security manual to consult. If it takes time to find the right

sections, people are likely to become discouraged and fail to follow the rule.

- The rule implies additional work, and this might lead people to ignore it.
- Two more general questions can be asked: does the rule make sense within the working context of the organisation? Have all staff members participated in drawing it up (thus encouraging ownership)?
- Finally, the human aspect of the work should not be forgotten. The rule could lead to a bureaucratized approach to people who come to the organisation asking for help.

→ **RULE 2:**

The country field office is responsible to the international headquarters in Geneva for the security of its local staff. Given the situation in the country, field trips to remote and high-risk areas represent one of the most vulnerable moments in terms of security. Therefore, the organisation's international security standards, which must be applied in every country, require local staff to:

- Prepare each field trip to high-risk areas properly, at least seven days in advance. Before travelling to the field staff should meet in order to review the relevant protocols covering the preparation of field trips (check the security manual). The field trip will not be carried out, under any circumstances, if all requirements are not met.



→ **Positive aspects:**

- The reference to international standards clearly implies the importance of the rule.

→ **Negative aspects:**

- The seven-day rule might be an obstacle. Also, in regions where the security situation is unstable and fragile, the rule might be insufficient, as the security analysis carried out on one day might not be valid the next.
- It might not be realistic to think that all team members will always be able to meet before trips. This might have an impact either on the enforcement of the rule (members circumventing it on occasions) or on the work of the organisation itself (meaning there is a risk that trips will be cancelled because of the rule).
- The way to involve new staff in the design of security rules and to encourage ownership is to include them in analysing and periodically assessing the rules. In organisations with a top-down decision-making process, staff should at least be able to give feedback on the real viability, efficiency and adequacy of the rules. In more inclusive organisations, staff will be able to participate in assessing and deciding on security rules. It might not be easy to strike a balance between participation and the efficient use of resources. The rules should be reviewed periodically, but care should be taken to avoid making changes too frequently, as this can lead to staff ignoring the rules. Notwithstanding these aspects, emergency situations can sometimes oblige organisations to redesign a rule quickly.

→ **RULE 3**

During field missions away from the city, security considerations should cover free time, both in the evenings and at weekends. All the organisation's staff must follow the following rules during their free time:

- You must not be on the street after 9 p.m., by which time you should be at your usual home or, if you are staying at a different house or a hotel, report to the person in charge. If you have a mobile phone, it must be operational at all times.
- Regional staff will define which places must not be visited after 9 p.m. for security reasons.
- Alcohol and other drugs must not be consumed.

- Personal actions that might compromise other people's security or the image of the organisation are not allowed.



→ **Positive aspects:**

- Overall, it is good that the rule deals with issues related to free time and security and takes into account times when staff are not officially working.
- Dangerous zones are defined, which makes it easier to avoid them.
- The rule also deals with issues related to alcohol and drugs, which may not be easy to address in some cultural contexts.

→ **Negative aspects:**

- Security issues related to drugs and alcohol should be better explained. Organisations should avoid referring to moral standards, but instead address the issue in a security-oriented way. Emphasis should be put on vulnerability and responsibility. It should be clear that if something happens, staff members need to be prepared to react. In some cases it might be easier to ensure compliance by setting a low level of alcohol consumption, while prohibiting the use of any illegal substances.
- In general, the rule does not explain the reasoning behind it. Such a rule-bound focus might make it harder to enforce. It could be good to provide a fuller explanation of why it should be respected. The principal problem is that the surest way to get someone to do something is to ban it.
- The criteria and requirements that have to be met before authorisation to travel is given are not clear, and the member of staff responsible for authorisation is not specified. The rule should also refer clearly to the relevant section(s) of the manual.
- Finally, it could be argued that the last point, on personal actions that might compromise the security of others or the organisation's image is rather vague. The type of actions – or the situations in which they might take place - are far from obvious and could require further clarification.

IMPROVE SECURITY AT HOME AND AT THE OFFICE



EXPLANATION

Base your explanation on the [NPM \(Chapter 1.8\)](#). The main security objective should be to prevent unauthorised access to the workplaces or homes of HRDs. Assessing office security is similar to conducting a risk analysis. The process uses the same concepts of threat, vulnerability and capacity. Highlight the fact that the vulnerabilities of an office must be assessed in the light of the threats faced and that, echoing the discussion about the observation of security rules, the security of an office is only as great as its weakest link.



ACTIVITY 3: ANALYSE THE SECURITY OF PARTICIPANTS' OFFICE OR HOME

Ask participants to analyse the security of their offices using the table provided in the [NPM \(Checklist: Office Security Review, p. 94\)](#). Divide participants into groups if necessary. Encourage participants to discuss their analyses to close the exercise. If you are working with mixed groups, ask participants from the same organisation to work together.


ACTIVITY 4: ROLE-PLAY: LEGAL SEARCH

Four people are assigned the following roles (these roles must be adapted to each context and to the current laws of each country):

- Judge, with a search warrant (adapted to the context).
- 2 policemen searching the place.
- 1 individual, with no identification papers, who hides a plastic bag full of cocaine and “finds it”.

Other participants are members of the organisation; their role is to decide on the reaction to the search.

When the role-play is over it should be evaluated. Base your feedback to participants on the concepts and elements found in **NPM Chapter 3.1**.

-  → Inquire about the framework covering legal searches in the country you are working in. Print them out and hand them out to participants at the end of the role-play.
- During the analysis of the role-play, ask participants how they felt during it. Insist on the fact that they will feel safer if they are familiar with the legal framework and are aware of their legal rights.
- Divide the evaluation process into three phases (this needs to be adapted depending on the exact terms of the law):
 - Actions to be taken before the search: inquire about your legal rights; review security protocols - especially concerning the secure management of information (**NPM 3.1**); train members how to react when faced with a search warrant;
 - Actions to be taken during the search: call a lawyer (or someone you are sure will answer and who will be able to call a lawyer and other useful people); review the search warrant to make sure that it is legal; do not let the police officers enter the building unaccompanied (this will depend on your legal rights to refuse to leave the premises when ordered to do so by the police); be aware of anything illegal that the law enforcement officers may do;
 - Actions to be taken after the search: Make sure that everybody is fine; assess the search; design a plan to react to it and to limit its negative impact.

CONCLUSION

- > Ask participants to recall the key learning points of the session. Insist on the key messages by referring to issues or examples that have been mentioned during the day.



ADDITIONAL RESOURCES

- > Van Brabant. Op. Cit. Chapters 18-21.
- > Comité Cerezo México. Op. Cit. Chapter 7.
- > Colectivo ANSUR. Op. Cit.

10. INFORMATION MANAGEMENT AND DIGITAL SECURITY



- > **CHAPTER 1.11** OF THE NEW PROTECTION MANUAL
SECURITY IN COMMUNICATION AND INFORMATION TECHNOLOGY
- > **CHAPTER 3.3** OF THE NEW PROTECTION MANUAL
SECURE MANAGEMENT OF INFORMATION

This chapter will prove useful for facilitators if risks to the security of digital information kept by defenders have been identified either during the pre-training assessment or during the training itself. In any case, this session is principally intended to raise awareness about a specific aspect of information technology (IT) security (see objectives below). Depending on the digital risk profile of the organisation, their training needs and the setup of the capacity building process, this can either be done as part of one training session dealing jointly with the interlinked dimensions of physical and digital security or as an introduction to a separate, more detailed, digital security training module. **However, facilitators need to ensure that the risk analysis carried out by the HRDs encompasses both dimensions and that plans to build capacity reflect the links between them. Otherwise the sessions will not be relevant or responsive to the risks faced by HRDs.**



LEARNING OBJECTIVES

- > Raise participants' awareness about the importance of IT security, with a focus on the risks associated with the loss and theft of data.
- > Indicate resources that will help HRDs improve the security of their information.



KEY MESSAGES

- > Risks to the security of information held by HRDs may come not only from technical failures and targeted attacks intended to obtain access to, or to destroy, the information they hold, but also from careless communication practices.
- > Protecting access to information and regularly backing up information can reduce the risk of data being lost or stolen.

THE SESSION

⚠ CHALLENGES THAT MAY ARISE DURING THE SESSION :

- Facilitators ought to have a minimum understanding of digital security tools (at user level) and in particular those that can assist in minimising the risk of losing data and unauthorised access to it.
- Defenders may be using computers and other devices regularly but still have only a very basic understanding of how they function. Keep all discussions as simple as possible and avoid technical terms that may be confusing or easily misunderstood. If this is not possible, explain the terms in simple, non-technical language and consider using illustrations. Ensure these explanations are visible throughout your sessions for further reference.

 THE SESSION STEP BY STEP :

Time	Acc. time	Activity	Tool / method / materials
05'	5'	Introduction: • Objectives and structure of the session	Have the points ready on a flipchart (or PowerPoint slide)
10'	15'	Risks to communicating securely	Flipcharts
45'	60'	Activity: Data backup and protection against unauthorised access	Flipcharts Sticky Post-its
		Guiding participants through the use of digital security tools (optional activity)	Laptop Flash drive (USB key) with latest installation version of "Security in a Box" tools

TIME KEEPING: CALCULATE 60' (1 HOUR) + * AND A 20' BREAK

LEARNING ACTIVITIES

This session looks principally at the risk of data loss (failure to make back-ups and misappropriation of information by perpetrators) and helps participants to identify current vulnerabilities related to the way they manage information stored on various devices: This information is called "Data at Rest". It focuses on simple yet fundamental procedures, as well as possible digital and non-digital tools and measures to increase HRD capacities to manage risk.

Facilitators can find learning materials in the [NPM](#) that they can use to help them prepare this session (see [Chapters 1.11 and 3.3](#)). As threats and digital information protection technologies evolve at a very fast pace, facilitators are encouraged to familiarise themselves with other materials on the topic. At the end of this section, there is a non-exhaustive list of additional resources for further reading.

RISKS TO SECURE COMMUNICATION

To introduce the topic, the facilitator might wish to begin by asking participants what means they use to communicate with their colleagues and to other people outside their organisation/community. Write down a list of the means of communication mentioned by participants on a flipchart. In case it is not mentioned, remind them that talking face-to-face is perhaps the most common way to communicate (sometimes inadvertently) sensitive information about their work. Thus, information security and protection is not just a question of sophisticated communication technologies.

Next, brainstorm with participants on the various ways in which information or communications can be legally accessed but also manipulated: e.g. when talking face to face or via mobile phone or as a consequence of aspects of the physical security of the office. Use the information in [NPM \(Chapter 1.11\)](#) for inspiration.

If participants consider they are at risk of being listened to during face to face conversations or when using mobile phones, recommend that they develop protocols for handling sensitive information during communications of this kind as part of their security plan. You can point to the above chapter for guidance.

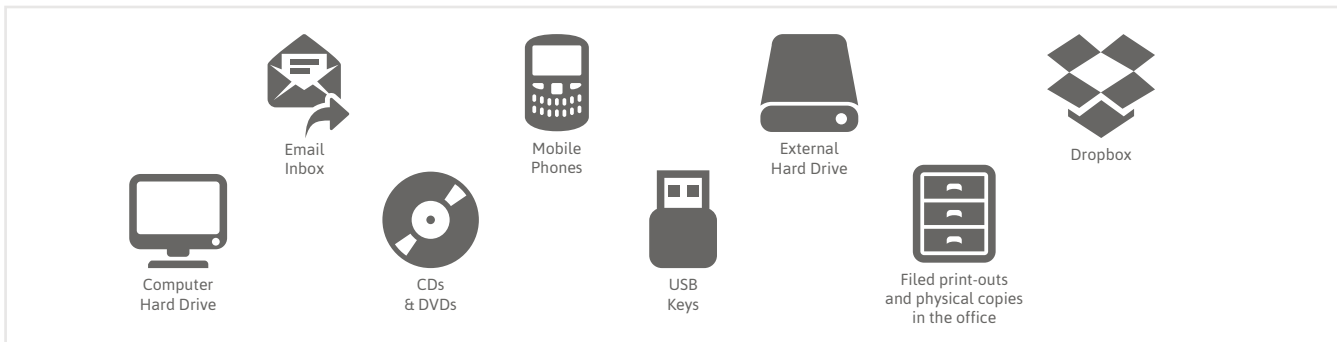
Move towards a different aspect of information security by asking participants how important the information is that they keep in digital formats: emails, reports, partner and beneficiary contact details, etc. If participants assign significant importance to this information, ask them to identify (or indicate for them, if they are struggling) ways in which they risk losing this information (e.g. through a technical fault, loss or theft of equipment, or unauthorised access like hacking).

 **ACTIVITY: DATA BACKUP AND PROTECTION AGAINST UNAUTHORISED ACCESS¹**

Depending on previous sessions with participants and the discussions on risks relating to information security, make a link to the risk of data loss and what it could mean for HRDs and the persons they work with and for. Ask them what ad hoc strategic measures they currently have in place to avoid the loss of their data.

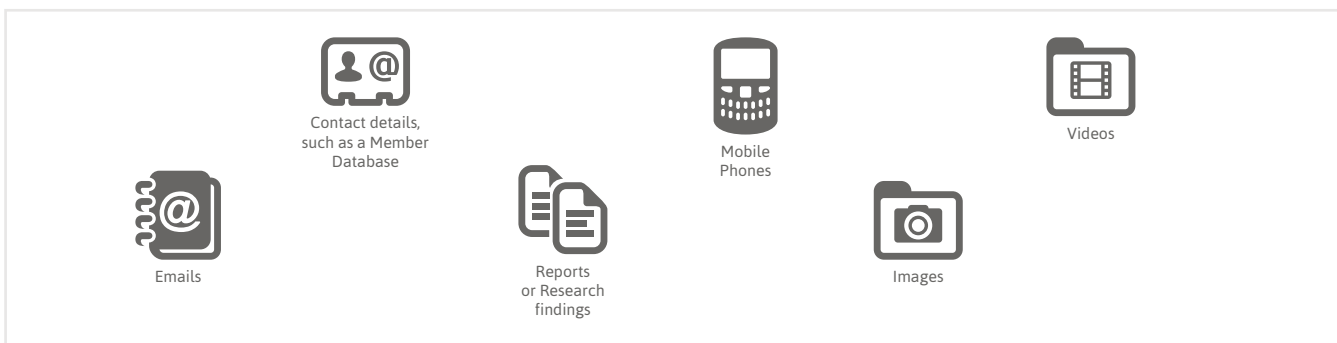
Prepare two flipcharts taped together and draw a matrix (see below) and stick this up in a clearly visible place on the wall. Explain to participants that this is an information mapping exercise that seeks to visualise what kind of information they have and where it is stored. This will form the basis for developing a strategy to reduce the risk of data loss.

Start by asking participants to list the different places where their information is stored. If no suggestions are forthcoming, you can prompt with the following:



Add the locations mentioned by participants to the top row of the matrix. Then ask participants what type of information or data they store in each of these places.

For example:



Write one example on a card/post-it and place it in the relevant part of the matrix: e.g. reports on the hard drive of the computer.

Ask whether there is another copy of this data somewhere else. If there is, you can use a different-coloured post-it and place it wherever they keep the duplicate. You can use this moment to differentiate between master copies and duplicates or back-ups. (In the example below red indicates master copy and yellow indicates duplicate).

¹ This activity has been adapted from Samir Nassar, Daniel Ó Clunaigh, and Ali Ravi from Tactical Technology Collective for the LevelUp project. Facilitators are also encouraged to read **NPM Chapter 3.3** for background information.

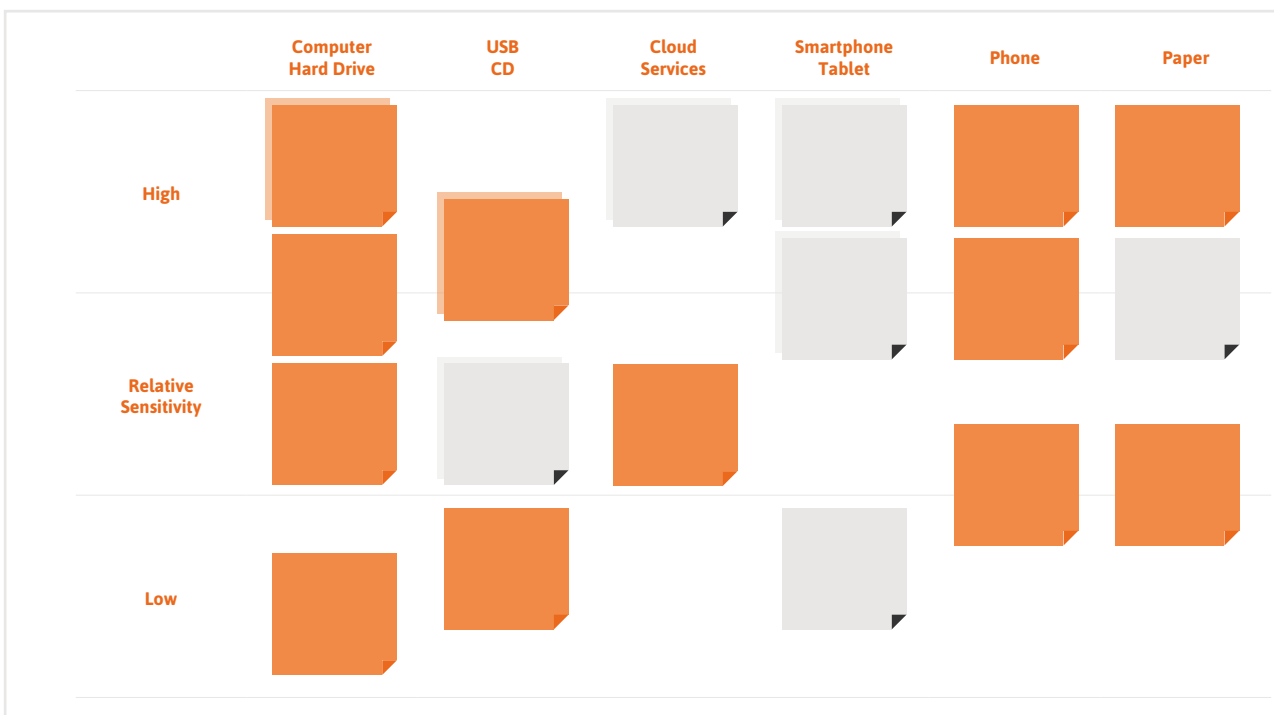
Repeat this process with one more dimension: data sensitivity (meaning data that, if lost or misused, might cause considerable harm either to the HRDs or to the people they are working with, such as victims of gender-based violence). Introduce a second (vertical) axis representing sensitivity. The higher on the chart a card/post-it is placed, the more sensitive the data it represents. Place the two cards/post-its on this axis representing their relative sensitivity. If you have limited time available, you are free to reduce this part of the exercise to one or two examples.



Next, form small groups: one group per organisation when participants come from different organisation or by thematic areas when all come from the same one. This activity can also be conducted as a brainstorming exercise in plenary if all participants are from the same organisation.

Allow 5-10 minutes for this exercise. It is advisable for the facilitator to observe each group and identify interesting characteristics (e.g. where there is a particularly large dependence on one device or copies/back-ups are few, etc.). By the end of the exercise each team should have completed a matrix.

An example might look something like this :



Explain that this matrix gives an idea of where the data is located. Ask whether this is all the data their organisation/community generates. The answer is, of course, that it is not – it is only a small percentage.

Then, take the matrix of one of the teams as an example. If trust levels among all participants allow, read out the information the group keeps on their computer's hard drive, which is usually the fullest.

To illustrate the vulnerability this entails, ask participants what might cause a computer to stop working.

- Virus or malware attack destroys data stored in a computer
- Stolen or confiscated computer
- Infrastructural problems like power failure damages a computer


You can ask participants to raise their hands to indicate which of the above has affected them in the past.

Now ask what would happen to the data if one of the above events were to occur. To emphasise the impact, you can dramatically remove each of the cards/post-its from the column and throw them on the floor. The remaining cards on the matrix represent all the information they would be left with.

Ask participants to think about what could be done to avoid this? The answer is likely to be that they should keep more copies in different locations. Point out that this is what we call backing up!

Now, if time allows, turn to the matter of the sensitivity of data. If possible, take the example of another team's matrix. If the exercise has been carried out in plenary, pick another column on the matrix. Ask participants what the impact would be if their phone/hard drive/USB key were stolen. Take the cards/post-its from the respective column, but keep them in your hand and read them. This illustrates that now someone else is in possession of the information held on the device. Ask what they could do with it and what situation the HRDs would be left in.

Drawing on the previous activity on data backup, ask participants to identify a minimum of three to five things that need to be done to reduce the vulnerabilities they have identified. These steps might be digital: e.g. mention Cobian Backup as well as non-digital solutions such as fundraising to buy back-up devices, develop backup protocols, etc. Depending on the composition of the training group, ask them to do this on organisational (for homogeneous groups) or individual level (heterogeneous groups).

-  → This activity is in essence a risk analysis concerning the data HRDs possess – and might lose – and helps to identify existing vulnerabilities.
- The ideal circumstances for this exercise are a training group with high levels of trust or that can easily be divided into relatively homogenous groups. For groups where trust levels are low or for heterogeneous groups who do not know each other well and may not be comfortable letting others know what information they hold and how it is kept, the exercise needs to be modified to make it more generic while maintaining the learning points.

GUIDING PARTICIPANTS THROUGH THE USE OF DIGITAL SECURITY TOOLS (OPTIONAL ACTIVITY)

If carried out, this part of the session is intended to address the vulnerabilities that have been identified and to strengthen participants' capacities to face the risk of data loss and unauthorised access both to **"Data at Rest"** (data stored on a device: see above) and **"Data in Motion"**.

"Data in Motion" refers to the exchange of information, e.g. via internet, email, mobile phone or social media, which HRDs frequently use for their work and to exchange information with stakeholders. One of the principal risks involves the possibility that opponents might gain unauthorised access to sensitive information, either by hacking into user accounts or by eavesdropping or intercepting information by other technical means. By helping HRDs identify existing vulnerabilities in this area you support them in establishing

procedures to create and maintain strong passwords, use safer (i.e. encrypted) channels of communication and/or ensure information itself is exchanged securely, e.g. by encrypting it.

To address vulnerabilities identified during these exercises, facilitators will want to be familiar with the following:

- Creating strong passwords (for email accounts, computers, files etc.)
- Encrypting information stored on devices and in motion
- Maintaining privacy for internet communication
- -Backing up information

Facilitators are encouraged to introduce participants to these digital security tools using the resources found at <https://securityinbox.org>



To work with the resources in <https://securityinbox.org>, facilitators are advised to:

- Be conversant with the use of the tools yourself by making it a part of your own security strategy: strong password practices, encrypting information stored on devices or sent via the internet or mobile networks, and regular data back up.²
- Carefully read through the corresponding section of the “How to” Booklet on the website <https://securityinbox.org/en/howtobooklet>. This will give you relevant information on which vulnerabilities a specific tool can address, which it illustrates using case studies that can be usefully adapted to the context of your participants.
- Be aware of the different features that the tools provide, and introduce only those that respond to the risks identified by your participants. This is to avoid overloading participants with information they might never apply.
- Make sure to download the latest version of the tools you want to introduce from the “Security in a Box” website ahead of the training session and to store them on your computer or on a portable device for your demonstrations so that participants can copy them. This will guard against possible delays should the internet connection during the training session not allow participants to download the software quickly.
- When selecting the venue for the training session, consider whether there is a regular power supply and back-up options, such as generators, to ensure the training is not interrupted by power cuts.
- Before the session, make a test run of the installation and all components you hope to introduce to be sure they function on your computer. This is essential for you to be able to guide participants through the installation and features via a projector.
- To avoid spreading computer viruses, ask participants whether they have an antivirus programme and to make sure it is up to date. You could also make a version of the free Avast antivirus software available for participants who have no antivirus or whose programme is not up to date.
- If participants use their personal or work computers for the training session (rather than hiring computers that have been serviced and cleaned of malware and possible non-essential applications) it is likely that it will be difficult to install the tools or to complete certain tasks, because of the different settings. As you are not a technician and time available for the session is limited, refrain from trying to fix these problems during the session. Instead, ask participants affected to work together with one of their colleagues to ensure that the session objectives can be met for the entire group.

² Considering the fast developments in this field, maintain an understanding of what is happening in terms of digital security and privacy issues by keeping updated via the Security in a Box website, AccessNow (www.accessnow.org), Ono (<https://onorobot.org>) and others. Where possible, attend digital security training not only to improve your use of tools or learn about others, but also to improve your facilitator skills in this area.

- It is desirable to have at least one computer per two participants to allow them to follow your instructions as well as practice the tools by themselves.
- Use the respective section from the “Hands on Guides” to prepare for the demonstration of the tools (<https://securityinabox.org/en/handsonguides>). Practice this in advance and anticipate questions. Keep your language simple and illustrate the relevance of the tools to the risks identified by defenders.³
- When introducing the tools, ask participants to close all other applications and follow you for the first demonstration via the projector screen. Then ask them to do the same themselves on their computer following your guidance on screen. Finally, ask them to repeat the same procedure without guidance. The more opportunity they have to practice the tools themselves, the deeper the learning experience.
- The use of digital security tools may be a challenge to quite a number of HRDs. Point out the benefits of using the tools in response to their identified risks. Underline that the more they use the applications the more comfortable they will feel with them.
- Point participants to the resources in <https://securityinabox.org> for further tools and guidance. All these tools are free and the toolkit is regularly updated.
- The Digital Security First-Aid-Kit for Human Rights Defenders outlines specific risk scenarios and provides guidance on immediate measures to remedy the situation. It also provides links to additional resources such as Security in a Box and others (<https://www.apc.org/en/irhr/digital-security-first-aid-kit>).

³ Level Up! is an upcoming resource for trainers in digital security that will provide information in how to prepare and deliver digital security training sessions. Refer to <http://level-up.cc> for inspiration and guidance.

CONCLUSION

- > Remind participants that the activity on data backup and theft/loss is aimed at providing them with insights into where their data is stored, which of it is sensitive, and which needs to be protected from unauthorised access, or backed up because it is currently only stored in one place. Encourage participants to recall key learning points and further training needs, which they should include in their action plans.
- > Should you introduce the use of specific digital security tools, let participants recall which identified risks they address and why they consider them worth using. To ensure application of the tools, consider developing assignments or “homework” so participants can practice and become comfortable with their use.



ADDITIONAL RESOURCES

- > Association for Progressive Communication (2013). Digital Security First-Aid Kit for Human Rights Defenders. <https://www.apc.org/en/irhr/digital-security-first-aid-kit>
- > Front Line Defenders (2009). Digital Security and Privacy for Human Rights Defenders. http://www.frontlinedefenders.org/files/en/eseccman.en_.pdf
- > Tactical Tech Collective. Me and My Shadow. <https://myshadow.org/>. Resources and tools limiting which information one leaves behind when using the internet.
- > Level Up! Facilitator's toolkit for digital security trainers. <http://www.level-up.cc>.
- > Tactical Tech Collective and Front Line have developed the reference toolkit <http://securityinabox.org> available in book form, on DVD and online. You are recommended to use of the online version as it has the most up-to-date versions of the software. Securityinabox.org addresses the following areas:
 - [How to protect your computer from malware and hackers](#)
 - [How to protect your information from physical threats](#)
 - [How to create and maintain secure passwords](#)
 - [How to protect the sensitive files on your computer](#)
 - [How to recover from information loss](#)
 - [How to destroy sensitive information](#)
 - [How to keep your Internet communication private](#)
 - [How to remain anonymous and bypass censorship on the Internet](#)
 - [How to protect yourself and your data when using social networking sites](#)
 - [How to use mobile phones as securely as possible](#)
 - [How to use smartphones as securely as possible](#)



Protection International AISBL

11 Rue de la Linière
1060 Brussels – Belgium

+32 2 609 44 05

<http://protectioninternational.org>