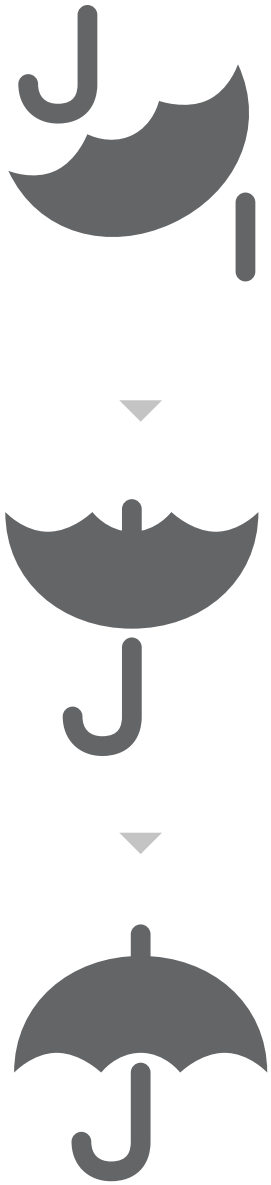
MONITORING PROGRESS

> 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	• Political context (actors & dynamics) • Risk profile • Organizational structure & dynamics • Current security management practices • HRDs reflect on current security management practices and desired change	• 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	• Assessment form • Security wheel • Training session plan
TRAINING	• 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	• 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	• Participant log books • Daily evaluation exercises • End of training evaluation • Facilitator debrief
PLANNING SESSIONS	• Visioning: what change do we want to achieve in our security management? • Formulating action plans • Schedule for follow up meetings/actions with facilitator	• 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	• Action plan
FOLLOW-UP (MULTIPLE)	• Tailored technical support • Monitoring progress against the action plan • Facilitating review of goals/actions if necessary	• 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	• Monitoring template
MONITORING	• Description of current security management practice • Evidence of attitudinal change (anecdoteal, observations, incident descriptions) • Comparison with baseline • Highlighting learning junctures	• What has changed? • Intended or unintended? • How did change come about? – which /actors contributed, limited? • Individual and institutional change • Lessons learnt • Best/worst practices	• 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 3 months
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