

PART II

ORGANISATIONAL SECURITY

In second part of this Manual we are covering security at organisational level, that is to say ways of improving security within defenders' organisations.

Security/protection does not simply mean having a security plan.

It requires ownership of the whole process, starting with improving the original organisational level of security, to implementing it, and later to managing the improvement process itself.

Acquiring ownership of the whole process is part of the security itself.

The organisational security process is pragmatic and inclusive.

It needs to be realistic and appropriate to the profile of the organisation.

Although it will require resources, changing behaviour is free and constitutes a crucial factor in improving security.

CONTENTS OF SECOND PART:

- 2.1** Assessing organisational security performance: the "security wheel"
- 2.2** Making sure security rules and procedures are followed
- 2.3** Managing organisational shift towards an improved security policy.

Assessing organisational security performance: the security wheel

Purpose:

Assessing your way of managing security.

Evaluating the extent to which security is integrated into human rights defenders' work.

In order to achieve this, we suggest a two-fold approach:

- ▣ Self assessment by the organisation of its security performance: the organisation looks at its own security performance by gathering objective information. The self assessment process can be collective and/or individual. It is interesting to actually see how the members of a same organisation can reach different conclusions about the security performance of the whole organisation.
- ▣ How 'others' perceive the organisation

ORGANISATIONAL SELF ASSESSMENT OF SECURITY

The security wheel

The organisational self assessment can objectively be conducted by implementing the security wheel and its eight spokes.

A wheel must be round to turn; in other words, all the spokes need to be of the same length.

The same applies to the security wheel and its 8 spokes (components) representing the security management in an organisation or group of defenders.

This assessment can be done in groups:

- ◆ sketch out the wheel
- ◆ fill in each spoke according to how developed you think it is
- ◆ list reasons (brainstorming) why specific spokes are less developed; as all spokes must be at least as long as the most developed spoke, suggest

ways of achieving that result: set objectives and relevant processes, anticipate possible problems and suggests solutions.

- ◆ Once you have completed this exercise, keep your security wheel and repeat the exercise a few months later. You will be able to compare both wheels and determine point by point whether things have improved.

The 8 spokes (components) of the security wheel

□ **Acquired security experience and cohesion:** practical and shared knowledge of security and protection, gathered through work. The starting and the ending points of the assessment.

□ **Security training.** Security training through courses or through individuals' own initiative during daily work.

□ **Security awareness and attitude:** Relates to whether individuals and the whole organisation really view protection and security as necessities and are prepared to work towards ensuring it.

□ **Security planning:** planning security and protection into your work.

□ **Assignment of responsibilities:** who is responsible for what aspect of security and protection? And what happens in cases of emergencies?

□ **Degree of ownership of security rules / compliance:** to what extent do people respect security rules and procedures?

□ **Analysing and reacting to security incidents:** to what extent are security incidents being analysed? Is the organisation's response adequate?

□ **Evaluating security and protection management:** to what extent does the organisation evaluate its security and protection management and to what extent is it updated?

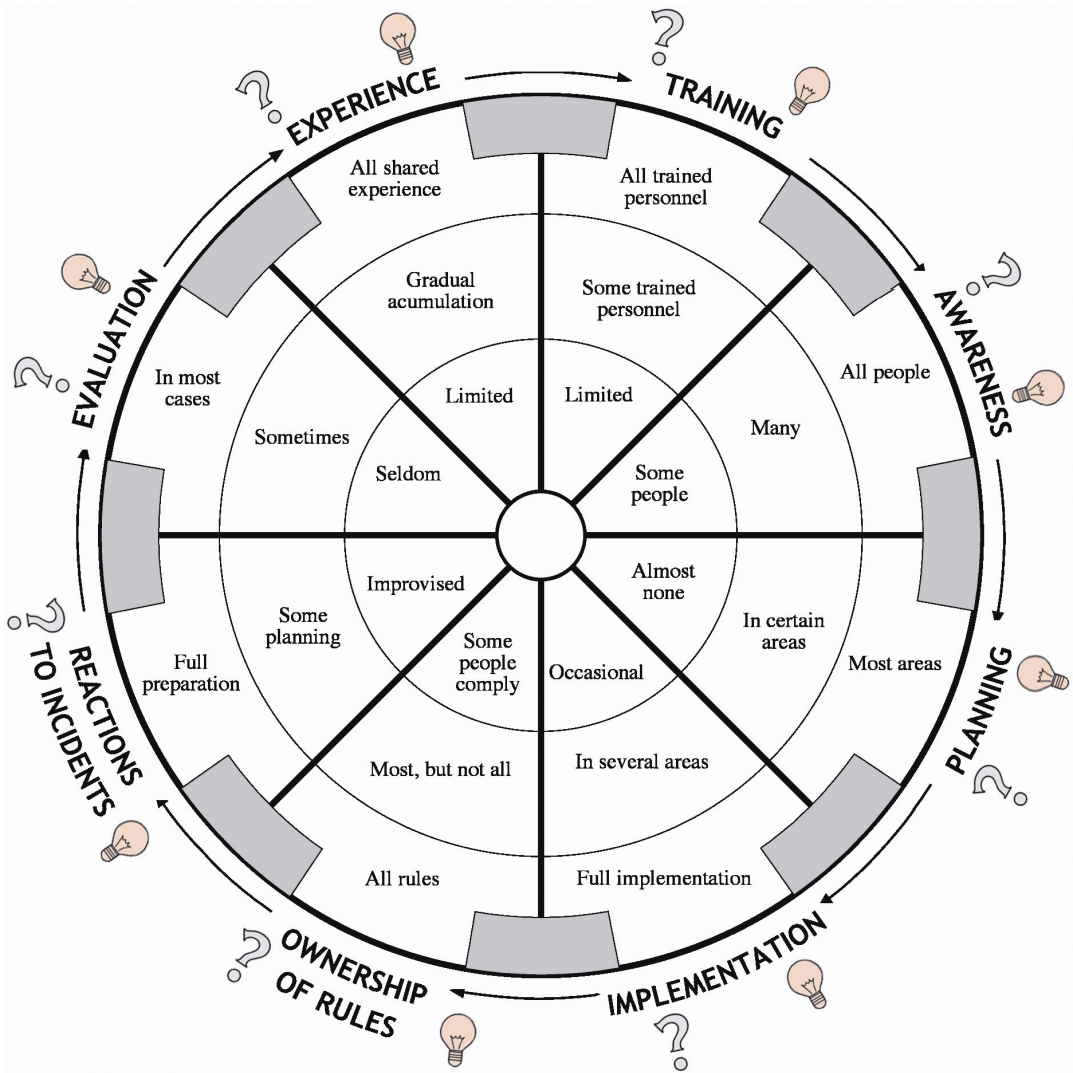


Here is a sample security wheel:

The security wheel is never perfect: Some components are more developed than others. It is therefore more useful to determine the degree of development of each component. In this way, you can identify which types of action need prioritising in order to improve your protection and security. The dotted lines going from the centre to the outside edge illustrate how developed this component of the wheel is.

? Possible problems related to this part of the wheel...

...and possible solutions to the problems.



Photocopy the wheel onto paper or acetate and add colour to the gaps between the spokes to illustrate visually the actual shape of the wheel for your group or organization. You will then easily be able to see which components are more - and less - developed.

Step by step analysis of the “security wheel”

A proper assessment of the security policy of an organisation requires time to examine the actual meaning of every single component of the security wheel.

1 • Security experience and cohesion acquired through work experience and sharing:

Accumulated practical knowledge and cohesion of security and protection. The start and end points of the assessment.

Bear in mind that the experience of just a few members does not equate to the experience of security at the organisational level but rather to the total of the experience of all its members: sharing experiences will therefore contribute to security cohesion.

The total knowledge will be reflected in the spokes; once you have developed all the components to your satisfaction, the total knowledge will have grown further as a result. Security knowledge will then probably be better developed and all the other spokes will need to follow suit. It is a never-ending activity for the simple reason that organisation members come and go, the political context changes and so does security. However, the good news is that as it is the result of all the other 7 spokes, for this specific spoke you do not need to do anything (unlike for the other 7 ones).

2 • Security training.

Indicate the security training you have had either through a course, or through your own initiative during your daily work.

Questions needing further development :

Are security training procedures available to everyone ? Do we upgrade them? Are new staff members trained? What difficulties would we encounter if we were to train everyone? What are the possible solutions?

3 • Raising security awareness and proper attitudes.

Questions used to determine the current level of awareness:

Is everybody truly aware of security and protection? How could we achieve it?

Awareness does not mean compliance (for example, smokers know how dangerous smoking can be and yet they keep smoking)

Questions to raise awareness:

What factors trigger revision of the security?

What are the stories that are told and what is the informal knowledge of security in the organisation?

What problems would we encounter in raising awareness? What are the possible solutions?

4 • Security planning:

Questions to determine the current level of security planning:

- Do we plan security and protection into your work?
- Is the security issue integrated (mainstreamed) into the whole institutional approach? (mission, strategic plans, areas of work, transverse themes) ?
- Is security an agenda item within most major meetings (and not the last item on the list)?
- What is the budget strategy (is it ad hoc for security, or is it included in other strategies?) and financial management?
- Do we carry out an analysis of the work environment -in working groups- (at local, regional and national level)?

Do we:

- analyse the impact of the work and how the organisation is perceived by actors that might be pose a threat?
- carry out a full risk analysis: threats, vulnerabilities and capacities?
- compile all security documents: review their content and see how they are used?
- draft and update security documents? Check whether they are up to date and how this can be achieved? Check whether the impact of the work and risk factors have been taken into account? Check if there are processes in place for daily consultation on security?

Do we have security schemes that are:

- simple and clear? Do they contain the necessary information in clear wording?
- drawn up in cooperation with all the people affected?
- appropriate to every work context?
- improved, developed and updated thanks to the initiative of different people of the working group?
- genuine and adapted to the "real world"?

Do our security schemes cover:

- all necessary items?

- communication, IT and information management?
- personnel management (including recruitment)? stress management?

Is everyone aware that a working group with a good structure, good internal communication flow, good public relations and good cooperation is a basic security requisite?

Questions aimed at further developing security planning:

What problems would we meet if we tried to tackle each of the above items?

What could be the solutions?

5 • Assignment of responsibilities:

Questions to determine the current level of assignment of security responsibilities:

- do we clearly know who is responsible for what aspect of security and protection? And in the event of emergencies?
- Are there organisational responsibilities and duties on workers and collaborators (including their behaviour away from work and family)?
- Does everyone take on their responsibility for security and are there specific responsibilities for different aspects of security? (What difficulties do we encounter?)

Questions to improve assignment of security responsibilities:

What problems would we meet if we wanted assign and share security responsibilities?

What could be the solutions?

Assigning responsibilities contributes to sharing security.

6 • Degree of ownership of security rules / compliance:

Questions to determine the current level of ownership of security rules / compliance:

- To what extent do people respect security rules and procedures?
- To what extent do each individual and the whole group contribute to the security plan drafting, and comply with the protection and security rules?
- Can we tell if security rules are not being followed, and if not, why not?
- Do people abide by security rules out of fear of reproach or because they are convinced that following the security rules will decrease the

consequences of risks? (e.g. a driver may wear their safety belt either out of fear of a fine or because they are convinced that it will decrease the consequences of a possible car crash)

Questions to improve degree of ownership of security rules/compliance:

What problems would we encounter in improving the level of respect of the rules?

What are the possible solutions?

7 • Security incident analysis and reactions.

Questions used to determine the current level of security incident analysis and reactions:

- to what extent are security incidents being analysed and do they generate an adequate feedback from the organisation? What security incidents occurred? How were they handled and what damage was caused?
- do we write reports (and how)?
- do we carry out analyses (how and at what level)?
- what is the feedback (deadlines, feedback procedure, responsibilities)?
- how do we evaluate the feedback?
- is training within the organisation based on the incidents (is it done at all? are there institutional channels for this?)
- in short, what is done with the incidents?
- is there a procedure for collecting, investigating, and analysing the security incidents to create a feedback and a basis for our strategies and our plans? are the conclusions mainstreamed into our work and evaluations (where necessary)?
- are there clear plans and responsibilities covering reactions in case of emergencies?
- to what types of emergency are they applicable?

Questions to improve security incident analysis and reactions:

What are the problems for improving every item listed above?

What are the possible solutions?

8 • Assessing security and protection management:

Questions to determine the current level of assessment of security and protection management:

- to what extent does the organisation evaluate its security and protection management and to what extent is it updated?
- is the assessment an institutionalised activity?
- are we aware that day to day work and reactions in the event of security incidents need to be assessed from a security standpoint so that they will contribute to the knowledge and experience of every single person and of the whole organisation?

Questions aiming to improve the assessment of security and protection management?

What problems would we encounter in improving the assessment of security and protection management.

What are the possible solutions?

HOW 'OTHERS' PERCEIVE THE ORGANISATION

Security and our image

It is important to look at the environment of the organisation to see how its organisational image is perceived and whether it corresponds to the image the organisation seeks to convey. It is also important to find out how others perceive the protection and security of the organisation. This should be done from the following points of view:

- from the point of view of the people with whom we work: counterparts beneficiaries,
- colleagues and similar organisations
- financing institutions and sponsors (some may be more receptive than others)
- authorities with which we are in relation
- other actors who might be potential aggressor
- ...

It is also important to ascertain what level of security cooperation there is with other organisations or networks, with counterparts, with people with whom we work, etc.

Here are two non-exhaustive lists of useful thematic questions:

I ♦ Organisational image and impact of the organisation work. How can we assess it?

- How do we learn about our organisational image?

- How to explain it to others?
- What is the purpose of the organisation?
- What are our activities?
- How do our activities affect armed actors or others?
- What capacities or power do we have to keep our work space open?
- What do we do to keep it open?
- How do we think our potential aggressor perceives us?
- Are we perceived as an organisation that handles well its work-related protection and security issues?
- Is there anybody who singles out our work or our handling of it from a security standpoint? Why? How can we tell?

II ♦ Organisational image and impact of the organisation work. How are we perceived?

Try to answer the following questions about us from the point of view of the 'enquiring' party of your: (repeat the exercise for as many parties as you deem necessary: "they" is you and "we" is the enquiring party)

- Who are they?
- What do they expect?
- What is their work?
- How do they hinder our work? What are the limits to our work?
- What can we do? How can we protect ourselves?
- How can we obtain what we want?

Once you have assessed the perception of others you need to see how you could change your image if it does not suit you. Not all perceptions can be changed, of course. But it helps to be aware of them as they may have an impact on your security and protection.

Summary

To assess your security you need a two-fold approach:

Self-assessment (a look at yourself) and assessment of how others perceive you.

Self-assessment can be achieved through the security wheel with its 8 spokes.

It is a snapshot of your current level of security and protection.

It allows development of each spoke so as to achieve a round wheel.

To develop your security wheel you need to start with an inventory of your current situation, set objectives and decide on relevant improvement processes. Try to anticipate possible obstacles during the progress towards your objectives. Try to anticipate solutions.

An assessment of how others perceive you can be achieved by trying to imagine how they would be talking about you.

Of course, you can also put the questions to trusted parties .

You need to find ways of changing any perception that does not suit you. Not all perceptions can be changed, of course. But it helps to be aware of them as they may have an impact on your security and protection.