Chapter 3: Risk analysis in programmes for the protection of human rights defenders

As a general rule, the risk analyses available to the authors in preparing this research were neither clear nor concrete;[1] in a sense, rather than efficient systems useful when analysing the risks faced by human rights defenders they present little more than a "list of needs", and classifications of the types of risk faced. As they may be consulted in the annexes to this book they are not presented in detail here. Instead, this chapter deals with a range of key questions related to the analysis of risks.

Risk analyses should respond to reality and to the needs of human rights defenders. If the systems used by the police do not fulfil this function, then protection programmes should contain their own system of risk analysis either in an attempt to reach agreement concerning adjustments to the schemes the police use, or to apply them directly, working in conjunction with the human rights defenders. Differences between the analyses might lead to conflicts of interpretation, but in any case it will be easier to adapt the programmes to varied circumstances.

It is also important to try and define risk, though this is not an easy task because the truth is that there is no single agreed definition of what risk means. The Colombian programme defines risk as the "objective probability that some danger faced by an individual or a group of individuals will be materialised in acts of damage or aggression".[2] Similarly, in the New Protection Manual for Human Rights Defenders[3] we say that "risk" refers to "possible events, however uncertain, that cause damage". The level of risk depends on the threats received but also on the degree of vulnerability of the defender to these threats and the capacity they have to confront them. For example, faced with a generalised threat against "everybody who works in Human Rights" in a city, organisations with greater capacity (a security plan, protection measures in the office, support networks etc.) will not face the same risks as much more vulnerable organisations (with no awareness of the importance of security, no protection for their office or for computer equipment, etc.). Thus, the management of risk focuses on acting in response to threats, vulnerabilities and capacities. For an in-depth treatment of this topic, see annexes).[4]

Risks are *circumstantial* (because they depend on context and circumstances), *changeable* (because they change when significant events occur) and *subjective* (because each individual in an organisation may perceive them differently). In other words, risk cannot be "measured" and it is therefore necessary to reach agreement about the level it has reached.

1 That is, the analyses that appear in the Guatemalan and Brazilian programmes; we have not had access to the Colombian programme, nor to the protocols used by the different police forces to evaluate risk.

2 Decree 1740 of 2010, article 3.

3 See the manual in question, which may be consulted at: *http://protectionline.org/-Protection-International,318-.html*

4 Adapted from Chapter 1.2 of the New Manual for the Protection of Human Rights Defenders (see bibliography).

Some protection programmes use a numerical system to determine the level of risk.[5] Others just draw approximate conclusions based on the views of the person who carries out the analysis. This chapter presents a process that may be used to determine the level of existing risk by consensus.[6] It involves two steps: first the determination of the level of risk; second, how to manage the risk according to the level that has been determined.

📖 Before continuing, it is important to differentiate between and separate the analysis of threats from the analysis of risk

An analysis of threats is carried out to study a threat and to try to determine the possibility that it may be made effective in an attack against a defender. For example, if a defender has received a death threat by telephone it is useful to analyse if it is likely to be carried out in the form of direct physical aggression. But this is not an analysis of risk; risk analysis is a more complex process that takes more factors into account.

We therefore recommend carrying out the analysis of threats *first* and the risk analysis *subsequently*.

I. Determining the level of risk

Determining the level of risk is not a question of seeking to "measure" it objectively, but to interpret it; that is, agree on how it should be understood according to a perspective of providing protection to the defender. The Colombian programme defines the "study of the level of risk" as the "result of the technical security analysis concerning the gravity and imminence of the situation of risk and threat faced by the individual, family or group of persons, as well as the specific conditions of vulnerability that affect them".[7]

Although there are different ways to determine the level of risk, in general the process involves determining if the level is "high, medium, or low", in reflection of the probability that something will occur and of the impact it would have if it did.

The probability of an aggression occurring: *what is the probability that an aggression will be committed (against individuals or an organisation).*

The following table may be used to characterise this probability:[8]

5 This is the case with the (non-governmental) case of UDEFEGUA (Guatemalan Defenders Unit).

6 The process is based on the results of the current research and previous experience in the field.

7 Decree 1740 of 2020, article 3.

8 Adapted from the New Manual for the Protection of Human Rights Defenders (see bibliography).

Table characterising the possibilities that a given aggression will occur in the following … (days or months)

Probability		Previous Reflections / in summary form	Influencing Factors								
			Threats and direct actions carried out up to now by the Aggressive Party (AP).	Ability to operate in the zone analysed.	Skills and resources of the AP.	Political, military or hegemonic motivation in the zone.	Economic motives.	Previous aggressions (against the same or different defenders).	Attitudes or intentions.	Ability of the security forces to prevent aggressions	Our levels of political influence in order to neutralise the AP.
Aggression very probable	It is very likely that it will occur, almost certain in fact; effectively we have to treat it as a fact.	The conjunction of threats and action is clear, and there is an intention to attack.	Clear and explicit threats, direct actions such as other threats or surveillance operations.	AP controls the zone, or operates at ease in it.	It has them.	The Defender clearly damages their ability to achieve objectives, benefits their opponents, etc.	The AP desperately needs equipment or resources in cash form.	Clear cases of previous aggressions.	Aggressiveness – clear current threats.	Inexistent, there is no capacity or will (the armed forces collaborate with , ore, the AP)	Limited (depending on circumstances) or inexistent.
Aggression probable	It is expected to occur; it is more likely to happen than not.										
Aggression possible	It might happen; it would not be strange if it did.	There are threats and minor actions, but apparently no desire to carry out direct acts of aggression.	Clear and explicit threats. Minor actions (low level or sporadic surveillance).	AP acts in nearby zones and could start operations in this one.	It has some, or could acquire them.	Partial – the Defender is an obstacle to their political or hegemonic objectives.	The AP is interested in equipment, cash resources or other income (eg from kidnapping).	There have been a few cases.	Not overly interested. Occasional threats; frequent warnings.	Low.	Medium to Low.
Aggression improbable	It might happen, though it would be somewhat surprising if it did; but the likelihood cannot be rejected.	The threats do not refer to direct aggression.	Veiled, non-explicit or anonymous threats. There is no history of actions.	Low capacity to act in the zone.	It has few or no resources to carry out an aggression such as that analysed.	None – the Defender does not constitute an obstacle to their objectives.	AP does not need our equipment or money.	No cases or exceptionally.	They claim to be close or to identify with us, or are indifferent.	Existent.	Good.
Aggression very improbable	It would be very strange if it happened; it has never happened before – there are no antecedents.										

***An example of the probability of direct acts of aggression**: the potential aggressor controls the zones where the defender operates but has no economic motivation for carrying out an attack. The work of the defender only limits the potential aggressor's political and military objectives partially and there are no precedents for similar aggressions in the zone. The attitude of the potential aggressor is indifferent and it is clear that it is not in their interests to attract the national or international-level attention or pressure that would result from an attack on the defender. However, the potential aggressor does, through third parties, issue veiled threats against the work of the defender.*

***Conclusion**: The probability of direct aggressions against the defender is in this case considered to be low or medium.*

It will be apparent that we use terms such as "given aggression" or refer to the execution of a specific threat that has been received. It is important to refer to *concrete* aggressions or threats.

It is also important to establish a deadline or timescale (two weeks, two months, six months etc.) to govern the probability analysis. For example, what is the probability of an aggression such as this occurring during the next six months? Or: is it likely to be repeated during the next two weeks?.

The Impact of an Aggression: *how great would the impact of this aggression be on the defender or the organisation (taking different factors into account).*

The following table may be used to characterise the potential impact of a given aggression:

How to determine the impact of an aggression				
Impact	**On individuals (in cases analysed or on other associated individuals)**	**On property, resources, information (in cases analysed or in relation to associated third parties)**	**On reputation and image (in cases analysed or in relation to associated third parties)**	**On the continuity of work (in cases analysed or in relation to associated third parties)**
Very High	Lives clearly at risk, there might already have been other deaths	Losses or irremediable damage	Overwhelming effects	Impossible to continue

High	Lives at risk, or physical integrity at risk (serious attacks), prolonged imprisonment, etc.	Losses or serious damage	Serious effects	Serious difficulties, it is not clear whether it will be possible to continue
Medium	Non-serious attacks, brief imprisonment	Moderate losses	Partially affected	Work will continue, with difficulties still to overcome
Low	Insults or similar	Light losses	Very little affected	Scarcely affected
Very Low	No	No	Not affected	Not affected

To determine the level of risk, it is necessary to combine the probability that something will occur with its impact. In this way it will be possible to classify the risk as Very High (VH), High (H), Medium (M), Low (L), or Very Low (VL), using the following table:

Determination of the level of risk					
Impact / **Probability**	**Very Low or None**	**Low**	**Medium**	**High**	**Very High**
Very Probable	L	M	H	VH	VH
Probable	L	M	H	H	VH
Possible	VL	L	M	H	H
Unlikely	VL	L	L	M	M
Very Unlikely	VL	VL	VL	L	L

It is apparent that "Very High" levels of risk correspond to a "Very Probable" attack that "endangers the life of the defender (for example, a murder attempt). "Very Low" risks correspond to a "Very Unlikely" action that produces "pressures" or "verbal harassment ".

In order to determine the level of risk using this table it is necessary to enter into debate and draw conclusions; it is not always easy to reach agreement. If it is not possible to agree between two levels of risk it is best to choose the higher, to ensure that the benefit of the doubt always favours security.

The constitutional presumption of risk, extraordinary risk, and the Colombian programme

The Colombian Constitutional Court has referred to the concept of the "constitutional presumption of risk" which it links to the "duty to pay particular attention to the population displaced by the authorities" when the "conditions that activate the presumption of risk" are fulfilled. These conditions are:

a. the presentation of a request for protection to the authorities by the displaced individual,
b. that the request was duly registered by the competent authority,
c. the request contains information that demonstrates, prima facie, that the individual has been displaced as a result of violence, sufficient evidence being the registration papers presented to the Unique Register of the Displaced Population, and
d. the information presented refers specifically to an identifiable threat to the life and integrity of the petitioner or their family or to an act of violence committed against them, related to concrete events that indicate they were the object of threats or attacks.

This presumption of risk should be applied by the authorities until its substance is determined by a "specific, technically conducted, security analysis". The current decree covering the Colombian programme has, for the first time, incorporated the presumption of risk in the case of displaced persons.[9]

The new regulation covering the Colombian programme[10] describes "ordinary" risk as "that to which all persons are subject, equally, as a consequence of their membership of a given society and which generates an obligation on the part of the state to adopt general security measures by providing an effective police service". Following on from this, "extraordinary" risk is defined as "that which persons are not legally obliged to assume and which brings with it the right to receive from the state special protection provided by its authorities". This legal distinction is very important, because it specifies a right to protection that was not present in previous versions of the programme. It is based on several sources, including the Colombian Constitutional Court's Sentence T-719 of 2003 and Decision 200 of 2007. The Colombian programme utilizes the Constitutional Court's characterisation of extraordinary risk:[11]

a. That it should be specific and individualizable.
b. That it should be concrete, based on particular and manifest actions or facts and not on abstract suppositions.
c. That it should be current and not remote or presumed.
d. That it should be important, that is, that it threatens to damage goods or legal interests, or the physical, psychological or sexual integrity that is valuable to the victim or witness.

9 Decree 1740 of 2010 (Section III).
10 See Decree 1740 of 2010 (article 3), in annex.
11 Decree 1740 of 2010 (article 3).

e. That it should be serious, and likely to be carried out given the circumstances of the case.

f. That it should be clear and discernible.

g. That it should be exceptional to the degree that it should not be borne by individuals in general.

h. That it should be disproportionate when compared to the benefits derived by the person from the situation that generates the risk.

It also adopts the definition of "**extreme risk**" as "that which threatens the rights to life and integrity, liberty and personal security and occurs when all the characteristics indicated for cases of extraordinary risk are present. Additionally, this type of risk should be grave and imminent and directed against life or integrity, liberty and personal security, with the evident intention of violating these rights ".

In its definition of risk the Brazilian programme incorporates the same characteristics assigned by the Colombian programme to extraordinary risk.

Once the level of risk faced by the defender or the organisation has been determined it is possible to pass onto the next stage, risk management.

II. Managing risk: decisions and processes to put into practice

Before taking decisions on managing risk, it is useful to examine first what can be done with it, as set out in the following table:

What can be done with risk? Strategic decisions (first of all)		
Level of Risk	**What can be done**	**How to do it**
Very Low or Low Risk	**Accept** the risk	Continue with habitual activities, without forgetting to monitor the context and the risk, in case there are changes.
Low, Medium or High Risk	**Reduce** the risk	This involves **acting on the risk** in order to reduce it. This can involve applying the risk equation (reduce risks, reduce vulnerabilities and increase capabilities: see annexes). Another alternative is **to share the risk**: by acting jointly with allies the risk of aggression is shared and may be reduced.

High or Very High Risk	**Avoid** the risk	When the risk is high or very high it is difficult to reduce it in the short term and it is necessary to initiate measures immediately to avoid it. These measures generally interrupt work or habitual activities and generate drastic changes during an indeterminate period of time. Simultaneously, measures should be put in place to reduce the risk in the medium term.

It is important to remember that when the risk is high or very high it is difficult to continue with day to day activities in the same way as before, because drastic measures are generally required to reduce the risk, including: changes in routines, the implementation of security measures, the dedication of time and resources to avoiding and reducing risk (acting to reduce the threats and vulnerabilities). These options are indicted in the following table:

How to influence the level of risk affecting a defender and/or organisation				
Situation / Risk	**Description of the general situation**	**Continuation of normal activities**	**Security plan and security measures**	**Time to be dedicated to security**
Very High	Very dangerous and unpredictable	No	Absolute priority	All that is necessary
High	Dangerous and unpredictable	No, save exceptions	Priority	All that is necessary
Medium	Dangerous but predictable or manageable	Yes, with changes to the activities most associated with the risk	Important: integrated into activities	Part of the time (reducing the amount of time usually dedicated to normal activities)
Low	Little danger, and manageable	Yes, in general	Normal	Normal
Very Low	Manageable	Yes	Normal	Normal

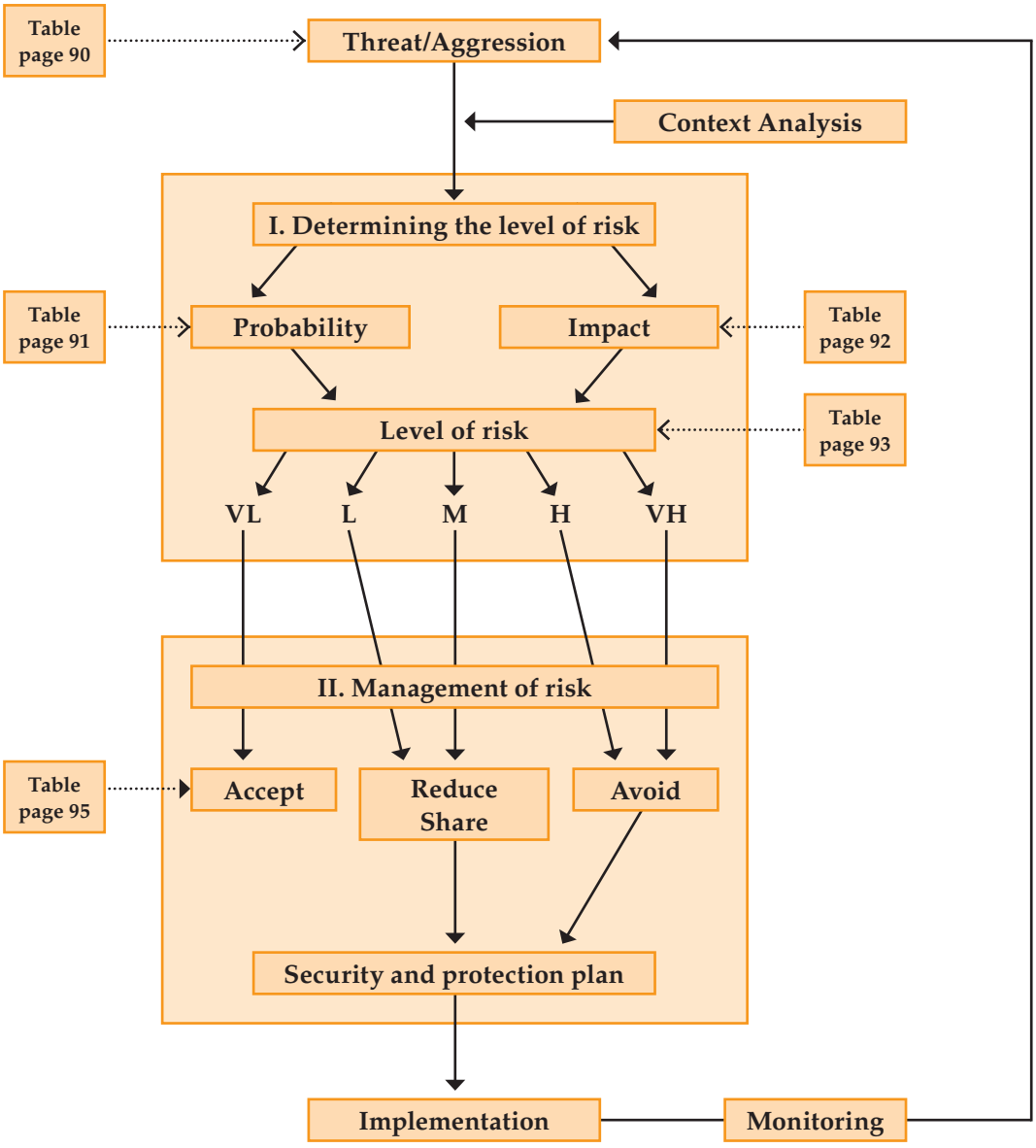
Risk analysis focused on risk management: taking decisions on security

The next step involves analysing the risk from the point of view of its components, so as to be able to establish a protection and security plan. At the beginning of the chapter risk was defined as "possible events, however uncertain, that cause damage". Risk was said to

depend on threats that have been issued but also on how vulnerable the target is to these threats and what capacity they have to face them; consequently, the management of risk means acting on threats, vulnerabilities and capacities. This topic is dealt with in greater detail in annexes.[12]

Summary: the process of analysing and managing risk

The following table summarises the process of analysing and managing risk; it draws on the tables and tools presented previously in the chapter.



12 Adapted from the New Manual for the Protection of Human Rights Defenders (see bibliography).

Finally, it should be remembered that:

- When defining the level of risk the idea is not to "measure" it objectively but to interpret it. That is, agree, from the point of view of the defender, how it should be understood.
- It is important to separate the analysis of risk (determining the level of risk) from decisions about how to manage it (the protection and security plan).
- Frequently, when it comes to analysing a situation there is a tendency to confuse the analysis of risk with the analysis of how it should be managed. Nevertheless, it is important to separate the two and to carry out first the analysis of risk (to determine its level) and subsequently decide how it should be managed (the protection and security plan).

  For example, a "medium" risk might be managed by implementing a simple protection plan.