4.2 Developing a security strategy

An organisation's security strategy in a particular operational context comprises a balance of approaches and the specific measures it decides to take. These are informed by the risk assessment process, together with the organisation's principles and values. This chapter introduces the three broad, overlapping security approaches that can shape a security strategy: acceptance, protection and deterrence.

4.2.1 Security approaches

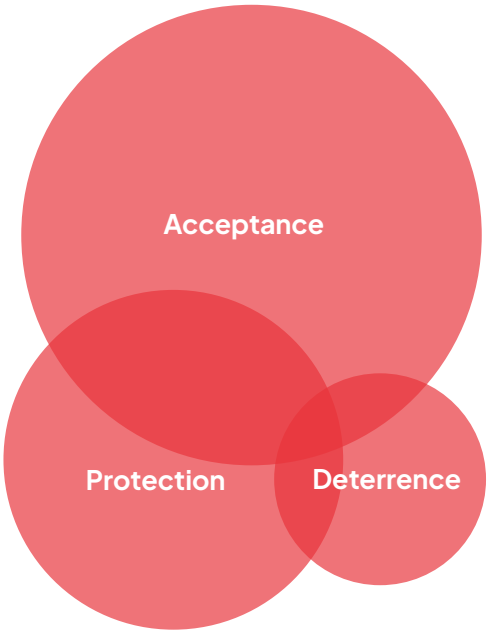
The concepts of acceptance, protection and deterrence each constitute a range of security options and actions, from 'soft' to 'hard'. As discussed previously:

- Acceptance measures attempt to reduce or remove threats by increasing the acceptance (the political and social tolerance) of an organisation's presence and its work in a particular context.
- Protection measures aim to reduce vulnerability to the threat but do not affect the threat itself[55] – this is often called 'hardening the target'.
- Deterrence measures aim to deter a threat with a counter-threat, such as the use of force (the classic example is armed guards).

Although acceptance, protection and deterrence are sometimes seen as separate strategies – each their own corner of 'the security triangle' – in practice, an organisation will usually choose a mix of options from each, depending on the operating environment. In different settings and as risks evolve, it may be appropriate to shift the emphasis from one type of measure (or overarching approach) to another. Rather than a static triangle, therefore, it may be more useful to imagine overlapping and interactive spheres, which can vary in emphasis depending on the context, risks and organisational strategy (see Figure 10).

55 Many security professionals, and previous editions of this GPR, used the word 'protection'. Note, however, that some security professionals use the term 'protective' (as in 'protective approach' and 'protective measures') to make a clear distinction between security risk management measures for staff, and protection as a type of humanitarian intervention focused on at-risk communities.

Figure 10 Example combination of measures in a security strategy



Given their principles and values, many humanitarian organisations view acceptance as the most appropriate and effective overarching approach and make it the foundation of their security strategy in a particular location (i.e. with most risk mitigation measures designed to increase acceptance, while actively avoiding any measures that may negatively affect perceptions and acceptance). This may mean, in some contexts, that an organisation decides not to use any deterrence measures at all, if doing so is perceived as not in line with the organisation's principles, values and acceptance approach.

Acceptance measures are not effective against all threats, which is why a combination of measures is often necessary. In environments where lawlessness or violence is pervasive or where armed actors have few incentives to negotiate, acceptance measures may have limited effectiveness on their own. However,

adding other types of measures does not necessarily mean abandoning an acceptance-led approach. On the contrary, the optics of adding visible protective measures, for example, may require more outreach and other active acceptance measures. The effectiveness of any approach will also be influenced by what other aid organisations are doing.

Protection and deterrence measures are not necessarily more effective in all cases and can bring their own problems. Protection measures focus attention on the organisation as a potential target and, unlike acceptance, do not address those who pose the threat. It can also lead to a 'bunker mentality', which can result in a restrictive operational model and a greater distance from target communities, all in order to reduce risk by insulating the organisation, its staff and assets. This makes it harder to develop relationships with others, which in turn makes it harder to get information about the environment and to communicate effectively with local interlocutors.

Deterrence measures – the least used among humanitarian organisations – have obvious downsides. If organisations display force, for example by driving with armed escorts or hiring armed guards for their offices, it is harder to convey an image of neutrality and non-violence.

A good security strategy needs a flexible combination of these measures, which may mean choosing one overarching approach that can guide the decision on what measures to prioritise. As a basis for any programming activity, it is good practice to cultivate acceptance and good relationships with the local population and their leaders, as well as relevant state and non-state actors. In more insecure environments with identified general risks to aid organisations, certain protection measures are usually advisable, particularly against crime. In highly insecure contexts, where there are significant risks to the organisation, deterrence measures may be necessary if this is the only way to protect staff and continue providing critical assistance, sometimes referred to as the 'principle of last resort'. If acceptance is the main approach, protection and deterrence measures can be adapted to maintain acceptance. Acceptance measures can be used to complement protection and deterrence risk mitigation measures.

Different measures have different resource implications. All carry a financial cost. Acceptance is perhaps the hardest to measure in financial terms but may require considerable staff time and possibly new programme initiatives, such as media outreach. Protection equipment carries a direct financial cost, while protection procedures (for example curfews or always driving with two cars) can add to

the budget by restricting operational capacity. A deterrence approach can have both small and large resource implications, which may be difficult or impossible to back out of in the long term (e.g. investing in armed protection).

4.2.2 Acceptance

Acceptance is often a broader organisational approach that focuses on fostering genuine relationships with affected communities and stakeholders while upholding core humanitarian principles. This approach is often seen as fundamental to providing legitimacy and consent for effective programme implementation. An acceptance approach also allows humanitarian organisations to distinguish themselves from other actors, such as military forces or private sector service providers.

In security risk management, acceptance is often understood as reducing or removing potential threats by cultivating and maintaining relationships with relevant stakeholders and gaining their 'consent' to operate in a particular location. In reality, 'consent' may not be the most appropriate concept to measure acceptance by. In practice, acceptance can be more helpfully understood as a continuum, ranging from accepted (most secure) to targeted (most insecure):[56]

- accepted
- tolerated
- rejected
- targeted.

Challenges to acceptance

The challenges to – and limitations of – acceptance are numerous. The following are some of the most prominent.

- **Funding.** How an organisation is perceived may be linked to where it gets its funding. The suspicion that those who provide the money control the aid organisation can create significant problems, particularly if the donor in question is a party to the conflict or is perceived as having a political agenda.

56 To learn more, see Fast, L. et al. (2011) *The acceptance toolkit: a practical guide to understanding, assessing, and strengthening your organization's acceptance approach to NGO security management.* Save the Children Federation (https://acceptanceresearch.wordpress.com/acceptance-toolkit/).

- **Principled humanitarian action.** In some contexts, both national and foreign governments may not want aid organisations negotiating or even communicating with non-state armed actors, even if this is necessary to undertake principled humanitarian action and access crisis-affected populations. Governments may penalise such negotiations, for example using counter-terrorism legislation. Organisations that accept funding with counter-terrorism clauses attached will need to ensure that all reasonable steps are taken to ensure compliance without compromising the humanitarian mission.
- **Advocacy.** The pursuit and preservation of acceptance may make it difficult for organisations to speak out about violations of international humanitarian law or human rights abuses as this can negatively affect relationships with various stakeholders. Organisational leadership benefit from having a structured approach to balancing advocacy efforts with security risk management concerns. (*See Chapter 2.2 on advocacy for a more detailed discussion.*)
- **Harmful information.** The implications of misinformation, disinformation, malinformation and hate speech for aid worker security are a growing area of concern and study. (*See Chapter 6.2 for a more detailed discussion on the challenges posed by harmful information.*)[57]
- **Proliferation and fragmentation of armed groups.** In many contexts the proliferation and fragmentation of armed groups is making it more difficult to determine who is in control of what territory, as well as who is in charge within an organisation (i.e. will negotiations with one representative be honoured by the rest of the group?). Some organisations have invested significant resources in monitoring armed groups to understand their internal structures and shifting patterns of territorial control.

Key components of active acceptance

Acceptance cannot be assumed; it must be actively forged and diligently maintained. 'Active acceptance' measures include strategic outreach to a wide range of stakeholders; developing staff skills in social, political and interpersonal relations and communications; and designing and disseminating core messages regarding the organisation's mission, objectives and programmes. Key components of an active acceptance approach include:

- Working with programme staff to integrate security risk management into programme design.

57 For a discussion on how technology can impact acceptance, see Al Achkar, Z. (2021) 'Digital risk: How new technologies impact acceptance and raise new challenges for NGOs' in GISF (ed.) *Achieving safe operations through acceptance: Challenges and opportunities for security risk management* (https://gisf.ngo/resource/achieving-safe-operations-through-acceptance/).

- Establishing and maintaining relations with key stakeholders, including armed actors. This can include engaging with national, regional and international actors, where relevant.
- Gaining acceptance from local populations (e.g. through meetings and socialising).
- Managing communications.
- Monitoring perceptions and public sentiment.
- Managing perceptions of staff and the organisation.

These are discussed in more detail in the following section.[58]

Programme integration

The ability of an organisation to meet people's needs in a transparent and accountable way is often critical to how it is perceived. Acceptance is widely recognised as connected to effective and responsive programming that meets the needs of a community. Community participation, consultation and local partnerships are often key elements of effective programming. However, even if programmes meet the needs of affected people, they may adversely affect specific actors or change political, economic and social power structures. Insofar as good programming is an essential component of acceptance, acceptance cannot be assumed from good-quality programming alone.

The connection between effective programming and gaining/maintaining acceptance should aim to be explicitly referenced in programme planning activities, included in programme plans, needs assessments and budgets, and incorporated into programme monitoring and evaluation tools.

Interacting with key stakeholders

Once key stakeholders have been identified and their respective positions, influence and disposition analysed, organisations can approach those who formally or informally exercise meaningful influence on whether an organisation can operate securely in a given environment. These may be friendly, unfriendly or neutral towards the organisation and can be identified in the actor analysis. National, regional and international actors must be considered alongside local stakeholders, as acceptance from these is becoming increasingly more important for effective humanitarian action.

▶ *See Chapter 4.1 for more on actor analysis.*

58 For a more detailed discussion of an active acceptance approach, see Fast et al. (2011).

It is important to assess the influence that each party has – in some situations having the acceptance of key influencers might be sufficient if it is not possible to secure the acceptance of all. Relying on staff from the area or using a respected intermediary (such as a religious or community leader) to reach out to other stakeholders on an organisation's behalf can support acceptance.

Building a relationship with key stakeholders usually requires more than rare, brief formal meetings. Messages can be conveyed not only in meetings but also through the type of meeting and how it takes place. Cultural customs should be followed and respected. Slowing down, taking time to meet and talk to people, explaining, listening, socialising and generally showing basic politeness and respect can all be important in securing acceptance.

Formal agreements, for instance with the government or with influential groups, can be useful in that they provide official recognition and explicit agreement on specific issues. With regard to security, agreements can spell out detailed responsibilities, including the procedures to be followed and a point of contact should security problems arise. Operational staff may wish to carry a copy of the agreement with them (in the relevant language) to facilitate access or dialogue. It is important to bear in mind that written agreements do not have the same value in every social environment, and other cultural practices may be more appropriate. Formal agreements can also be problematic, for example if they are valid for only a limited period of time, if they draw attention to areas where authorities may be inappropriately seeking to regulate or impede aid organisations' activities, or if they consume more staff time than they are worth. Formal agreements may also not be recognised across all levels of a group/entity. These factors should be considered before entering into formal agreements.

Non-state armed actors

Organisations working in an area under the de facto control of an armed group are likely to have to signal their presence to them and obtain assurances that their work is acceptable and that staff will not be harmed. Questions to consider when interacting (or considering interacting) with these actors include:

- What is the relationship between the armed group and the local population?
- What is the armed group's relationship with the organisation's staff?
- What is the command structure and state of discipline? What are the aims and objectives of the armed group?

- How might dialogue and negotiations with the armed group affect relations with others (including authorities)?
- What requests or demands (for example paying 'taxes' or getting daily 'permission' to operate) might be made, and how should the organisation respond?

Understanding these dynamics and risks requires a proactive capacity to analyse them. It will often make sense to work with other aid organisations to pool capacities and enable a common approach and common red lines (non-negotiable limits) when interacting with non-state armed actors.

▶ *See Chapter 4.1 for more discussion on armed groups as part of an actor analysis.*

Local populations

If there is a high level of acceptance, members of the local community may make suggestions as to how risk can be reduced, and in some cases may provide critical information and warnings to the organisation. Their influence, however, should not be overestimated, and in some circumstances communities may not be in a position to meaningfully reduce security risks at all. They may be powerless to influence other actors, may overlook or misjudge new threats, or may benefit more from supporting another actor.

There is a difference between mere tolerance of an organisation's presence and programme and true acceptance. People may accept an organisation's presence only because they are in desperate need, or may use aid as one source of support but may not feel an active responsibility for the organisation's wellbeing. Listening and responding to what people want, treating them with respect, acting transparently and being accountable may deepen relationships and encourage a greater level of acceptance. These relationships may even override the material dimension. An aid organisation can find itself unable to provide an adequate level of assistance or periodically even any assistance at all, and yet remain accepted based on the quality of the relationship.

Managing communications

For all stakeholders, communications need to be clear and consistent. An organisation and its staff should know and be able to explain – in succinct, easy-to-understand language – who they are, why they are there, what they want to do and how they relate to others. A simple question and answer sheet for staff can be helpful.

In the case of international and federated organisations, the need for consistency extends to aligning messaging globally. While certain communications may be adjusted slightly for different audiences, the overall message should aim to be the same, whether from head office or at a project site.

Public statements should reflect an organisation's values, principles and mandate and be contextualised for local understanding, as well as being mindful of the impact on local perceptions.

Critical public statements about local authorities require careful consideration. Key factors to weigh include the necessity of public disclosure, when to inform the subject, the phrasing and substantiation of claims, and the method of release.

▶ *For a more detailed discussion, see Chapter 2.2 on advocacy and security.*

Managing perceptions of staff

How staff are perceived can influence perceptions of the organisation as a whole. Identity-based characteristics play a role in this and can present both strengths and vulnerabilities, depending on local perceptions of those identity characteristics.[59]

▶ *See Chapter 1.2 for more discussion on identity-based factors and perceptions.*

Appearance and behaviour are also important. Personal appearance can carry important social and political meanings, and inappropriate behaviour can cause resentment and aggravate existing suspicions and tensions.

Respect for social and cultural norms (e.g. customs around dress, alcohol and interpersonal relations) can improve perceptions of staff and the organisation. Not all customs can be known or respected by those who are new to the context, but mistakes can be more easily forgiven if accompanied by a polite, composed and respectful attitude, or a clear position as to why customs are not being followed.

59 For a discussion of the benefits of recruiting a diverse and inclusive staff for acceptance, see Williams, C., Kinch, P. and Herman, L. (2021) 'Promoting a blended risk management approach: the place of programming and diversity within a SRM strategy' in GISF (ed.) *Achieving safe operations through acceptance: challenges and opportunities for security risk management* (https://gisf.ngo/resource/achieving-safe-operations-through-acceptance/).

Religious norms should also be considered and respected wherever possible; faith-based organisations may need to be extra careful about their image and activities.

Managing perceptions of the organisation

It is important to consider how the organisation and its activities are perceived. Are programmes what the local community most want and need? Some programming may not be considered a priority or may be negatively perceived by certain segments of the community. How do stakeholders who are not benefiting from the programme view the organisation and its staff? Are these stakeholders in a position to negatively impact acceptance among others, obstruct programmes or harm staff?

Understanding these issues entails listening to people and adapting accordingly. Even if a programme has wide acceptance within a community, it may still aggravate other stakeholders. This is true in virtually all sectors: a food aid programme may anger local traders by cutting into their profits; providing free health services may draw patients away from paid-for clinics, frustrating local health officials; and recording protection threats against the population may anger those responsible for the violence.

Another consideration is the exit strategy. Organisations may run good programmes but find that poorly executed exit strategies undermine the goodwill that had developed over the period of the programme. This means that they may struggle to gain acceptance in future.

Capacities and competencies for acceptance

Acceptance has practical implications, in terms of human resources, finances and administration. An active acceptance approach requires staff with certain key competencies. These can include:

- The ability to map key actors and establish a wide network with stakeholders.
- A thorough understanding of the mission and values of the organisation.
- Strong relationship-building and negotiating skills.
- Fluency in the local language and excellent communication skills.
- The ability to analyse changing political and security conditions.

Effectively applying an acceptance approach requires leadership from senior staff, who will need to have not only the requisite skills, but also sufficient time relative to their other responsibilities.

Acceptance is not cost-free. There are operational costs, including:

- Staff time, including hiring additional staff with security, outreach or media responsibilities.
- Training staff on how to communicate the organisation's mission and values, as well as cross-cultural communication and diplomatic and negotiating skills.
- Additional travel (vehicles, fuel, staff time) may be required to meet stakeholders.
- Translation of organisational materials or messages into locally appropriate formats and languages.
- Paying for the use of radio and television and other media, where necessary.
- Additional time required during the design phase of a programme.
- Communication materials, such as flyers.

These costs should be identified in the programme design and integrated into the budgeting process.

► *See Chapter 3.3 for more information about funding security.*

Pursuing an acceptance approach may also require adjustments to administrative or legal standards within the organisation, such as in the following examples.

- Although suppliers are generally chosen based on price and quality, an acceptance approach may require spreading contracts over different sectors of the local population so that people feel that the benefits are shared fairly. Likewise, it may be a good idea to buy locally, even if a non-local provider offers better value for money.
- The organisation may choose to adjust its recruitment procedures to contract a balance of diverse profiles (considering ethnicity and whether people are from the local area, for example).

Monitoring perceptions and measuring acceptance

There is no simple way of knowing how an organisation is perceived and whether (and why) it is accepted. It can be a positive sign of acceptance if relevant stakeholders:

- Publicly commit to accept responsibility for staff security.
- Share accurate security-related information with the organisation (e.g. warn that someone has been asking around about the organisation or that a certain threat is likely).
- Actively cooperate with or support the organisation's activities.
- Allow access (e.g. armed groups let organisation staff through checkpoints to reach programme areas).
- Help to secure the release of an abducted staff member or recover stolen assets.
- Acknowledge that the organisation has made a positive difference in people's lives.
- Apologise if members of a group do the organisation harm.

Acceptance can be the result of one staff member's strong relations in a particular location or setting. Organisations should be aware of this, and the potential implications if this staff member leaves the organisation, or perceptions of that individual change.

Acceptance may also diminish over time as people's needs and expectations evolve. Once a situation has stabilised, new aspirations can arise. Organisations should strive to continually monitor attitudes among local populations and key stakeholders to gauge levels of acceptance and any changes that might interfere with access and security.

A lack of acceptance, however, may have nothing to do with the organisation itself and cannot necessarily be improved by its efforts; it may, for instance, be a rejection of the concept of humanitarian action as a whole.[60]

60 For a more detailed discussion on the limitations of acceptance, see Daudin, P. (2021) 'Acceptance under stress: old recipes for new problems' in GISF (ed.) *Achieving safe operations through acceptance: challenges and opportunities for security risk management* (https://gisf.ngo/resource/achieving-safe-operations-through-acceptance/).

How to monitor and measure acceptance – some ideas

- A good understanding of the context and relevant stakeholders is a foundational element of monitoring acceptance.
- Introduce acceptance analysis as part of existing ways of working. This GPR presents it as a step in the security analysis process. Assessments of acceptance could also be integrated into security audits or community forums.
- Levels of acceptance can be gauged against objective criteria/indicators, such as the frequency of meetings with key stakeholders and the level and nature of interaction with key actors. Incident data can be useful but should not be the only indicator.[i]
- It may be helpful to break down relevant stakeholders and determine the level of acceptance of each, and outline useful information and key follow-up actions.[ii] It may be also beneficial to break down the acceptance levels of different actors in the location in question: the aid sector as a whole, the organisation and specific programmes and teams.[iii]
- Ways to gather information to inform this analysis include:
  - monitoring social media posts and mainstream media
  - conducting focus groups and consultations
  - undertaking periodic perception surveys
  - establishing feedback mechanisms
  - documenting the nature of informal conversations.
- Once acceptance levels are determined, these can be fed into a dedicated action plan or incorporated into risk mitigation measures and other activities. Unpacking the different factors that can influence perceptions, and determining the level of control the organisation has over these, can guide action (e.g. staff behaviour vs the political motivations of armed groups).

[i] For more examples of indicators, see Fast et al. (2011).

[ii] See, for example, GISF (n.d.) *2. Acceptance analysis*. NGO Security Toolbox (https://gisf.ngo/toolbox-pwa/resource/2-acceptance-analysis/).

[iii] See, for example, Billaudel, R. (2021) 'Measuring and improving acceptance: ACF's experience and perspectives' in GISF (ed.) *Achieving safe operations through acceptance: challenges and opportunities for security risk management* (https://gisf.ngo/resource/achieving-safe-operations-through-acceptance/).

Monitoring and analysing acceptance levels is a largely subjective exercise. This subjectivity can be managed by encouraging multiple individuals to participate in the evaluation process and having them share concrete examples to explain their impressions, using multiple sources of information, and using objective and standardised indicators across teams and locations.

4.2.3 Protection

Protection measures aim to reduce vulnerability. This can be achieved either by hardening the target or by increasing or reducing its visibility.

Hardening the target

Physical assets and procedures can reduce the likelihood of a threat getting near the target, or reduce the potential impact of harm on the target. In practice, this could mean:

- Site security equipment, such as installing lighting and alarm systems, erecting perimeter walls or installing metal gates and metal bars on windows (*see Chapter 7.2 for more details*).
- Asset protection, such as safes for cash and valuable equipment and vehicle alarms.
- Protection procedures such as controlling visitors' access, vehicle access and parking arrangements, and hiring guards to patrol locations and warn if there are intruders.
- Using armoured vehicles, personal protective equipment (PPE) and blast film on windows.
- Training staff on digital security (*see Chapter 6.2 for more details*).
- Driving in convoys, or arranging staff accommodation so that residences are grouped close together.

Strength in numbers can be effective but may not necessarily stop a determined attacker and could be counter-productive if greater numbers of casualties are the aim, or if another organisation is targeted and others become collateral victims. Likewise, while communications equipment is usually necessary, visible and expensive equipment may attract unwanted attention. Light and sound (e.g. movement-sensitive floodlights outside a building) can give some advance warning of an attack, allowing staff to take evasive action (get into a safe room, slip out) or call for assistance. Again, however, these devices may not prevent an incident.

Low-profile/low-visibility programming

Low-visibility programming has become increasingly common among aid organisations, especially when acceptance is determined not to be a viable approach. It involves removing organisational branding from office buildings, staff, vehicles and residences. It can also involve the use of private cars or taxis. In very high-risk environments, anything that might link staff to an organisation – organisation identity documents, mobile phones, computers – may be 'sanitised'. Staff likely to stand out from the local population may be moved to another location. In extreme low-profile postures, aid recipients may not be made aware of the source of assistance.

Another tactic of a low-visibility approach is to use removable logos for vehicles in areas where visibility is discouraged. Knowing when to display a logo, and when to take it off, demands a very good, localised and dynamic risk assessment. It is important to bear in mind, however, that removable magnetic stickers can easily be stolen and used by others to impersonate the organisation.

A low-profile, low-visibility approach can make programming more complicated and can distance the organisation from sources of information that might otherwise enhance its security. It might also lead to suspicions and misperceptions of what the organisation is doing, undermining acceptance. It is a difficult approach to maintain if the organisation is seeking wider recognition for its work from the public or from donors. Organisations generally do not see a low-profile approach as a permanent way of operating; rather, it is often viewed as exceptional and time limited. It may also be adopted at the start of a programme, and then gradually moderated as operations increase.

4.2.4 Deterrence

Deterrence involves posing a counter-threat: essentially, discouraging would-be attackers by instilling fear of counterforce or other serious consequences. Armed protection is the strongest form of deterrence used by aid organisations. There are other potential deterrents, however, and this section covers them briefly before going on to an in-depth examination of armed protection in humanitarian operations.

Forms of deterrence

Legal and diplomatic leverage

There are legal protections for aid workers under national and international law. Unfortunately, legal deterrents are not always effective. Some aid organisations may secure some leverage from the backing of foreign donor governments, particularly in negotiating access or resolving administrative problems with national governments, but their influence will be limited, and close interaction with donor governments can undermine the appearance of independence and neutrality.

Suspension of operations or withdrawal

In the face of certain threats or after security incidents, organisations have temporarily suspended their aid programmes or threatened to do so. The continuation or resumption of the programme is then made conditional upon the resolution or amelioration of the problem. Anecdotal evidence suggests that this tactic does not always work very well, and that organisations often resume their programmes despite no noticeable improvement, which can undermine their credibility and any such similar threats in the future.

The following are circumstances under which a suspension or threat of suspension may be effective:

- If it is not perceived as punishing people not linked to the causes of insecurity and who are not in a position to improve security.
- If an influential section of the population or local leadership/authorities can be mobilised on the organisation's behalf.
- Where organisations are prepared to maintain the suspension until the situation is satisfactorily resolved, and will not annul the decision too quickly because of internal or external pressure.
- Where other organisations do not undermine the action by stepping in to fill the gap – a common front ideally needs to be established before operations are suspended.

Unless the incident is very serious, a selective suspension (e.g. in a given location or for a given period) or the gradual reintroduction of services may provide more room for manoeuvre. A total suspension tends to create a difficult all-or-nothing situation.

▶ *See Chapter 4.3 for a practical discussion of the security implications of suspensions and withdrawal.*

Informal affiliation

Another deterrence option is to affiliate informally with influential local actors. In this scenario, an attack on the organisation might be implicitly perceived as an affront to these actors. This option needs to be approached very cautiously as it could undermine the organisation's humanitarian principles and its acceptance with other stakeholders, and could even result in the organisation becoming hostage to the protection of the powerbroker in question.

Armed protection

Humanitarian organisations do not normally use armed protection. However, there may be exceptional circumstances where it becomes necessary in order to enable humanitarian action, such as for humanitarian convoys entering major combat environments or where authorities demand it as a condition for access. That said, while armed protection might provide a measure of security and protection for humanitarian aid workers in the moment (though they can also do the opposite and draw fire), it can also complicate efforts to sustain humanitarian access in the long term. In other words, the practice undermines principled humanitarian action. IASC guidelines offer several reasons to avoid using armed escorts for humanitarian convoys because of the counter-productive implications in the long term.[61]

The relationship between armed protection and humanitarian action is fraught. Although virtually all aid organisations at one time or another have used some form of armed protection, it is often considered anathema, and discussions about it are highly sensitive. Cooperation with an armed actor – including a UN-mandated force – can lead local, national and international actors, as well as the population, to associate humanitarian organisations and aid recipients with the political and/or military objectives of that armed actor. This could potentially undermine the actual and perceived neutrality, impartiality and independence of the humanitarian organisation and the broader humanitarian community, as well as its acceptance. The impact of armed protection on acceptance is not always straightforward and can vary depending on the context and other influencing factors.[62]

61 IASC (2013) *IASC non-binding guidelines on the use of armed escorts for humanitarian convoys* (https://reliefweb.int/report/world/iasc-non-binding-guidelines-use-armed-escorts-humanitarian-convoys).

62 For a discussion on this, see Jourde, J. (2021) 'Private security contracting and acceptance: a dangerous match?' in GISF (ed.) *Achieving safe operations through acceptance: challenges and opportunities for security risk management* (https://gisf.ngo/resource/achieving-safe-operations-through-acceptance/).

While this section provides a more systematic framework for considering the matter, it is not intended as an argument for the use of armed protection but rather an exploration of potential benefits, risks and challenges. Before deciding whether to use armed protection, it is advisable to consider the pros and cons in the specific situation and explore all possible alternatives.

The following questions can be considered when deciding whether to use armed protection:

- Under what circumstances does the organisation permit the use of armed protection, in principle?
- Do the benefits of using armed protection in this context outweigh the risks?
- Are there serious concerns about how to manage armed protection, and can these concerns be overcome?
- How will the use of armed protection affect perceptions of the organisation particularly, and aid organisations generally, and impact levels of acceptance among key stakeholders?
- What are the local culture and practices relating to the use of armed protection? (This can affect how its use is perceived and accepted.)

At every step in the line of reasoning, it is possible to arrive at the conclusion that armed protection may not be appropriate. Bear in mind also that the need to consider armed protection at all may indicate that the threshold of acceptable risk has already been crossed, and the real decision that needs to be taken may be to withdraw or not begin programming. If this threshold has not yet been reached, or if armed protection could reduce the risk to a more acceptable level, then three major areas come into play in thinking through the decision: principles and ethics, context and management.

Issues of principles and ethics

Some argue that armed protection is against the basic principles of humanitarian action. This position tends to be based on ethical or long-term operational considerations. The ethical argument holds that humanitarian action is never compatible with the use of force. From an ideological perspective, an organisation may refuse armed protection because its use, as a matter of principle, contributes to the ongoing production and distribution of arms.

The long-term operational consideration is that, whereas armed protection might be justifiable in a given context, it may also erode the overall image of humanitarian action worldwide and may therefore lead to increased insecurity elsewhere or in the future. According to this line of reasoning, resorting too quickly or too often to armed protection undermines global efforts to increase respect for international humanitarian law and independent humanitarian action.

There are also practical considerations. Armed escorts make aid work much less flexible in terms of movements, as permissions and escorts often have to be organised in advance. Making movements more predictable may increase an organisation's vulnerability to attack, particularly if escorts are not fully trustworthy.

Arguments in favour of the use of armed protection hold that it can be acceptable as a last resort, and when people's survival would be at risk if humanitarian and other assistance were curtailed.[63] In some contexts, the use of armed protection to facilitate the provision of aid may be a function of the state exercising its obligations under national and international law or government policy.

Another major consideration concerns who benefits from armed protection:

- Is it only the aid organisation and its staff, or can the protection provide wider public benefits and enhance public security?
- Will the use of arms and armed guards – perhaps recruited locally – have a pacifying effect on the local situation, or will it increase tensions?
- Is it contributing to the 'privatisation' of security, whereby only those who are able to pay can obtain security?
- Is it indirectly putting others at risk by making them soft targets in comparison? It is important to consider what effect, if any, it has on the broader security environment.

Even if the use of armed protection is deemed necessary and legitimate, it may not be ethical or practical to pay for the service from private contractors, groups or individuals. Protection from a state or internationally mandated police or military forces may be provided free of charge in some contexts, but not always. Following experiences with protection rackets among Somali militia guards in the 1990s, some aid workers argued that aid organisations should never pay

63 UN and IASC (2008) *Civil–military guidelines & reference for complex emergencies.* UN Office for the Coordination of Humanitarian Affairs (OCHA) (https://digitallibrary.un.org/record/697614?ln=en&v=pdf).

for armed protection. The reality is that most have done so when they judged the circumstances required it. It is also sometimes a legal obligation in some contexts.[64]

Dependence on support from an armed actor can also make it extremely difficult or impossible to operate without such support in the future, undermining the sustainability of humanitarian operations. The provider of armed protection may develop a financial interest in maintaining the service. Additionally, the sudden cessation of armed protection can expose a humanitarian organisation as a soft target.

One organisation's decision to use armed protection has implications for others, as it can influence the image and perception of all humanitarian organisations, and therefore potentially affect acceptance and relationships more widely. This is a topic that merits structured interagency reflection and discussion. While generally rare among NGOs, armed guards and/or armed escorts are commonly used by UN agencies operating in contexts deemed high risk, such as Afghanistan, Iraq and Yemen. In many contexts, this has led to divergent security postures between UN and NGO humanitarian actors. During clashes in the Gambella region of Ethiopia in 2022, UNDSS recommended the use of armed escorts for humanitarian deliveries. Some international NGOs were later alarmed to discover that their local teams in Gambella had acted on this recommendation.

Questions of context

Beyond questions of principle, ethics and risks to an organisation's acceptance, a set of further, context-specific questions can be posed when deciding on the use of armed protection.

- *What are the threats and who are the targets?*

Deeper analysis can shed light on the source of the threat, the target and the motives of potential perpetrators. Important distinctions can be made between threats related to site security and movement security, and threats specifically to the aid organisation (its personnel and assets) and more generally to affected populations. Even where armed protection appears justified, it may not provide a reasonable deterrent, or may increase the risk. For example, if burglars suspect that a resident has a firearm, they may turn violent if surprised in the act. If road bandits see an armed convoy, they may shoot before robbing it. Who is the target is also an important consideration. If armed protection is provided by government forces or a particular faction, the organisation may become a

64 Stoddard, A., Harmer, A. and DiDomenico, V. (2008) *The use of private security providers and services in humanitarian operations*. HPG Report 27. London: ODI (https://odi.org/en/publications/private-security-providers-and-services-in-humanitarian-operations-2/).

legitimate target in the eyes of the armed opposition. There is also the risk of accidents from 'friendly fire' or mishandled or malfunctioning weapons.

Maintaining the distinction between the organisation and its armed protection

Aid organisations can consider the following actions to distinguish or distance themselves from armed protection:

- Ensure armed actors protecting convoys travel in separate vehicles.
- Prohibit weapons inside the organisation's premises or vehicles.
- Avoid wearing clothing (including colours) that resembles that of armed forces.
- Refrain from using military assets (e.g. trucks, helicopters); repaint and re-mark if unavoidable.
- Exclude armed guards from compounds unless absolutely necessary.
- Use armed bodyguards only for targeted threats like kidnapping or assassination, applying 'close protection' when needed.

Whether these steps actually help to maintain a perceptual distinction and allow the organisation to retain some part of its civilian and non-combatant image often depends on the specific local context.

► *Who is being protected?*

In dangerous environments, organisations tend to think about measures that will enhance their own security. It may be helpful to consider whether and how security could be improved in the area more generally. For example, armed guards in a refugee camp might be deployed in a way that protects not only organisation staff, but also refugee women at risk of sexual assault when collecting water and firewood. A system might be developed whereby the armed guards of several individual organisations patrol the neighbourhood and therefore increase the security of all. Where a UN peace operation is present and has a mandate to protect civilians, troops may be deployed to areas that are dangerous both for aid workers and for the local community.

► *Who is providing protection?*

It is also important to consider who is providing the armed protection. Potential sources include national military actors, national police, an armed resistance group, UN peacekeepers or police, local militia, private security companies and armed guards directly on the organisation's payroll. In some circumstances, an organisation not opposed in principle to the use of force may find that none of the potential providers is acceptable and effective, leaving the organisation the choice between operating without armed protection or withdrawing.

Example questions when choosing an armed protection provider

- What is the political position of the provider in a given conflict? Can the organisation be seen as taking sides if it associates itself with a particular actor?
- What is the provider's public image and reputation?
- How important for the provider is the extension of protection to an aid organisation compared with its other objectives? The provider may have another agenda (for instance engaging the enemy or capturing a criminal) that in critical moments may override concern for, or even jeopardise, the organisation's security.
- How professional is the provider? Are guards well trained, reasonably compensated, provided with functioning equipment, well instructed, supervised and disciplined?
- How much management control does the organisation need or want? Having more direct authority over the providers of armed protection allows for greater control, but also makes the organisation directly accountable for their behaviour and actions.
- What are the provider's 'rules of engagement' on the use of force and where does liability sit should force be exercised and injuries incurred?

► *See Chapter 2.1 for a broader discussion of private security providers, including some more detailed questions about code of conduct.*

Questions of management

A key managerial question relates to the rules of engagement (i.e. when force can be used and to what degree). The basic rule is usually that force can only be used to protect life when clearly threatened, and as long as the threat persists. In other words, lethal force can only be used in defence and not, for example, to shoot a burglar, even an armed one, who is fleeing and no longer constitutes an immediate threat. What constitutes an immediate threat to life and wellbeing should be worked through in concrete terms, imagining different scenarios.

Rules of engagement should also be clarified for the protection of assets. While an organisation's instinctive preference may be that no force should be used when only assets are at risk, is it acceptable to do nothing while a warehouse is emptied or all the food in a convoy is stolen by armed actors, especially if there are people that really need and are dependent on those supplies? Organisations should aim to be very clear at what point and in which scenario engagement is acceptable.

Case example: Rules of engagement in practice

One international organisation has used unarmed guards from a private security company in the Democratic Republic of Congo and South Sudan. The company also has an armed response unit with either its own armed guard or an embedded armed police officer. While the organisation primarily uses unarmed guards, discussions with the private security company also covered key questions including the rules of engagement in the event this armed response unit was summoned.

Another important management aspect is to agree procedures and approaches for a number of possible scenarios, including what to do when a visitor refuses to be searched or insists on bringing in their own armed guards, and how far to go in the pursuit of fleeing robbers or attackers.

For instances where armed protection is sought, agreement may need to be reached on:

- Who provides the weapons (this is normally the provider of the personnel).
- What type of weaponry the guards will use (e.g. pistols, single shotguns or machine guns).
- Who is responsible for providing the ammunition and for checking that the weapons are well maintained and properly registered.
- Who is responsible for the provision of additional equipment, such as clothing and torches for guards.
- What vehicles, if any, armed guards have access to – armed guards do not always come with vehicles and decisions may have to be made about if and when they can use the organisation's.

Command and control work both ways: if an organisation puts itself under the protection of an armed actor, it may be expected to abide by the armed actor's rules. For example, suddenly leaving a convoy, speeding ahead or driving off may not be accepted by the security provider.

In a multinational peacekeeping force, different national militaries tend to have different traditions and cultures, including with regard to command and control, rules of engagement, and what is considered appropriate or excessive use of force. Detailed in-depth consultation with commanders at different levels may be required to ensure a common understanding. Different commanders may have different views, and it can be helpful to have a detailed written agreement with a senior commander to manage relationships across different levels. It is advisable to monitor changes to make sure that any replacements are fully briefed.

► *To learn more about civil-military coordination, see Chapter 2.1.*

Summary of key managerial questions

Key management questions to consider include:

- Are the policies, procedures and management competences necessary for handling this relationship available within the organisation and the location in question?
- What are the necessary contractual stipulations?
- Who maintains command and control, and who has authority and responsibility for what?

- Who in the aid organisation makes the decision/approves the use of armed protection?
- Will the armed guards always be present or only at certain times or in certain places?
- How are tenders drawn up and bids assessed from private security providers?
- What inquiries can be made concerning the professionalism and integrity of a potential service provider?
- Who are the guards answerable to, who has the authority of command and who is in charge of discipline?
- Where external security forces provide armed protection, what is the authority of their commander versus that of the organisation?
- Who determines the rules governing the use of deadly force, and who ensures that guards have fully understood them?

Policy

Organisations benefit from having an organisation-wide policy on the use of armed protection. Important points to consider include:

- Clarification of the organisation's position regarding the use of armed protection in principle.
- The conditions that could justify the use of armed protection, for instance during the evacuation or relocation of staff in periods of extreme insecurity (this can include references to programme criticality and the consequences of using armed protection).
- What alternatives have been considered to address risks, and if armed protection is truly the last resort.
- The key considerations and risks (legal, reputational and physical), both for the organisation concerned and for others, when choosing potential providers, and how they are to be evaluated.
- The terms that need to be agreed between the organisation and the provider.
- The organisational procedure for decision-making and periodic review.

- The obligation to accompany the use of armed protection with increased communication efforts to explain its rationale – that is, how it can support other security approaches, especially acceptance.

Sample policy

Under the policy of one organisation, armed protection can be considered when:

- large numbers of lives are at risk;
- the threat is related to widespread banditry, not political;
- the provider meets relevant standards;
- the deterrent can be effective; and
- the use of armed protection is authorised at the appropriate organisational level.

A policy on armed protection is not the same as a policy on private security companies, even though private security companies are often the providers of armed protection. An organisation might contract private security companies for other purposes (e.g. risk assessments or security audits) and other types of actors can also provide armed protection. The use of either should be guided by established policy.

► *To learn more about private security providers, see Chapter 2.1.*

Further information

Research and discussion

Al Achkar, Z. (2021) 'Digital risk: How new technologies impact acceptance and raise new challenges for NGOs' in GISF (ed.) *Achieving safe operations through acceptance: challenges and opportunities for security risk management* (https://gisf.ngo/resource/achieving-safe-operations-through-acceptance/).

Bamber-Zyrd, M. (2023) 'ICRC engagement with armed groups in 2023' *Humanitarian Law & Policy*, ICRC (https://blogs.icrc.org/law-and-policy/2023/10/10/icrc-engagement-with-armed-groups-in-2023/).

Daudin, P. (2021) 'Acceptance under stress: old recipes for new problems' in GISF (ed.) *Achieving safe operations through acceptance: challenges and opportunities for security risk management* (https://gisf.ngo/resource/achieving-safe-operations-through-acceptance/).

GISF (2021) *Achieving safe operations through acceptance* (https://gisf.ngo/resource/achieving-safe-operations-through-acceptance/).

Stoddard, A., Harmer, A. and DiDomenico, V. (2008) *The use of private security providers and services in humanitarian operations*. HPG Report 27. London: ODI (https://odi.org/en/publications/private-security-providers-and-services-in-humanitarian-operations-2/).

Williams, C., Kinch, P. and Herman, L. (2021) 'Promoting a blended risk management approach: the place of programming and diversity within a SRM strategy' in GISF (ed.) *Achieving safe operations through acceptance: challenges and opportunities for security risk management* (https://gisf.ngo/resource/achieving-safe-operations-through-acceptance/).

Guidance and resources

Fast, L. et al. (2011) *The acceptance toolkit: a practical guide to understanding, assessing, and strengthening your organization's acceptance approach to NGO security management*. Save the Children Federation (https://acceptanceresearch.wordpress.com/acceptance-toolkit/).

GISF (n.d.) 'Acceptance analysis template - xlsx'. *2. Acceptance analysis*. NGO Security Toolbox (https://gisf.ngo/toolbox-pwa/resource/2-acceptance-analysis/).

United Nations and IASC (2008) *Civil–military guidelines & reference for complex emergencies.* UN Office for the Coordination of Humanitarian Affairs (OCHA) (https://digitallibrary.un.org/record/697614?ln=en&v=pdf).