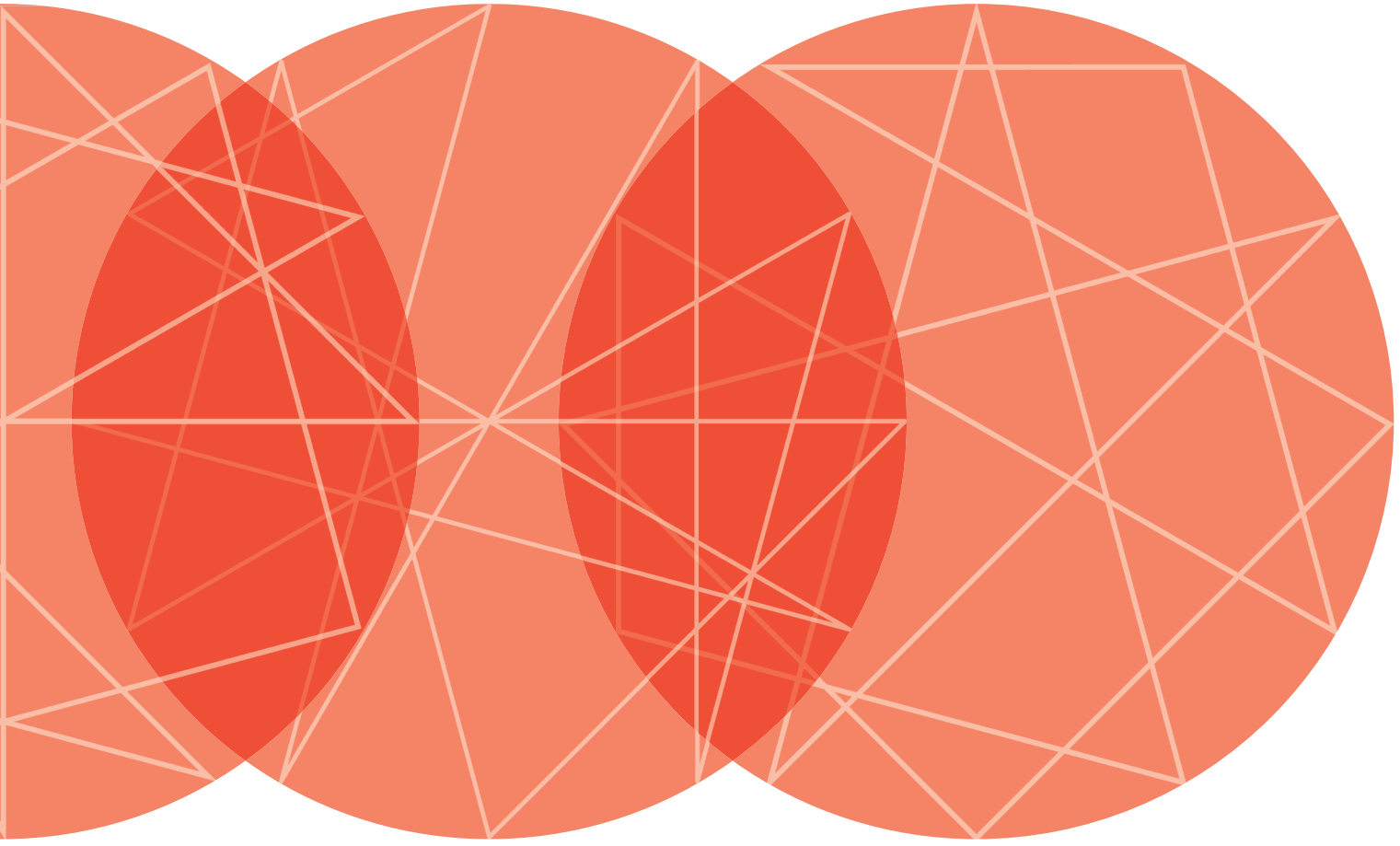
eisf

Security Management and Capacity Development:

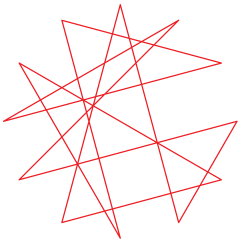
International agencies working with local partners

EISF Briefing Paper



European Interagency Security Forum (EISF)

eisf



European Interagency Security Forum

The European Interagency Security Forum (EISF) is an independent platform for Security Focal Points from European humanitarian agencies operating overseas. EISF members are committed to improving the safety and security of relief operations and staff in a way that allows greater access to and impact for crisis-affected populations.

The Forum was created to establish a more prominent role for security management in international humanitarian operations. It provides a space for non-governmental organisations (NGOs) to collectively improve security management practice, and facilitates exchange between members and other bodies such as the UN, institutional donors, research institutions, training providers and a broad range of international NGOs (INGOs).

EISF fosters dialogue, coordination, and documentation of current security management practice. EISF is an independent entity currently funded by the US Office of Foreign Disaster Assistance (OFDA), the Swiss Agency for Development and Cooperation (SDC) and member contributions, and is hosted by Save the Children UK.

Acknowledgements

This Briefing Paper was initiated by Oliver Behn and Madeleine Kingston, written by Iesha Singh and the EISF Secretariat. It was also edited by the EISF Secretariat.

EISF and the author would like to thank George Shaw, Sicko Pijpker, Euan Mackenzie, Adele Harmer, Maarten Merkelbach, Tom Brabers and Anthony-Val Flynn for reviewing the paper and providing valuable input and feedback at various draft stages; James Darcy and Julian Sheather were important in developing the ethical perspective; Shaun Bickley should not be forgotten for his support; together with Elisabeth Baraka at A4ID for facilitating access to pro bono legal advice; Sean Hardy from Mayer Brown International LLP for reviewing the paper from an English Law perspective; Edward Kemp for providing valuable input on duty of care; and Chamutal Eitam for helping to bring all the pieces together.

We would also like to thank all those who agreed to be interviewed for the paper and who shared their valuable insights and perspectives.
A full list of participants can be found in Annex 3.

Disclaimer

Abbreviations

ACF	Action Contre la Faim (Action against Hunger)
CAP	Consolidated Appeals Processes
CP	Contingency plan
CSD	Centre for Safety and Development
ECHO	Humanitarian Aid and Civil Protection Department of the European Commission
EISF	European Interagency Security Forum
ICCO	Interchurch Organisation for Development Cooperation
IFRC	International Federation of Red Cross and Red Crescent Societies
INGO	International non-governmental organisation
MoU	Memorandum of Understanding
NGO	Non-governmental organisation
WFP	World Food Programme
OFDA	Office of US Foreign Disaster Assistance
SLT	Saving Lives Together
SOP	Standard Operating Procedures
UN	United Nations
UNDSS	UN Department of Safety and Security
UNHCR	UN High Commissioner for Refugees (Office of)
WFP	World Food Programme

Contents

Overview

International agencies are continually reviewing the way they work with their local partners, most recently in response to changing security dynamics and an increasing awareness of security risks. However, their desire to support local partners can be hampered by cost implications, limited resources, over-reliance on local knowledge and skills and a partial understanding of the needs of partner organisations. This is compounded by confusion over the degree of responsibility international agencies bear towards their local partners.

This paper has two broad objectives. First, it aims to provide a better understanding of issues related to security and the responsibility of international non-governmental organisations (INGOs) to ensure the safety and security of their local partners.[1] Secondly, it provides insights into strategies for INGOs to provide support to their local partners in terms of security management. These strategies are based on those of agencies already implementing differing levels of support to their local partners for security management.

The paper notes the increase in the transfer of risk to local partners. The debate on 'risk transfer' has led to wider discussions about the changing nature of INGOs' roles and responsibilities with regard to their partner organisations. Legal responsibilities will depend on specific circumstances such as: the contractual terms of the partnership agreement, the nature of the relationship and the legal context (eg, which law applies). Ethical responsibilities, however, can be assessed through analysing, for example, how the association between the partners affects the risk profile, the degree of risk transfer and the threshold and capacity to manage risk, etc. It was found that organisations with more partner-driven and development approaches generally have better developed practices for partner support in security management.

The paper notes four key areas for support to local partners in current practice:

- development of organisational security policies and strategies (eg, security culture)
- knowledge transfer and capacity development
- communication and information exchange
- provision of physical resources.

Developing the capacity of local partners demands continuous investment and regular feedback and interaction between the partners. Partner support will face challenges during rapid onset disasters and spikes in acute humanitarian situations, where other priorities might prevail. A lack of resources (both physical and financial) and expectations around the nature of the partnership and commitments might also pose problems for effective partner support. In order to decrease security risks, mutual understanding of risks and prioritisation of security and related capacity development should be prioritised by all partners.

Thirty-three people from 23 organisations (including INGOs and UN agencies working in both secure and insecure contexts, with humanitarian and development mandates) were consulted for this paper.

1 For the purpose of this paper a local partner is defined as a national non-profit organisation (eg, NGO or community-based organisation). Other partnerships do occur in the field, eg, with government bodies and/or national for-profit companies/contractors. These are different from the above partnerships in ethical, operational and legal terms.

Introduction

The last years have witnessed growing concern by international agencies about how to work with their local partners in the South. This has been driven by a steep increase in observed risk of national staff and local partners and concerns about 'risk transfer'. Given the changing security dynamics and growing awareness of the inherent risks in implementing programmes, security and support to security management have become crucial. While it is increasingly recognised that support for security management is necessary, much of the discussion has so far centred on national staff within international NGOs (INGOs), while there has been little discussion about supporting local organisations working in partnership with INGOs.

Efforts to support local partners have been hampered by potential cost implications and limited resources, but also by an over-reliance on local partners' knowledge and skills and a partial understanding of their needs. Often, local organisation staff have an understanding of security management and the threats they face which differs from that of their international counterparts. Prevailing attitudes summed up by phrases such as 'these things happen' and 'we live here – it's normal' can lead to more risk-taking behaviour than is deemed appropriate by an international organisation. Local partners may often be reluctant to raise security concerns as they think it could affect their ability to obtain funding.

Another factor that hampers support to local partners is a lack of understanding of the varying degrees of responsibility that international organisations have towards their partners – and the limits of these responsibilities. There is also a limited level of practical guidance and resources available at the operational level to strengthen security management support to local partners. Where tools exist (particularly among more development-oriented organisations) these are often not widely shared and, consequently, awareness of existing tools and practices is low.

This paper sets out to go some way towards remedying the confusion around responsibilities, and increasing awareness of what is being done. The objectives are twofold:

1. to provide a better understanding of issues related to security and any interconnected responsibility of INGOs towards supporting the security of their local partners
2. to provide insights into approaches that can be used by INGOs to improve support to their local partners in terms of security management by discussing existing practices and tools. Existing tools that can be adapted are shared in the annexes.

The paper is intended to provide a first step towards a wider debate on partnerships with local organisations in terms of managing security risks.

Chapter 1 discusses three different models of partnerships between INGOs and local organisations and how these affect both responsibilities and ways of working. The three models are: partner-driven, consultative and sub-contracted. The section also looks into the changing security context and how this leads to an increase and change in risk transfer to local partners.

Chapter 2 looks at the legal and ethical responsibilities that might arise as a consequence of partnerships between an INGO and a local organisation. In terms of legal responsibilities, there is very little information available and generally any responsibility will be dependent on specific circumstances. Ethically, a number of principled questions are presented that international organisations can use to determine the nature and degree of their differing responsibilities towards their local partners. The section also provides a framework for ethical decision-making that organisations can use to decide how to deal with security management support.

Chapter 3 examines existing examples and tools for partner support, according to their phase in the project life-cycle and operational conditions. The project life-cycle is broken up into four distinct phases: project start-up, project planning and approval, project implementation, and project review. An additional section on support to partners during crisis management is also included. A diagram that can be used as a checklist in the development of partner capacities for security management is provided at the end of the chapter. Two tools that can be used to assess partner capacity and security management needs (which were developed by the ACT Alliance and the Centre for Safety and Development) are included as annexes.

Chapter 4 looks at the various challenges and questions that may arise when considering support to partner organisations to manage security. These centre on:

- differing perceptions and thresholds of risk between international organisations and local partners
- embedding a security culture
- ensuring transparency around resource needs
- how to behave within different humanitarian contexts
- questions around compliance and differing standards.

The conclusion underlines key areas for support.

Methodology

In order to understand the issues at stake, as well as what resources are available, a review of both primary and secondary documents was undertaken. These included the (internal) policies and handbooks of a number of UN agencies and INGOs, as well as external reports and presentations on security concerns and management. (For an overview of open-source documents, see resource list.)

A number of semi-structured interviews were conducted with key stakeholders during June and August 2011. In total, 33 people from 23 organisations were consulted (see Figure 1 below and Annex 1 for more detail). Unless otherwise referenced, all the information in this paper has been obtained through these discussions.

This paper focuses on partnerships between international organisations (predominantly INGOs from the North) and local organisations in the South. While trying to take into account the perspectives of local partners, the paper is written from the viewpoint

Fig 1: Interview participants by category

of international agencies, with examples tending to gravitate around Afghanistan and Pakistan. Understanding responsibilities, needs and practices from the perspective of local partners, although essential, was beyond its scope. Further research would significantly complement this paper, or perhaps challenge it.

For the purposes of manageability, neither government nor private 'partnerships' were included, although they would no doubt have added valuable perspectives. The same can be said of the work being undertaken by the Red Cross/Crescent movement with national societies. Some references to partnerships between UN agencies and local organisations are included, but these are limited.

Chapter 2 gives an outline of the legal context for working with local partners. However, it is not a comprehensive legal overview and is not intended to provide legal advice. Readers should seek specific legal advice before taking any action with respect to the matters discussed. A recent policy paper by the Security Management Initiative, *Can you get sued? Legal liability of international humanitarian aid organisations towards their staff*, provides extensive further reading on the topic, although it does not specifically deal with agency liability towards local partners (Kemp and Merkelbach 2011).

It cannot be overstated that this paper is not intended to be a comprehensive or even a representative compendium of all perspectives or initiatives being undertaken. Nor does it claim to provide all the answers. It is a first step in an increasingly important area of aid operations.

1 Partnership context and background

INGOs from the North have long worked with local partners in the South, ranging from local and community-based organisations to governments and private companies. These partnerships have been forged in different ways for different reasons.

This paper defines partnership as an association between two organisations, in this case between an INGO (or other international organisation) and a local organisation.[2] Whereas the word 'partnership' might, in some contexts, imply an equal distribution of power, in the case of partnerships between INGOs and local organisations the power distribution is often de facto disproportionately skewed towards the INGO as this is the party providing the resources, with various conditions of accountability.[3]

For the purpose of this paper, a local partner is defined as a national non-profit organisation (eg, an NGO or community-based organisation). Unless otherwise specified, the partnerships referred to are between INGOs and local partners.

1.1 Unpacking partnerships

Globally, partnership models operate across a spectrum:

- Partner-driven model: where aid projects are essentially led, owned and implemented by the local partner (as the critical decision-maker), with the INGO providing some form of resource support and overall accountability role
- Consultative model: where projects (strategy, process and outcomes), as well as decision-making, are shared and owned by both the local partner and the INGO, although the latter might also support with resources and play an overall accountability role
- Sub-contract model: where the INGO formulates the project, makes decisions and maintains overall accountability for it, while the local partner implements it.[4]

Development organisations most often situate themselves at the partner-driven end of the spectrum and emergency organisations at the sub-contract end. In practice, the divisions are not so clear-cut, with grey areas between the models, as illustrated in Figure 2.

Fig 2: Spectrum of partnership models

Partner-driven model	Consultative driven model	Sub-contract driven model
HIV/AIDS Alliance		
ACT Alliance/ICCO		
CAFOD		
Oxfam GB according to context and need		
Save the Children according to context and need		
	Concern	
	Action Contre la Faim (ACF)	
		UNHCR
		WFP

2 This is not a legal definition of partnership. Many different relationships are termed 'partnerships': there is no shared definition of a 'partnership' per se.
3 Accountability requirements might include reporting demands (financial and narrative), procurement guidelines and project standards.
4 Adapted from: Oxfam International 2010: p.6.

The last decade has seen an increase in such North/South or international/local organisation partnerships within both emergency and development contexts. This reflects a number of different trends:

- an increasing move towards sustainability and local ownership of programmes where the strengthening of civil society is a specific organisational purpose
- a growing requirement to increase scale and population coverage in the aftermath of emergencies such as the Haiti earthquake and Pakistan floods, which have made partnerships with local organisations essential
- a documented upsurge in insecurity (see below), particularly in acute and chronic emergency settings leading to increasing difficulties in maintaining and /or increasing access to vulnerable populations. Consequently, due to remote management practices, risk transfer often occurs to local partners that continue to have, or are perceived to have, safer access.

1.2 Risk transfer due to changing security dynamics

Data from the Aid Worker Security Database confirms a pattern of an upsurge in insecurity. Data from 1997 to 2010 indicate an overall increase in violence against aid workers, although the latest years have noticed a slight downturn (Stoddard et al 2011a; Van Brabant 2012: 16-17). This downturn is predominantly attributed to a diminished aid presence in extremely insecure environments such as south-central Somalia and Darfur, Sudan, partly due to reduced access (Stoddard et al 2011a). It is not clear if this relative reduction is a permanent one. Nor is this reduction evident in some of the other higher risk contexts such as Afghanistan. The latest Aid Worker Security Report (2011) also notes that the overwhelming majority of recorded incidents affected national aid workers although, per capita, international staff are facing higher rates of attack. The report suggests that statistical evidence does not accurately capture many of the incidents that local partners encounter.

In line with changing security conditions in many operational contexts, the last two decades have witnessed a significant shift in the approach adopted by most international agencies, both development and humanitarian, towards security risk management. As a result of greater insecurity and limited access, many organisations are practising what is known as 'remote management', relying increasingly on local partner organisations for the implementation of programmes. This leads to risk transfer when an organisation 'consciously seeks someone else to carry out certain activities in a highly insecure context' (GPR8 2010: 21).

The increased reliance on local partners, and subsequent concerns about risk transfer from the international to the local NGO, raise questions about the legal and moral responsibility of international organisations towards local partners (Stoddard et al 2011a: 16 and Finucane 2011: 7). What are the roles and responsibilities of INGOs towards developing the capacity of partner organisations to manage security? To understand this, INGOs have to recognise differing risk profiles of partners and differing capacities to manage that risk.

The nature of threats

Across the board, aid workers are subject to a wide range of threats including:

- Crime: street robberies/mugging, armed raids, car-jacking, road banditry, kidnap for ransom/ express kidnap
- Terror attacks: roadside improvised explosive devices, car/truck bombs, suicide bombers, bombings or gun attacks in public places, grenade attacks on compounds, abduction and kidnapping
- Combatant/armed activity: shelling, crossfire, landmines (GPR8 2010: 40-41).

Organisations may be targeted for political or economic motives, or they can be accidentally affected due to armed activity in the operating context (ie, they are simply in the wrong place at the wrong time). The threats to individuals and programme operations range from less critical incidents, such as street robbery, to highly disruptive incidents, such as kidnapping. To gain a better understanding of the various risks and potential consequences, the programme assessment therefore needs to include a full risk analysis, including an assessment of: threats and vulnerability, probability and the potential impact of specific risks in a particular context, as well as considering programme criticality and possible mitigation measures.[5]

5 Mitigation measures might include dialogue and communications to improve community acceptance of and support for projects, varying routes and times for travel to reduce exposure (protection), or the use of armed guards – usually as a last resort for most agencies (deterrence).

Categorising contexts

This paper differentiates between contexts that are extremely insecure or highly insecure.

The vast majority of documented attacks have taken place in Afghanistan, followed by Sudan, Somalia and Pakistan. Each of these contexts has seen an increase in aid workers being targeted for their perceived association with Western military and political agendas. In Afghanistan and Pakistan in particular, kidnappings and the use of explosives have been on the rise. Contexts like these can be said to be 'extremely insecure' contexts.

They can be compared with 'highly insecure' contexts such as Sri Lanka, Democratic Republic of Congo, Haiti, the West Bank and Gaza, Chad and Uganda, where risks are high but may be based more on economic threat or tangential armed activity, as opposed to politically motivated threats. The targeted use of extreme tactics such as kidnapping or explosives against aid workers is also less likely (Stoddard et al 2011a: 3-7).

1.3 Differing partner risk profiles and needs

The notion that local staff and/or partner organisations are less at risk than international staff and organisations is gradually being replaced by the concept of 'differing risk profiles', and differing capacities to manage that risk. Generally speaking, the risk of encountering a particular threat depends on both:

- **External contextual factors:** the type of threats present in a particular context and the organisational understanding of this and
- **Internal organisational factors:** determining the organisation's profile (vulnerability to particular types of threat and security management procedures and mitigation measures in place).

Local staff and partners may be exposed to different risks from international staff, or may be more exposed to specific risks, depending on various internal and external factors.

Organisational risk profiles are affected by characteristics such as:

- identity and image (actual and perceived)
- value of assets and facilities
- affiliation –such as association with particular ethnic, faith or politically-based groups
- staff composition – ethnicity, gender, nationality
- type of project – agencies reported that food distributions and protection/advocacy projects were particularly vulnerable to the risk of violence (see Box 1).

External perceptions of image and affiliation, etc, are known to be more important than the perceptions found within an organisation itself.

There are a number of additional factors that can expose local partners to higher risk:

- They may be less able to resist pressure from local actors (eg, pressure to hire family members or to fulfil requests made by powerful individuals).
- Constant exposure to danger may make them more prone to perceive risks as part of their 'normality' and less able to objectively assess their level of risk (known as 'danger habituation').
- Fear of losing funding from the international partner may result in risk-taking behaviour.

Based on their risk profiles, partners need to calculate the residual risk that will remain once measures to manage and mitigate that risk are undertaken. Partners will also need to determine the threshold of risk that is organisationally acceptable, ie: the point beyond which an organisation might consider the risk too high to continue operating directly or at all. Thresholds may vary depending on the criticality of the programme.

Local partners, however, may have less opportunity to develop and appropriately adapt the kind of security management skills increasingly supported in international organisations (GPR8 2010: 114 and Stoddard et al 2011a: 9-11).

The next chapter looks at the main definitions in the partnership context and goes on to assess the differing degrees of responsibility that might exist between international organisations and their local partners.

Box 1: Food distribution and protection/advocacy project risks

Food distributions run the risk of corruption, as well as violence and threats over the targeting and distribution process. During the 2010 floods in Pakistan, World Food Programme (WFP) helicopters were pulled down and attacked. In Haiti violence regularly broke out around food distribution points soon after the 2010 earthquake.

Protection and advocacy programmes may highlight not only the shortcomings but also the active abuse and violence committed by those in power – particularly sensitive with authoritarian states. In Darfur, Sudan, organisations as a whole, as well as specific personnel, have been expelled and/or arrested due to the publication of reports or 'perceptions' of their connection with human rights instruments such as the International Criminal Court. Similar issues have been experienced in Ethiopia in relation to the Somali regional State, where organisations have seen their access diminish following advocacy initiatives on behalf of populations in need.

2 Responsibilities for partner security

Disclaimer: This chapter should not replace or supplement the provision of specific legal advice to individual non-profit organisations with respect to their liabilities and obligations. This paper should not be relied upon for specific legal advice by any non-profit organisation or other third party. EISF and the author shall not be liable to such persons.

2.1 Legal responsibilities

As international organisations rely increasingly on local partners to implement programmes, questions have arisen regarding the responsibility of international organisations towards their local partners.

This chapter discusses the distribution of legal responsibilities, ie, what is the 'duty of care' towards local partners in case of security risks. Very little information on the legal treatment of responsibility for partner security is currently available. This paper provides some insight into principles that may be relevant. However organisations are advised to seek specific legal advice. Section 2.2 explores the concept of ethical responsibility in more depth.

The opening position when considering the legal position is that activities of local organisations will be governed by national laws. Additional considerations may become relevant when the local organisation enters into partnership with an INGO.

2.1.1 Partnership

It should be noted that the term 'partnership' has a very specific definition in law which is fundamentally different in nature from what is often termed a 'partnership' between an INGO and local NGO. This relationship would usually be considered a 'sub-contract' in legal terms, under which the INGO pays the local NGO for provision of specific services. The operational nature of such a sub-contract or 'partnership' relationship will include consideration of factors such as the degree of control one party exercises with regard to the other or the level of disclosure of information to each party before entering the partnership. If the actual nature of the interaction is deemed to be one of inequality, dependence, or greater proximity, it is more likely that legal responsibility will have passed from one party to the other.

Based on the sub-contract relationship, there are three causes for possible legal action brought by a partner and/or its staff:

1. breach of the agreement by either the INGO or the local partner
2. personal injury brought about by external parties (armed groups, beneficiaries, etc) against staff of the local partner
3. compensation claims by programme beneficiaries towards the local partner (eg, because of wrongly delivered services, harm caused by service delivery etc).

The key concern of this paper is personal injury to staff of the local partner (ie, point 2), but organisations may also find it helpful to consider potential claims by programme beneficiaries as this might arise as an issue in the future (ie, point 3). What should be noted is that, unlike the classic employee-employer relationship, there is not a bi-lateral relationship but a triangular one between the staff member of the local partner, the local partner as an employer and the INGO as an employer/contractor of the local organisation.

In certain instances, where staff of a local partner are affected by a security incident, the INGO may become directly exposed because it will have (or will be perceived to have) the greatest resources for compensation for the claimants.

The fact that an INGO has subcontracted a local NGO to implement projects does not per se absolve the INGO

of any responsibility. In principle, you cannot exclude liability towards staff, even of the sub-contracted party. A court may find shared liability at least.

Actual legal responsibility will be determined on a case-by-case basis dependent on the contractual terms, the nature of the relationship, and responsibilities arising from national or regional law.

2.1.2 Scope of responsibilities

As noted by Kemp and Merkelbach (2011), in the context of an employer-employee relationship, responsibility is clear: 'generally speaking, employees are owed the highest level of responsibility as they have reduced capacity to act voluntarily and employers are in a better position to understand and control risks'.

As for staff who are not directly employed but contracted, this responsibility is reduced proportionally depending on factors such as the degree of control the non-employee has over their work environment, execution of tasks and access to information about prospective risks (ibid: 21).

Duty of care

Duty of care is the legal obligation to 'adhere to a standard of reasonable care while performing acts (or omissions) that present a reasonably foreseeable risk of harm to others' (ibid: 20).

Duty of care exists for both the local partner and the INGO. The local partner has direct control over its activities, which may cause loss or damage. The INGO shares responsibility based on knowledge of the activities performed by the local partner, knowledge of appropriate risk management procedures, its resources, and general oversight. This is particularly the case when transferring risk.

2.1.3 Limiting the scope of responsibility

INGOs may seek to include a clause in contracts agreeing a waiver of legal recourse. However, this may not stand up in court. If there is an element of risk transfer from the INGO to the local partner, courts might consider whether appropriate risk management strategies have been applied. For example, what were the foreseeable risks and appropriate and reasonable mitigating measures that should have been implemented? How does the relationship between the INGO and local NGO affect the risk profile of the local partner, and is that foreseeable (eg, could deliberate targeting of perceived Western interests be anticipated)?

The terms of the partnership agreement may clearly state the distribution of responsibility for security management between the partners, although few partnership agreements appear to have specific and formal provisions for security management or support, even where partner evaluations prior to the agreement have assessed security management needs.[6]

The INGO must be seen to continue to take reasonable steps to manage risk, even if it has taken on a sub-contractor. If local NGOs are carrying out work in the name of the INGO, the INGO also has an ethical responsibility to that partner (see Section 2.2).

There are only a few examples where either global security management policy has been defined or roles and responsibilities for security management and practical security support have been considered in a partnership agreement. Below are examples of steps that have been taken by two organisations:

- **Example 1** HIV/AIDS Alliance: a Memorandum of Understanding (MoU) is signed with all partners (on an optional basis, except in defined high-risk settings where it is compulsory). The MoU sets out key standards, principles and frameworks, minimum core standards and party responsibilities and expectations with respect to security management. The MoU facilitates monitoring of compliance (although this remains a challenge) and an understanding of where to focus capacity-development support, including in relation to security management.
- **Example 2** Oxfam GB: Oxfam GB specifically states in its Letter of Agreement with partners that the partner will be responsible for providing a safe and secure environment for its staff and that the partner will take appropriate measures to do so, ensuring that security, health and safety are a high priority and managed effectively. The Good Partnership Conversation, part of Oxfam GB's best practice, will then establish any (voluntary) support that the organisation might provide to partners.

The limited provision for security issues in partnership agreements may, in part, be due to the immediate and potential financial costs of any agreement to provide support in respect of a partner's security. This may be compounded by limited information and understanding

6 A recent report states that INGOs increasingly include a policy position in their security policies stating that implementing partners are responsible for their own safety and security management (Finucane 2011: 7). It should be added that this might not be sufficient to exclude liability, depending on the applicable legal system and nature of the relationship.

in the aid sector about potential legal liabilities relating to partner security (Stoddard et al 2011a: 13 and Kemp and Merkelbach 2011: 13), as well as the lack of understanding about security and risk management by the people involved in drawing up partner agreements.

The question arises as to whether or not a local partner can argue that an INGO's decision to reduce or restrict funding has caused damage in case of an incident. Courts will look at what would have been reasonable measures, with one consideration being financial. For example, in a specific context the UN Department of Safety and Security (UNDSS) deemed that there was not a significant risk of roadside improvised explosive devices (IEDs) and, as a result, it was not common practice among INGOs to provide armoured vehicles or financial support for this to their local partners. A subsequent explosion caused damage to staff of a local partner that might otherwise have been reduced had an armoured vehicle been used. The court would be likely to find that armoured vehicles were not a reasonable mitigating measure in that context at that particular time.

2.1.4 Liabilities imposed by national/regional law

As highlighted in section 2.1.3, partnership agreements may incorporate provisions seeking to limit or exclude the liability of one partner to the other in relation to security issues. The treatment of such clauses in law will also depend upon the applicable national or regional legal system, which may hold such clauses to be ineffective. For example, English Law does not permit the exclusion of liability for death or personal injury caused by negligence.

Which legal system applies to determine liability?

It is important to identify which legal system applies, because different legal systems will treat the question of legal responsibility in different ways. In a context in which partners of different nationalities are involved, the jurisdiction, or legal authority to hear a case, may be derived from the nationality or residence of the parties, place of injury, or place of registration of the international organisation. Regional law may also be relevant to determine responsibility (eg, in Europe, European Union regulations apply). Jurisdiction can be specified in the contract, however such clauses may not be enforceable in court.

How to assess liability?

Once these considerations have been addressed, if it is shown that responsibility has passed from one partner to the other, liability would usually be determined according to applicable national laws. In common law legal systems (eg, in the UK and certain states in the US), liability will generally be determined under the concept of 'duty of care', although there may be specific health and safety laws that apply. In civil law systems (eg, France), they tend to use a concept known as 'strict liability'.

'Duty of care' refers to the legal obligation to 'adhere to a standard of reasonable care while performing acts (or omissions) that present a reasonably foreseeable risk of harm to others' (Kemp and Merkelbach 2011: 20). This requires proof of fault. However, 'strict liability' attributes responsibility without consideration of fault – there is no need to show intent or negligence, only loss or harm. This is a much higher standard of responsibility.

Box 2: Duty of care under English law – an example

Under English law, for a duty of care to exist, any damage suffered must have been foreseeable, there must be a sufficiently proximate relationship between the parties and it must be 'fair, just and reasonable' for the court to impose a duty of care. 'Individuals and organisations have legal obligations to act towards others and the public in a prudent and cautious manner to avoid the risk of reasonably foreseeable injury to others' (Claus 2010: 8-9 and Klamp 2007: 2-3)

Liability may exist where an organisation is considered negligent in failing to meet the standards of care that a reasonable and prudent organisation under similar circumstances would be expected to exercise – so adding an element of 'community standard'. What other similar organisations in the same sector are doing may influence the court's view of whether measures taken between partners to partnership agreements were adequate and reasonable (Klamp 2007: 2-3).

For a 'duty of care' to exist between partners to a partnership agreement in relation to security issues under English law, it is likely that the relationship would have to be sufficiently close, such that one partner is providing some sort of service relating to security or security management to the other, or one partner has assumed some sort of responsibility in respect to the other's security or security management.

It should be noted that the consequences of legal liability due to breach of a partnership agreement or duty of care in respect to security issues could potentially be damaging, both financially and in terms of reputation as well as any knock-on effects on staff motivation and organisational funding.

Box 3: A note on UN immunity

An examination of the potential liability (both under a partnership agreement and in respect of duty of care) owed by the UN and its constituent agencies towards partners is a complex subject beyond the scope of this paper. However, it is worth noting that the UN and its constituent agencies generally have immunity from national laws. This immunity may emanate from national laws or the international laws which govern UN agencies. In contrast, INGOs would typically enjoy no such immunity – they are subject to the national law of the jurisdictions in which they operate, and those in which they are registered, as well as to international law – with all the differences in terms of legal system application and enforcement that this may entail (Kemp and Merkelbach 2011: 58).

2.2 Ethical responsibilities

A number of discussions have centred on agencies having a 'moral obligation' towards their local partner.[7] However, the concept of a 'moral obligation' is quite subjective and open-ended, being dependent upon the person expressing it.

This paper therefore focuses on the notion of ethical responsibility and ethical principles.[8] Most development and humanitarian work is governed by an ethical vision and an ethical strategy to fight poverty and injustice or to save lives and alleviate suffering by following humanitarian principles. In this sense, activities of an aid organisation are governed by standards of behaviour that are judged to be right or that uphold a particular moral standard. Similar concepts can be applied when defining an ethical relationship or partnership.

Taking some of these ethical concerns into account, a number of organisations have developed guidelines to support their partners in security management:

- **Action Contre la Faim (ACF) and Oxfam GB** have guiding principles and relatively comprehensive handbooks on how to work with their partners. Specific provisions for security management support are being planned. Although voluntary, these form part of their good practice standards.

7 See for example Finucane 2011. In his paper, limitations of the concept of 'moral obligation' are also put forward.
8 Based on information from the Santa Clara University and the UK Clinical Ethics Network

- **The UN's Inter-Agency Standing Committee (IASC) Saving Lives Together (SLT)** platform provides a framework for UN and NGO security collaboration with recommendations in areas such as: collaborating and consulting in security training; information and resource sharing based on 'best practices'; the integration of security concerns into the Consolidated Appeals Process (CAP) for funding; and adherence to Common Humanitarian Ground-Rules (UN IASC 2011). Currently, there is little consistency on including security in the CAP and many NGOs have reservations about a greater inclusion of security in UN funding appeals in case donors see the UN as a 'one-stop shop' for security and subsequently limit what is available for security requirements specific to a particular organisation.

  Established by the IASC in 2006, and endorsed by the UN, the revised 2010 SLT recommendations remain patchy in their application and reach. There is limited understanding and awareness of them even within the defined humanitarian contexts to which they apply and, although not excluded as such (this depends on the position of the host government and the attitude of the UN and INGOs present), local NGOs are rarely sufficiently included (Christian Aid 2010: 4 and Stoddard et al 2011a).

  That being said, the WFP, for example, established a Policy and Training Unit in 2009 within which initiatives under SLT were to be reviewed to facilitate better integration and cooperation with partners on security and safety matters (WFP 2010: 13).

- **UNHCR** has an internal security policy that looks at the responsibilities arising from any risk transfer to partners and ways to assist partners (international and local) to be as safe as possible. In this, UNHCR may also inform partner NGOs about their security guidelines and encourage their adoption as a matter of prudence (and to the extent permissible by mandate and capacity) while keeping in mind that each NGO is responsible for its own safety and security (UNHCR 2007: 8).

  The security policy looks at a spectrum of opportunities from the low cost to the higher cost possibilities. It includes communication, information-sharing (including invitation to briefings and trainings), advocacy to Governments for communication frequencies, the loan or provision of equipment to partners and evacuation where relevant and possible.

- **The International Red Cross and Red Crescent Movement** has a framework to support safer access for National Societies, which looks at the application of fundamental humanitarian principles in practice, as well as training in and resources for security management.

These examples notwithstanding, the question of what an ethical standard should be based on and how it should subsequently be applied, still remains. Ethical responsibility clearly becomes more important the greater the deterioration in security conditions and the greater the programming responsibilities assumed by the partner as a result. At the same time, the more important the project or programme objective, the more risk an organisation is likely to take.

Unpacking agency references to their 'moral obligation' resulted in a variety of reasons being given for agencies to support local partners in developing their capacities for security management. Some of these are ethical; others are more pragmatic. They include:

- **Association:** the relationship between a local partner and an international organisation can in itself engender a risk for the local partner of being perceived as part of a particular, often Western, agenda. This is the case in the extremely insecure contexts of Afghanistan, Pakistan, Somalia and Iraq. Association can lead to the perception that the partner is wealthier than it really is. Association can also influence perception in the other direction, eg, the security and vulnerability of the international organisation can be affected by perceptions about a local partner and its behaviour.

- **Risk sharing/transfer:** with international organisations increasingly choosing to work with or through local partners in insecure contexts, local partners take on elements of the risks to which the international organisation would have otherwise been exposed. The nature and degree of risk will depend on the local partner's profile as well as that of the INGO, which of course changes over time due to changes in the context or changes in decision-making and resource management responsibilities.

- **Programme accountability:** to ensure effectiveness, impact, coverage, sustainability and so on. This demands a responsible use of resources as loss of assets or injury to a staff member reduce operational capacity and can lead to project suspension or closure. In addition, the assets lost could end up fuelling pre-existing violence, by being absorbed into a war economy, for instance.
- **Organisational vision and remit:** for some organisations the development of local community and association capacities is either an objective in itself or integral to shared commitments to achieve common objectives.
- **Protection of the agency:** support to local partners to reduce risks and minimise any potential negative domino security effect on the international organisation itself, other organisations or the wider community.

With the above considerations in mind, a number of key ethical principles can be extrapolated and subsequently strengthened by drawing upon studies in ethics. These can be used by aid organisations to assess their security responsibilities towards their partners. Some of these principles are specific to security management. Some go beyond this to more general programme implementation as affected by security concerns.

The debate continues as to the limits of responsibility and subsequent engagement: how far should international organisations go towards ensuring that partners have the right terms and conditions, staff and equipment, knowledge and (adapted) systems to implement the relevant project/programme? These limits will vary according to organisational vision and objectives, as well as the nature of the programme and context, i.e. they will depend upon the contours of each organisation's response to the above ethically-informed questions.

With this in mind, a framework for ethical decision-making has been drawn up to support security management of residual risk (see Figure 3). This can be helpful to ensure the ethical quality of any decisions related to security management of those risks which remain after all internal and external factors are taken into account (known as 'residual risk'). The framework attempts to take into consideration both humanitarian and development values, as well as the question of whether or not the partnership has changed the partner's risk profile and threshold of risk acceptance.

Box 4: Ethical principles for partners to assess security responsibilities

Criticality: how critical is the programme?
The importance of this question grows in relation to the level of risk. Does the programme warrant accepting a greater level of risk or a greater allocation of resources to mitigate those risks? Humanitarian INGOs seeking to save lives and alleviate suffering are more likely to accept a higher level of risk, particularly in rapid onset and/or acute conflict situations.

Do no harm: what harm might ensue from a security incident? Harm from a security incident could have a physical, financial, reputational, psychological or programmatic impact. An incident can affect the beneficiaries, the partner itself and related INGO staff, other organisations or people. The level of 'harm' will be affected by the nature of a particular risk, as well as its potential impact. Harm may be balanced out by the potential for 'good' and/or it may be mitigated with support. This in turn may depend upon relative priorities and damage: for example, how critical will capacity development be in the short term as opposed to implementation of life saving activities?

Autonomy: has the partner provided free and informed consent to the level of security risk?
The partner should be aware of the risks undertaken. Knowledge of the level of risk, together with formal and voluntary acceptance of these risks is required. Assessing this can include consideration of the following points:

- Was the local organisation present in an area before starting to work with the international organisation?
- Would the partner have been exposed to the same risks without engaging in the partnership?
- Are there any additional risks associated with working with an INGO or other international organisation; does the partner understand the risk perspective of the INGO and how this may differ from their own?
- Is the partner fully aware of the same security information as the INGO (eg, the INGO may have additional information at another level)?

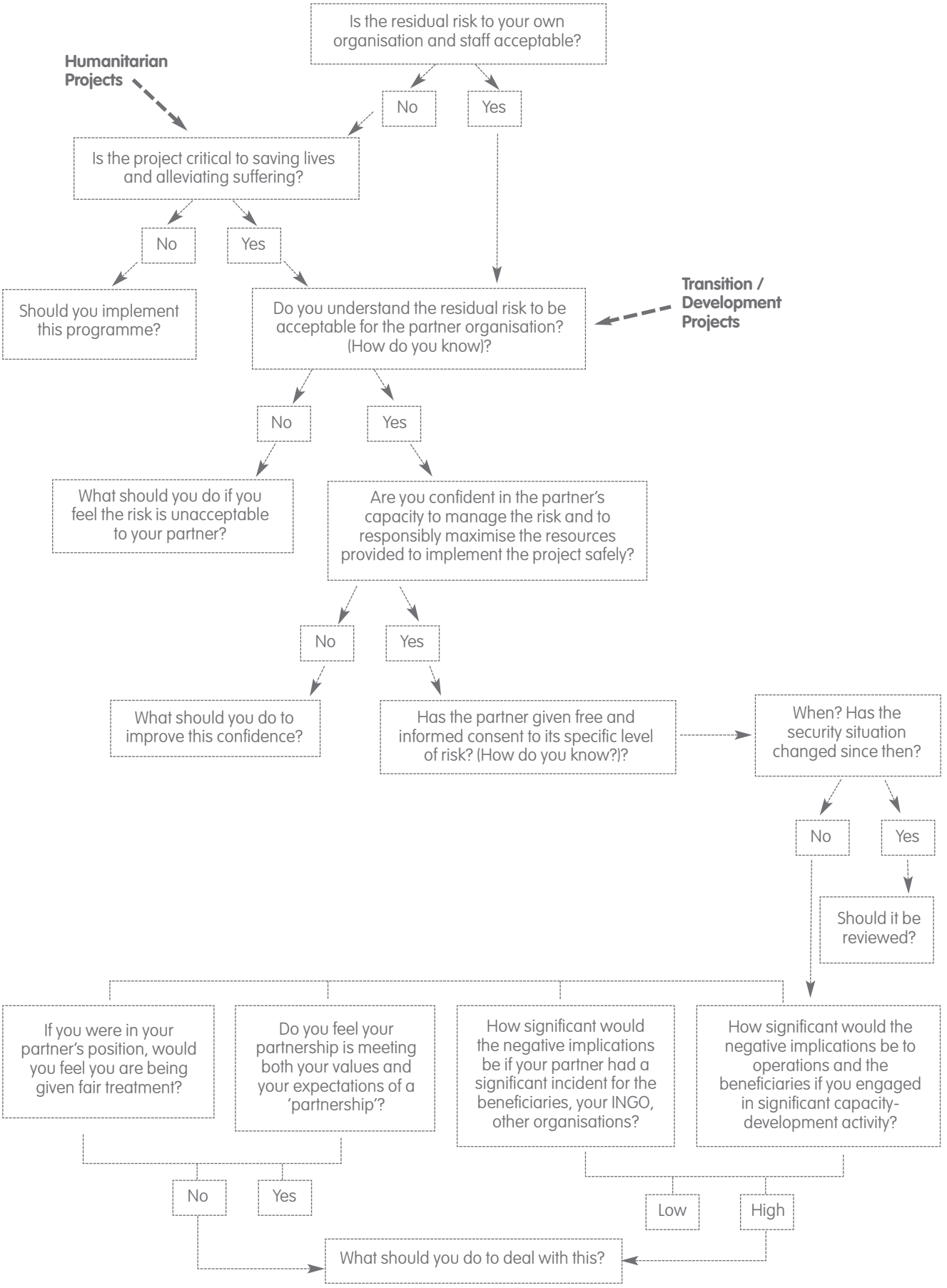
Addressing the question of 'autonomy' involves examining any power imbalances in the relationship between the international and local partner.

Custodial: how accountable and responsible is our use of resources? This principle looks more generally at programme management, with security being a critical component. Programmatic decisions should maximise available resources, skills and knowledge in order to benefit populations in need. Behaving in a trustworthy and responsible manner is an integral component of this. In this sense, there is a balance to be made between managing risk safely, responsibly and accountably versus using project resources in a similar manner.

Justice: are we treating others fairly? This principle is about fairness or equity in the distribution of benefits, risks and costs of an activity/project. Are we being fair in asking the partner to accept a certain level of risk, and in providing (or not providing) capacity development support or financial resources to enable them to do this?

Fidelity: are we being faithful to institutional and professional vision and roles? This relates to the nature and objectives of the partnership and whether or not the trust, responsibilities and expectations from that partnership are being respected. Organisations with a specific objective to develop the capacities of their partners would have a greater responsibility with regards to security capacity development than others without that objective.

Fig 3: Framework for ethical decision-making



The practice of partner support

International organisations often engage with, and support their partners in, security management at field level. Yet formal principles, tools and legal frameworks for guiding partner support in security management are limited.

There are four key areas of support:

- development of organisational security policies, strategies and practice (e.g. security culture)
- knowledge transfer and capacity development
- continuous communication and information exchange
- provision of physical resources, for example, communication equipment, medical kits, etc.

Support can be provided throughout the project-management cycle and during crisis situations as illustrated by the practical cases in the remainder of this section.

Current practices of partner support appear affected by:

- **The model of partnership, the relationship** between the two organisations, and the sense of responsibility derived from this. Where two or more international organisations are working with the same local partner – either in different geographical areas and/or on distinct projects in the same area – questions of coordination and lead can arise.
- **Organisational country priorities:** In extremely insecure contexts, organisations are more likely to support local partners' security management due to wider country-specific and/or global organisational priorities.
- **The nature and timescale of specific partner projects and corresponding objectives:** In humanitarian crises, the focus will often be on an emergency response: scaling up and saving lives, as opposed to capacity development. Existing partners might be disempowered following (temporary) reversal of organisational priorities, while new partnerships might be established under short-term sub-contracting models.
- **The availability of human and financial resources:** This is dependent on local and international organisational willingness to support a security culture and contingent structures, systems and funding, including donor relations. A challenge might also be posed by relationships within an organisation, between different teams with differing priorities (eg, between staff responsible for security and operational/programme staff).
- **Access and whether or not visits by non-local staff are possible** according to the international organisation's security policies and protocols. In many instances the international organisation will have a presence in-country, but might still be remotely located from the local partner. In some instances the international organisation might not have a presence in-country. These factors can all affect the international organisation's awareness of the situation and sense of urgency around security support.

A number of international organisations are working on capacity development of local partners regarding security. In some instances agency practices are guided by formal policy, while in others it is developed on a country-by-country basis, not always with a common or systematic approach. The remainder of this section discusses a number of examples of partner support taking the project and risk management cycles as a starting point.[9]

9 Given the relatively limited analysis of the effectiveness of these examples, they have not been described as examples of 'best' or 'good' practice. Also, while different operating contexts have been taken into consideration in this paper, the organisations consulted often shared examples from Afghanistan and Pakistan, thus limiting the number of examples obtained from other areas.

Box 5: A note on development/ humanitarian organisational differences

In extremely insecure environments a number of (humanitarian and dual-remit) INGOs often have specific security officers/advisers in country to support security management. These positions can be full-time security officers, but the role can also be incorporated into a post with more general management/operational responsibilities.

Where full-time in-country security officers/ advisers are present, there is more in-house capacity to dedicate time and resources to partner capacity development (either systematically or on an ad-hoc basis).[10] The question then becomes one of prioritisation between the INGO's own needs and those of its partner(s). In countries where no specific and separate security position exists, the question of competing priorities and needs will be all the more salient.

Development organisations following the partner-driven model are more likely to look towards head-office security officers as resource persons for partners, and may not have offices in country. Given that head-office security officers also tend to cover a large number of countries, they need to prioritise the intensity of any engagement. In most cases, face-to-face trainings, capacity-development and use of training providers on a consistent and systematic basis are simply not possible due to a lack of resources. Direct interaction for all countries is therefore unsustainable.

An alternative approach is being developed by ACT Alliance and others. They are discussing the potential for regional technical support hubs/regional emergency officers to support security, whether on a consultancy basis or otherwise. This structure would increase their capacity, although it might still involve remote support, particularly in less insecure countries.

3.1 Project start-up

The decision to work with local partners starts with the programme or project strategy, design and structure. These all influence population coverage, activities, outreach and movements –factors that subsequently influence risk exposure. When the decision to engage with a local partner is taken, the project start-up phase contains two components: assessing partner capacity in terms of security management (within overall project management) and risk analysis for both organisations within the partnership.

Partner assessment

The decision to work with a particular partner is made before the operational response (ie, in the planning phase) or during an operational response when there is a need to adjust the manner of response due to a change in security, to secure better sustainability, or as a result of a political requirement. The partner selection process is often conducted as part of a standard organisational process, which is used to identify appropriate and potential partners.

Most organisations use partner assessments to formally evaluate a potential partner's values, structures, systems and capacities across all sectors. Increasingly, there is a focus on security (either integrated or as a separate component). This part of the assessment may be conducted by the INGO's security or programme personnel or, particularly within development programmes, by the partner itself.

While very rarely a deal breaker in itself, since a potential partnership is usually subject to wider programming priorities, the security assessment sets the tone in terms of the partner's strengths and weaknesses regarding security management and any relevant support that might be necessary. The principal challenge arises in terms of availability of resources and feasibility of capacity development, which is particularly the case within rapid onset disaster contexts.

During this phase the potential implications of a partner's image and relationships should also be assessed (whether perceived or real, and to what extent they might impact on the international organisation's image, reputation and security).

10 This is not to deny the contingent questions around security management ownership and line management capacity and what is most effective.

Examples: Project start-up phase

1. ACT Alliance, with support from the Centre for Safety and Development (CSD), ranks partner capacity in security management according to different levels: poor, fragile, basic, advanced, and professional. During the ranking they take into account specific criteria such as: security policy, crisis management, resources, security plans, training, briefings, responsibilities, attitudes, reporting, information-sharing, and analysis and programme integration.[11] A simple diagram helps to visualise the ranking. The tool was developed in Afghanistan with a small number of key indicators that can be checked over a very short timeframe. This makes the tool very practical for use in emergency settings. A more in-depth checklist can also be used to gain greater insight where possible (see Annex 1). The tool was first implemented by CSD and is now being taken forward internally by the ACT Alliance.

2. Save the Children in Pakistan has a specific partner security and safety assessment form that looks at security responsibilities and tries to identify gaps in knowledge and the practice of protocols and procedures (eg, the partner's vulnerabilities). The form includes criteria such as: general security, travel security, facility safety and security, information management and internal communication assessment, vulnerability analysis and context analysis. The partner security and safety assessment is undertaken by Save the Children's security team and the process includes follow-up by the same team.

3. The HIV/AIDS Alliance provides its partners with a toolkit (Security Handbook linked to its Security Policy) that includes an adapted version of the CSD/ACT Alliance matrix for rapid self-assessment by the partners themselves. Guidance on the process and use of this matrix are provided to partner security focal points over the telephone and Skype (including a Webex conferencing facility). This can be quite a long process. Only focus/priority countries receive visits from Head Office to troubleshoot and provide assistance with the process of self-assessment. Verification is therefore mainly done by assessing outputs and cross-checking with other information sources. A wider partner accreditation process, of which security is one component, is used as a condition of acceptance within the Alliance. This includes assessment of systems and measures to safeguard staff and assets.[12]

Risk analysis

Most international organisations undertake their own risk analysis at the outset of any project and update this either regularly thereafter and/or following any significant incident. These risk analyses are often aimed at the programme and may not always include organisational security. The depth and quality of these risk analyses also vary widely among organisations. Following the risk analysis, security protocols and plans detailing mitigation measures and procedures are drafted and implemented at country level, and sometimes at project level.

In the same way that a risk analysis is critical for an INGO or other international organisation, it is also critical for the partner. It cannot be assumed that partners have undertaken a risk analysis for their own organisation, whether in relation to working in a new area or within a changed security environment. Providing support mechanisms and/or opportunities for partners will probably be needed to build this capacity and ensure informed consent from the partner.

During this phase, assumptions about the nature and degree of partner acceptance by communities, armed groups and other critical stakeholders (often part of an international organisation's own strategy) can also be reviewed, as well as the way in which the local organisation will be affected by engaging in a partnership with the INGO and vice versa. The local partner's resources and the adequacy of these resources to conduct project activities safely should also be part of the assessment.

11 The HIV/AIDS Alliance has adapted this to include 'safety and security culture' more specifically.
12 For instance: does the organisation have appropriate systems in place to safeguard its staff and assets? Have measures been taken to protect staff and others on the organisation's premises and in the field? Have effective measures been taken to protect the organisation's major assets? Is the organisation able to respond effectively to emergencies at the office and in the field?

Examples: Risk analysis

1. Concern in Pakistan and Afghanistan has offered training for its own staff and invited partners. Training is not tailored to the partner's specific needs, but provides space for them to work on their own specific risk analyses.

2. CAFOD in Afghanistan and South Sudan sent in external and internal expertise to identify threats and risks with partners.

3. HIV/AIDS Alliance security risk assessment is an integral component of the Security Toolkit provided to partners (as mentioned in Box 6).

3.2 Project planning

Following the risk analysis, operational security strategies need to be drafted and resources mobilised as the project or programme begins to take shape. In this phase, three issues are usually pivotal, namely: minimum or prioritised security standards, partner security management structures, and the budgets and resources required for security. Discussions about the overall security strategy and the different measures and mechanisms to be adopted will be critical (depending on the extent of 'control'/influence the INGO has over the local partner). They should include a review of both partners' acceptance and other security strategies, including application of humanitarian principles.

Many organisations share their own security plans and protocols with their local partners, as examples from which to work, or share basic templates. How to ensure that the local partner has an active (rather than only a passive) acceptance strategy needs to be considered, as well as other security strategies they may employ where appropriate (such as protection or deterrence approaches). For example, local organisations may be under pressure to use armed guards, particularly when they have foreign visitors. A 'local gun culture' may mean that the partner does not see the concerns associated with the use of armed guards or armed escorts.

Minimum or prioritised security standards?

International organisations should consider whether or not it makes sense to identify, agree on or encourage core minimum standards that international organisations would like to see applied, particularly in extremely and highly insecure areas. Although this will differ on a case-by-case basis, an obligation to follow certain standards may entail legal obligations for the INGO (as the funding partner).

If standards are applied they will need to be contextually relevant and risk-profile appropriate. This may be an issue when a local partner has several different international organisations as partners as they may well have differing standards. In such situations, coordination between the international organisations is key.

Examples: Security standards

INGOs communicate security standards to their partners in different ways

1. The HIV/AIDS Alliance has 'preferred' standards for partners in defined high-risk countries that fall into four categories:

- **General management:** adequate funding for security measures and management, incorporation of differing vulnerabilities into security planning cycle (gender, HIV/AIDS status), human resource management, security of premises, stress management
- **Security management:** country security plans, guards and weapons, incident reporting, risk assessment, emergency number, security focal points
- **Travel:** briefing, driving, equipment, training, withdrawal
- **Specific security threats and emergencies:** evacuation, kidnap for ransom, office closure

2. The World Food Programme (WFP) generally provides its partners with a manual for the implementation of food distributions. The manual looks at all aspects of the distribution process, with security concerns and standards integrated throughout (WFP 2005).

Partner security management structures

There is a question as to whether or not INGOs should actively involve themselves in their local partners' structures, ie, in the roles and responsibilities that underpin effective security management.

Without considering roles and responsibilities, significant confusion can occur at critical moments, which could, for example, lead to important decisions not being made. Support might therefore entail ensuring or encouraging policy, job descriptions and organograms to ensure that responsibility for security is held by the appropriate level of seniority. These should then reflect security management needs, together with corresponding personnel performance management criteria and potential disciplinary mechanisms.

In parallel, ensuring the presence of partner liaison officers and security focal points for local partners within the INGO can also be important.

Examples: Partners' management structure

1. Oxfam GB in Afghanistan has requested all partners to ensure they have specific, known security focal points with whom to liaise. Oxfam GB also suggests terms of reference for these positions.

2. The Centre for Safety and Development (CSD) has standardised templates available for security structures, governance and job descriptions that have already been used by various rganisations.[13]

Security budgets and resources

Local partners should be encouraged to ensure security management is covered within their programme budgets, including core funds for equipment or material to assist in safety and security management. INGOs should be open to funding such requests when properly justified through risk analysis and development of appropriate mitigation strategies. Choosing whether or not to fund may have legal implications. Partners can also be supported to apply for institutional funds directly or through the international organisation.

It is important that the resources provided are appropriate to the specific context and partner risk profile, and do not raise the level of risk. Examples of sensitive choices that avoid creating an unwanted 'international' profile, for instance, might include: renting vehicles locally rather than importing four-wheel drives, and providing mobile phones rather than high-frequency radios.

Examples: Budgets and resources

1. Oxfam GB in Afghanistan encourages its partners to look at their budgetary needs for risk management so that these can be met from existing funds or incorporated into future proposals.

2. Save the Children in Pakistan shares templates and guidance manuals with their partners. These are used by their own staff to draw up security budgets. The templates and manuals include sections on equipment, training, personnel, facilities, technical support and office/residence safety, along with guidance on how to make budget calculations.

3. The HIV/AIDS Alliance has a tool to link exposure to risk with the security responses necessary and subsequent budget requirements.

4. The UN in Tunisia/Libya incorporated security costs into the Consolidated Appeal Process (CAP) as part of the implementation of Saving Lives Together (SLT). In Somalia, the UN has incorporated a specific budget line for 'enabling programmes'. Similarly, WFP in Pakistan supports security budgets for prioritised locations.

3.3 Project implementation

The INGO's role in supporting security management of its local partner during project implementation will generally take two forms: capacity development and information-sharing. While capacity development for security management should be initiated and conducted during the project planning phase, this is rarely the case. Most often it occurs in parallel with project implementation. Information exchange on security, on the other hand, tends to take place during both the planning and the implementation phases, since it is critical to both project and security management.

13 Online available at OpenSecurityDocs: http://www.opensecuritydocs.org/

Capacity development for security management

The main difference between capacity development for security and capacity development for other areas of programming is that security affects everyone in the organisation. Each individual within an organisation has some level of responsibility regarding security, both individually and organisationally. Each individual needs to understand how to manage security according to their role and responsibilities, and each organisation needs people at the right levels (headquarters and field) who understand security management to ensure its effective implementation.

It is important that local partners realise that security management is essential for effective implementation of programmes and projects and that they do not see it solely as one demand among many INGO/UN demands (such as gender equality, accountability, etc).

Different approaches can be used to support capacity development involving anything from contextual information-sharing, best practice information, and technical advice to specific capacity development schemes. It can done both face-to-face and remotely. Support tends to be based on initial partner assessments and/or subsequent gap analyses, although sometimes it can be done on the basis of assumptions about what might be needed. In order to facilitate effective capacity development a number of organisations have signalled the importance of:

- An enabling environment: a context where the local partner feels it will be supported rather than sanctioned for being open about gaps and potential needs
- A two-way process: to enable effective learning, adaptation to realities, and alignment with the particular strengths of the organisation. Particularly prominent examples of cross-learning have been around negotiation at checkpoints, dealing with crossfire situations, and behaviour during a kidnap.

In terms of approaches to support capacity development the following can be particularly effective:

- Partner training provides an opportunity to promote cooperation and exchange between local organisations, allowing them to establish their own security networks and peer groups that can function without the involvement of an international partner. Pakistan's Water, Environment and Sanitation Society (WESS) is a good example of how training can facilitate internal capacity development. Those employees who have received training are expected to brief their colleagues with the lessons learnt. Building on similar examples, the ACT Alliance is planning to formalise a 'training of trainers approach' and roll it out more widely in high-risk countries, so that trained partner staff can act as a subsequent catalyst or facilitator for others.

Other good practice examples used to build up capacity (although not on security per se), can possibly be applied to strengthening local partners' security management structures.

- Embedding expertise (expatriates or otherwise) into the partner organisation can aid the partner's response and allows for coaching the partner in security management. Similar approaches have been undertaken for general programme management and technical support by CAFOD in Haiti and Oxfam GB in Pakistan. Large organisations such as Save the Children, Oxfam GB and Act Alliance have a small number of security experts within their emergency/humanitarian response personnel who can be posted on short notice for management and capacity-development support to regional and country offices. This has been done in Pakistan, Nigeria, Kenya (Dadaab) and Côte d'Ivoire. While local partner staff may benefit from spill-over, this support could potentially be more strategic and structured.
- Seconding partner staff into the INGO project or programme office for on-the-job security training or shadowing. This approach is useful in extremely insecure situations where no direct access to the project exists for the international organisation (nor international or senior national staff). Oxfam GB did this in Pakistan during the flood response, specifically to build up capacity on managerial and technical expertise (water, sanitation and hygiene education).

Capacity development as a long-term activity

Effective capacity development generally requires significant follow-up and feedback over anything from 12 to 18 months. Even if a security management plan is in place and the employees have received training, it does not necessarily enable them to manage security risks effectively. This entails investing in a process of capacity development as opposed to one-off workshops, which are less likely to maximise support or change. While feasible in chronic emergencies, this may not, however, be possible in rapid onset complex

emergencies unless undertaken proactively. For effective and sustainable security management, senior (director level) staff who have oversight responsibility for security should also be involved at all stages of the process.

Monitoring and evaluation of capacity development

One of the challenges for capacity development lies in measuring its outcomes and impact. It is common for organisations to undertake pre- and post-training tests – not only immediately after the training, but also some months later.

A review of the outcome of capacity development can be done by bringing partners out of inaccessible areas to discuss the evaluation in person. It can also be done remotely, but here you need to rely on additional indicators. Information sources and information exchange mechanisms are used to verify the results.

Box 6: Capacity development undertaken by multiple organisations

Three distinct approaches to capacity development are outlined below, along with examples of organisations using them:

In-house workshops that cover the fundamentals of security management (policies, risk analyses and security strategies, protocols, focal points, behaviour during an incident, crisis management, etc). These tend to take place in the most accessible geographical location and/or where resources may be maximised (eg, partner staff from Pakistan's Baluchistan and KPK provinces go to Islamabad, while South-Central Somali partners may go to Somaliland or Kenya (depending on visas)). Diaspora staff can assist in overcoming problems of direct access.

Both in-house and external consultants can be used to provide tailored trainings that align with the remit, values and principles of the organisation. Some organisations prefer in-house staff for sustainability. Trainings are usually interactive with power-point presentations, role plays, simulations, question and answer sessions, working groups, videos etc.[14]

External courses: partners are encouraged and/or supported to attend courses run by other agencies such as RedR, CSD, and country-specific groups such as ANSO, GANSO and NSP.[15] Although such trainings have less space for the specific organisational remit, vision and activities, they can be useful for partners working with many international agencies and wanting to develop their own in-house skills and adapted systems. They also often take place in the nearest safe and accessible place.

Comprehensive toolkits such as manuals, CDs and on-line resources that provide training modules together with centralised – but remote distance – support and feedback from the head office of the international partner. The Interchurch Organisation for Development Cooperation (ICCO) provides partners with a framework consisting of questions to guide them on the development of their own systems, while the HIV/AIDS Alliance has a structured system with well-developed processes and tools that are reinforced by the provision of support in a phased manner. The HIV/AIDS Alliance also encourages the establishment of peer group support among their partners.

UNDSS has an online security learning centre that is accessible to partners and IFRC has created open-source online training for personal security and security management that is accessible to all.[16]

14 It was noted that bringing partners from different countries together can sometimes work well when faced with common risks (eg: Afghanistan and Pakistan; Ethiopian Somali Regional State and Somalia) or when the organisation is ready to share information and has a certain level of understanding and practice. Courses can, however, be more complicated when staff such as guards and drivers are sub-contracted from private agencies, potentially causing confusion about support, systems and roles.
15 NGO-based security organisations in Afghanistan, Gaza and Somalia.
16 UNDSS accessible at: https://dss.un.org/dssweb/Resources/BasicSecuritybrIntheFieldBSITFII.aspx; IFRC accessible at: https://ifrc.csod.com/client/ifrc/default.aspx

Examples: Capacity development over time

1. Save the Children in Pakistan established that a minimum of 12 months was required for a 'good enough' level of local partner capacity development with a direct, hands-on presence. Other requirements included working closely together with local partners, whereby the INGO is closely involved in risk analysis and subsequent steps taken by the local partner, through consistent coaching and engagement.

2. Security focal points among HIV/AIDS Alliance's partner organisations are mentored by email, Skype and webinars. Monthly progress and security teleconferences take place for each country based on an accessible security management handbook and an e-learning platform hosted by the organisation, with free access for all Alliance Security Network affiliated staff. South-South dialogue/peer groups are encouraged through intranet forums. Distance support is generally provided, although visits may take place for priority countries. Support timelines are individually tailored according to need.

3. ACT Alliance and ICCO in Afghanistan and Pakistan proposed engagement over an 18-month period divided into several distinct phases:

- Phase 1 (months 1–3): selection of the partners it was most critical to work with, followed by development of an appropriate training course for them
- Phase 2 (months 4–5): implementation of a four-day security management course for security focal points and other key programme staff, as well as a one-day workshop for directors to ensure buy-in
- Phase 3 (months 6–7): provision of support to partner organisations to develop their security plans through their security focal points and with the head-office adviser from a distance (telephone calls, Skype, emails, etc)
- Phase 4 (months 8–9): implementation of a two-day follow-up workshop to discuss progress, challenges, strategy and action plans as well as timelines; establishment of a network among participants
- Phase 5 (months 10–18): consolidation and monitoring of previous support with ongoing assistance from a distance and a further two workshops of one to two days each, for follow up.

Proactive, not just reactive, engagement of partners throughout the process is seen as critical.

Examples: Monitoring and evaluation

1. Save the Children in Pakistan conduct an immediate evaluation and follow up with refresher/improvement workshops after six months or so. The same questionnaire is used pre- and post-training, allowing the evaluator to monitor changes. It looks at key elements, including: roles and responsibilities for security; security awareness, interactions with beneficiaries and communities; safety during travel; specific incident behaviour and incident reporting modalities.

2. CSD also supports the use of pre- and post-training tests to identify staff quality and awareness on security policies.

Information exchange for security management

Information is critical to overall project accountability and quality. Moreover, it is key to evaluating security risks and making decisions about the acceptability of risk and appropriate risk mitigation measures. Information exchange and networking/coordination can not only improve the effectiveness of aid delivery, it can also reduce the costs of security risk management for individual organisations.

Both parties can have critical and complementary information, so information exchange should ideally come from both the INGO and the local organisation(s) and be continuous and, where necessary, confidential. Some organisations fail to share information because they do not realise how important it is, while INGOs may forget that local partners are an essential source of information.

Several international forums have been established over the last few years that are aimed at information sharing on security-related issues. Although INGOs and local organisations can greatly benefit from the information shared in these forums, it is essential to understand any related information dissemination policies and protocols related to the specific forum before information is shared.

It should be kept in mind that depending on what is discussed and who is present, participation in a security forum can increase the security risk to all partners – local and international. This is particularly the case in authoritarian and highly polarised violent contexts where suspicion may be rife. In these instances, judgement calls on the viability of local NGO involvement in security forums will be necessary.

Box 7: A note on coordination mechanisms

In a limited number of insecure countries, organisations like NSP (Somalia), ANSO (Afghanistan), GANSO (Gaza), and ISAO (Yemen) provide a range of security services including incident reports, security trends analysis and training.[17] As noted by Stoddard et al (2011b: 13), while these networks are in theory, useful mechanisms for extending coordination and support to national partners, there is not much evidence of it happening in practice.

While the Saving Lives Together (SLT) platform has led to the deployment of a small number of NGO liaison officers by UNDSS in high-risk areas, these are more difficult to access for local NGOs/associations. A reason for lack of engagement has been quoted as a lack of trust by both parties. Mechanisms have yet to be found that are more inclusive of local partners and, in many instances, it falls upon the INGO to channel any benefits of SLT to their local partners.

17 While very useful, concerns do exist that in-house and project-specific contextual analysis can diminish with the arrival of security forums. Moreover, analysis may be useful for managers, but not necessarily for field teams.

Examples: Information sharing

1. Save the Children in Pakistan sends their local partners daily, weekly and monthly security updates to support them in areas where they previously had no access to international coordination mechanisms.

2. CAFOD in South Sudan held a workshop with its partners looking at the different types of information needed (context monitoring, travel safety, security incidents) and how to exchange it according to the situation (SMS texts, HF/VHF, telephone, face-to-face conversations, internet.

In terms of security information, it is important for INGOs and their local partners to:

- verify and ensure the reliability of the information
- undertake information analysis
- contextualise the information
- connect the information to wider patterns and trends.

This is essential in order to inform security decisions. Both local and international organisations have their own information sources and could benefit from support to make better use of them.

Incident reporting and monitoring

Some partners are formally required to inform their international partner of incidents while for others this is not necessarily the case. Incident reporting can be difficult and does not always happen due to:

- differences in the perception of risk
- differences in the understanding of what constitutes an incident
- sensitivities about information use
- lack of understanding of the importance of reporting.

This can hinder both timely support by the international partner and proactive analysis and development of mitigation measures. It is, therefore, important to ensure that there is clarity about what information is needed and when, why and how it will be used, as well as providing tools (existing database, incident reporting forms). Moreover, mutual trust and transparency are essential if information exchange is to be timely and effective.

One INGO that provided assistance on incident reporting is Oxfam GB. They sent a trainer to work with their partners in Afghanistan for two days, focusing in particular on incident reporting and analysis.

3.4 Crisis management

Support to partners for crisis management can be sensitive, particularly in contexts where association with an international organisation can raise the stakes, for example a kidnapping (and the price of release) or an accident (and the compensation to be paid).

It is therefore important that the role of the INGO during a crisis is discussed and agreed on before any crisis (expectation management). This can include discussions about the financial and material support the INGO may be willing to provide (eg, evacuation/relocation services, medical aid) and any implications. The importance of developing contingency plans proactively should also be emphasised to the local partner.

Some agencies report that they offer advice on crisis management to local partners. This is often done remotely, through phone calls or e-mails. Proactive support relating to how to behave in scenarios such as car-jacking and armed robbery was also mentioned.

Examples: Crisis and incident management

1. Concern in Afghanistan and Pakistan has invited local partners to participate in training focused on incident management (checkpoints, crossfire, etc).

2. HIV/AIDS Alliance offers support on crisis management to local partners from its head office crisis management team.

3.5 Project review

Partner assessments are most valuable when they reflect the current context and status of a partner – hence, the need for periodic reviews and audits as part of the project/programme cycle or when a particular incident or change of context occurs.

These periodic reviews should normally assess whether or not security protocols and plans are being followed and what systems are being used by the organisation. It should also include a formal assessment of the security context, staff understanding of risks, any change in risk level, and whether or not the protocols and plans are appropriate to managing those risks. The review should also include the outcome of any capacity development initiatives.

Such a review may well conclude that the local partner and the partnership are effective. Outcomes that point towards a serious deterioration of the security context or lack of partner capacity should lead to a review of the project implementation or to the termination of a particular project.

Reviews can be done by the international organisation with the local partner, or by the partner itself. Where direct access to the local partner is not possible, third-party involvement might be a possibility (eg, verification through security quality assurance teams, key community leaders, and beneficiary feedback).

Example: Project review

HIV/AIDS Alliance reviews its partners once a year through a process that includes partner self-assessment, with security as one component. Requiring a level of trust and triangulation, these assessments feed into the project planning process, identifying training needs and calculating financial needs for the coming year.

3.6 Support areas for local partners

Drawing on wider programme initiatives, the diagram in Figure 4 summarises what has been done, or can be done, to support the development of partner capacities for security. The diagram provides a useful checklist when developing the capacities of a partner in the area of security management.

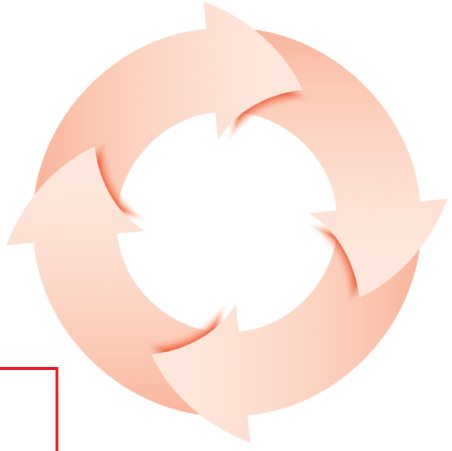
Fig 4: Capacity support cycle for partner's security

Project start-up

- Assessment of partner capacity in security management, or ask partner to do this: review the capacities and vulnerabilities in policy, systems, structures and knowledge; identify areas for further potential support
- Support to partners' risk analysis, taking into account their differing profiles and vulnerabilities

Project review

- Reaction to a major incident directly affecting a partner, prompting dialogue over risks and management
- Review/audit of security management and practices
- Review of relevant support strategy



Project planning and approval

- Support to partner to draft appropriate security plans and protocols through providing examples, advice or specific training courses
- Discussion around the necessity of minimum standards;
- Dialogue over management structures and security focal points: organograms, job descriptions and core competencies; disciplinary processes for breaches of security
- Inclusion of provisions for financing the necessary resources for safe and responsible project implementation; sharing of tools for this

Crisis management

- Provision of trainings on how to behave in security incidents
- Assistance in the development of pro-active contingency plans
- Discussion of the INGO's role when partner is affected by an incident (eg, medical support, evacuation, financial support for relocation)
- Discrete advice where relevant
- Advice from own head-office crisis management team where relevant

Project implementation

- Provision of in-house workshops looking at outputs and processes necessary for proactive and reactive security management and encouragement/support for partners to attend external security courses run by other agencies and country-specific groups
- Encouragement of partners to establish peer groups/networks and to ensure training outputs are disseminated.
- Provision of comprehensive toolkits (hard copies or online resources where internet is accessible) with advisory support where possible
- Potential embedding of expertise into partner organisation for a given period of time to mentor and coach key partner staff around security management or secondment of key partner staff into the international organisation for hands-on training or shadowing
- Monitoring of all capacity development to review nature and duration of support necessary
- Support of timely, appropriate and relevant security information exchange including contextual analysis and incident reporting with training if necessary. Existing tools can be shared.

The challenges of capacity development for local partners

This chapter looks specifically at some of the challenges and questions that arise on both sides of the partnership, locally and internationally. They apply to the different phases of the project and risk management cycles as referred to in Chapter 3.

4.1 Differing perceptions of risk, differing needs

One of the challenges often mentioned is the differing perceptions of risk and thresholds of acceptable risk influenced by each agency's different vulnerabilities and risk profiles. This can either drive or impede engagement.

Local partners often have better (local) networks and better knowledge of the immediate social, political and economic climate than their international partners. At the same time, their constant exposure to danger, and fears of losing funding and jobs (part of the power imbalance), can potentially lead to greater risk-taking.

International partners, on the other hand, might be more influenced by a relatively limited knowledge of the local context. They may be more risk averse due to a greater awareness of major incidents against international agencies globally, uncertainty about local risk-mitigating measures, and concerns regarding legal liability. INGOs often display a lack of understanding of their local partner's vulnerabilities. Clearly, questions of perception and reality can affect both parties in a partnership.

There appears to be a greater degree of consensus about risks among international and local actors in extremely insecure contexts. Where consensus is not possible, dialogue is critical to help overcome these differing perceptions. This can, for example, be done by working on the joint definition of indicators to objectively monitor changes in the level of risk, or by looking at programme impact and discussing appropriate mitigating actions according to the risk analysis together.

For international organisations, it is important to familiarise themselves with the approaches and methodologies of their local partners and adapt to the context and the partner's specific risk profile and needs. An additional challenge arises when a local organisation has to deal with multiple international partners that each have their own perceptions and needs. This will require coordination among the international agencies.

4.2 The importance of a security culture

The presence of an appropriate security culture in both the international and local organisations plays a significant role in determining the level of responsibility, engagement and, ultimately, achievement of any capacity development.

For an international organisation, prioritisation of security management from the Board down to programme and human resource departments appears to make a difference in creating a more systematic and consistent approach to capacity development. Security needs to be embedded in the organisational culture in order to create sustainable structures and systems for themselves as well as to support their partners' security needs.

The development of a security culture is just as important for the local partner. Thus, security responsibilities need to be clearly articulated and led by people with credibility, institutional backing and adequate resources.

For many INGOs, institutionalised security systems are still in development, which further hampers outreach to local partner organisations. As one

respondent aptly observed, "We need the policy and principles before we can have the tools." Findings from a recent paper on legal liability by the Security Management Initiative are instructive in this respect. The paper found that around 30% of international aid organisations interviewed have an institutionalised system of security management and reporting; around 30% had no such system; and another 30% had only just started to introduce security management plans (Kemp and Merkelbach 2011: 10-11).[18] Where agencies have limited institutional awareness and commitment themselves, it will be difficult to support others.

4.3 Resources

As previously mentioned, in order for capacity development to be effective, investment in resources, technical capacity and time are essential. Aid organisations (both international and national) need to be able to quantify their security needs and be transparent and realistic about the funds necessary.[19] Many organisations still feel pressure to keep security costs down in order to maintain the balance between indirect and direct programme costs. Yet in humanitarian emergencies, particularly in extremely/highly insecure contexts, some government donors such as ECHO and OFDA (USAID) are willing to accept budget lines specifically for security as long as they are justifiable. It is important that the INGO/UN inform their local partners of funding rules and the importance of clear and transparent budgeting regarding security.

Concerns have, however, been raised about the consistent application of these donor policies between countries, profit and not-for-profit organisations, and headquarters and field offices.

In practice, where funding comes from UN agencies or donors such as the Global Fund, including budget lines for security can be more difficult since capital costs (radios, vehicles) and overhead costs (communications, head office support) are not accepted in many contexts. The same is true for training.

At the same time, short-term funding timeframes make it difficult to plan for significant and consistent capacity development, even within chronic crises. On the other hand, donors that fund development projects seem more hesitant to budget for security.

What is required is greater donor lobbying and awareness-raising (within the international organisation and towards local partners) on the importance of integrating security into core organisational and programme budgets.[20]

The debate around other security-related issues, such as evacuation and negotiating with kidnappers, is even more complex, with possible far reaching consequences. To what degree should partners be supported, both legally and ethically and in terms of programme costs and security risk management?

4.4 Humanitarian contexts

Partner capacity development is most challenging within emergency settings, in particular in rapid onset and complex emergencies. Ideally, capacity building should take place before a crisis. However in rapid onset emergency contexts, faced with the complexities of working with unknown partners within short timelines, organisations newly entering the area often prefer to implement projects directly, at least in the first phase. In other instances, partner assessments and partner capacity development may be de-prioritised in relation to other more urgent (often life-saving) priorities and efforts to scale-up to increase programme coverage.

There are differing opinions as to what the cost-benefit ratio and impact of greater security capacity development might be to organisational momentum and emergency response in rapid onset emergency settings. Questions that often come up in this respect are:

- In an emergency at what point, if at all, do you support partner capacity development?
- At what point does the balance of priorities between scaling up to save lives and alleviate suffering on the one hand, and establishing the foundations for a transition to recovery and development on the other hand, change and allow space for partner capacity development?

18 That said, around 88% of organisations did allocate human resources to security. Findings are based on interviews with 38 international organisations in 2009. They do not evaluate the actual implementation of any systems or policies.
19 In the US, the existence of charity ratings agencies like Charity Navigator act as a disincentive for US agencies to register programme costs of less than 85-90% of the total. This tends to drive down the funds devoted to security, particularly when not integrated into programme costs per se.
20 The Good Humanitarian Donorship Initiative has recently launched a work-stream on security, which may act as an opportunity in this regard.

- Who should make decisions about the necessity for capacity development: the INGO, the local partner, the authorities and/or the community affected?
- What will be the modalities and parameters of such capacity development?

The answers to these questions will differ according to agency vision, remit and values. In chronic humanitarian situations and countries known to be at risk of rapid onset emergencies, there may be scope for some proactive capacity development by dual remit agencies likely to respond and already present in-country. Save the Children UK for instance, has a Fragile States programme covering 12 countries which aims to develop overall in-house programme capacity to respond to emergencies. Can such a structure be expanded to key partners and their security management?

More recently, dual-remit agencies are increasingly emphasising work on disaster risk reduction (DRR) and resilience. Partner capacity development for security should be part of the preparedness work under DRR

4.5 Questions of Compliance

It could be said that the impact of a potential security incident – whether it results in loss of assets or injury to persons within the partnership or outside – warrants compliance to certain (contextually adapted) procedures and standards. However, setting aside the debate about 'whose' standards (particularly in situations of multiple partnerships), one critical question comes to the fore. If a local partner has a significant security incident, despite following agreed standards, what might be the implications for the legal responsibility of the international organisation? How far does the chain of responsibility stretch? And is there a legal difference when the partner is obliged to follow certain standards or merely is encouraged to do so?

Different partnership models result in different ways of working between the international organisation and the local partner. Within a partner-driven model, the international partner is more likely to facilitate positive changes in security management providing suggestions to their local partner that should find expression through mutual trust and respect.

The HIV/AIDS Alliance reserves the right to expel members from their network for repeated failure to meet minimum standards. It is felt that this demonstrates serious attention to security risks and partner safety.

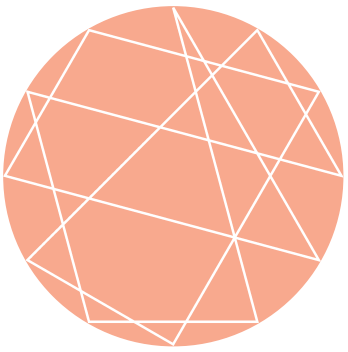
Box 8: A note on faith-based organisations

Management of risk, including security risks, can sometimes be more complicated within faith-based organisations where the dominant religious impulse may be to leave a person's fate to God. Where this is the case, tensions may exist between the dictates of faith and religion on the one hand, and those of organisational policy on the other.

How does the concept of being a faith-based organisation impact on the perception and acceptance of both the international and the local partners)? How might they affect each other's perception and image?

For example, tensions may arise when an organisation feels that security indicators point to evacuation, while an individual believes in the need to stay and trust in faith. Who prevails? Faith-based INGOs may also have less choice about whether or not to work with a certain partner. Irrespective of the INGO's assessment of the local partner, an INGO might still be willing to work with a local organisation if it belongs to the same community of believers. Withdrawal of funding or termination of the partnership (directly or through non-renewal of contracts) may not be an option.

Such tensions require careful negotiation and, in some instances, might require both institutional and individual changes in mindset in order to improve security for both parties.



Conclusion

The objective of this paper was, first, to explore issues related to security and the responsibility of INGOs to support the security of their local partner organisations. Overall, organisations with more partner-driven and development approaches have advanced furthest in supporting partner capacities for security management, although they may not necessarily be working in the most insecure contexts (either the countries themselves or specific areas within a country).

Many of these organisations have developed tools for capacity building, which can be adapted to the security needs of more humanitarian-oriented organisations. Already, some progress has been made within the more extreme/highly insecure settings by both humanitarian and dual-remit organisations. Pakistan and Afghanistan are probably at the 'cutting edge' of much of this progress with other insecure contexts, such as Somalia and Darfur, arguably hampered by the relatively smaller number of international agencies and civil society organisations working there (due to access limitations). It is, however, recognised that within the broader spectrum of assistance activities, agencies could do more to prioritise their partners' security needs and support capacity development on security management.

Secondly, the paper set out to provide insights into the strategies employed by INGOs to provide support to their local partners in terms of security management. Four key areas for support to local partners in terms of security management were identified:

- development of organisational security policies, strategies and practice (eg, security culture)
- knowledge transfer and capacity development
- communication and information exchange
- provision of physical resources.

Mutual trust and respect, together with adaptation of the mechanisms and tools to support and verify security management needs and capacity development, is key. Capacity development should be seen as a 'process' over time, with regular feedback and interaction in order to maximise gains in terms of knowledge and skills development, as well as attitude and behaviour change.

The main challenge will arise during rapid onset disasters and spikes in acute humanitarian situations, unless organisations are able to undertake security management preparedness work with identified partners in advance. This may be possible for some; not for others. Challenges will also arise in terms of the physical resources available and management of expectations around the nature of the partnership and commitments, as well as issues of compliance and the implications, particularly legal, that this may have.

A precondition for any forward movement on the issue of partner capacity development is mutual understanding of risks and prioritisation of security and related capacity development for all partners. The ethical arguments for increased focus on partner capacity development are there, but the primary question remains: to what degree will this be pursued in practice? This question can only be answered by each individual agency according to context.

ANNEX 1

Partner Security Level Assessment Tool (Source: CSD Matrix, developed by the Centre for Safety and Development)

	1. Poor	2. Fragile	3. Basic	4. Advanced	5. Professional
Security Policy	We have not articulated policies and principles	We have some policies and principles on paper	Policy principles and responsibilities are clear and agreed upon	We have a clear and adequate security policy, accessible to everyone	Staff feel involved with security policies, contribute to update them
Crisis Management	There is no crisis plan in place	We have a written crisis plan	Crisis plan is updated regularly	Crisis plan and infrastructure are regularly tested and updated	Meetings are regularly organised to develop specific scenarios
Resources	We have no budget for security	Budget can be made available on request	Budget is available for basic equipment and training	Budget for security is available for all equipment and training	Budget is integrated in all programme budgets
Country/Location Specific Security Plans	We do not have security plans	We have some working procedures on paper	Some working procedures are in place for every country where we have field presence	Security plan for every country and risk assessment for every location, updated regularly	Every member of our staff is familiar with clear and accessible security plan and adheres to it
Security Training	We do not train our staff in security	Some international staff are trained	All international staff are trained on personal level	All staff are trained, managers are trained in security management	All staff are trained on every level and skills are maintained
Security Briefing	Staff are not briefed	Some staff briefed at HQ	All staff are briefed at HQ before departure	All staff are briefed at HQ and upon arrival in field	All staff are briefed before and debriefed after every trip
Responsibility	Staff take no responsibility for their own personal security	Staff take responsibility for their own security	Staff take responsibility for their own security and that of their colleagues	Staff take responsibility for security of themselves and colleagues and keep others liable for their actions	Staff take responsibility, keep others liable and make suggestions for improvement
Attitude	Security is not an issue in our NGO	Security is an issue for some or after a serious incident	There is a basic awareness of security in our NGO among all staff	Security is taken into consideration in the decision-making process	Security is seen as a precondition to operate
Incident Reporting	Incidents are not reported	Serious incidents are reported	All incidents are reported (including near misses)	Incidents are reported, analysed and actions might be taken	Incident reporting is seen as crucial for organisational learning
Security Info Sharing and Analysis	One info source, info shared among those directly involved	Limited info sources, info shared between all staff	Info gathered from various sources, info shared with other NGOs	Info confirmation through multiple info sources, initiative towards external info sharing	Systematic info gathering, when security networks do not exist we initiate them
Programming	In programme set-up and implementation, no consideration for security situation	In programme set-up and implementation, some consideration, but not systematic	Security considerations are an issue in programming	Security considerations are a precondition to programme design	Specific programme design, based on security situation and scenarios

Checklist of organisational security perspectives

(Source: the ACT Alliance Security Library)

The purpose of this section is to develop the security-related awareness and capacities within an international organisation and/or their partner organisation. The checklist contains relevant security issues to be discussed within the international organisation and/or with staff responsible for security of the partner organisation.

1. Security policy and organisational set-up

- Which security concept is followed? Why?
- Which security risk reduction strategies are followed? What % of time/energy is devoted to each of them? Why?
- Is security management integrated in decision-making at the highest organisational level? What is the relative importance of security issues in operational decisions?
- At what level is the donor influencing/pressuring security-related decisions/activities?
- Is any security-related scenario forecasting applied? Did it prove to be effective?
- Do clear and relevant organisational security principles exist? Are they communicated and adhered to?
- Does a clear and relevant organisational security responsibility/authority division exist? Do the various job holders have appropriate tools for decision-making and application of their responsibility? Do the job holders apply those responsibilities?
- Does the organisation have an explicitly or implicitly defined risk threshold?
- Does the organisation have (explicit) risk-reduction measures to mitigate the security risks? At central/country and local level?
- Do effective communication/feedback mechanisms exist to address necessary improvements? Is the organisational climate open enough to report (near) security incidents, even when the involved staff made mistakes? Do management and staff show willingness for organisational learning?
- Are staff members (systematically) briefed/trained in identifying and mitigating risks?

2. Contextual adaptation

- Is identification and mitigation of risk undertaken only in a general way, or also at local level?
- How frequently are risk analysis/security plans updated?
- Are there single sources of security information, or multiple and reliable sources? How are these sources used? Any networking? What is done in the case of conflicting information?
- Is a multi-dimensional actor, threat and vulnerability analysis applied?
- Based on this analysis, are appropriate risk-mitigation measures applied?
- Are risk-analysis and risk-mitigation measures shared by all staff?
- Are the 6 steps of the security circle applied in the security plan?
- Is a local security assessment part of the set-up of any new programme (area)? Who conducts this assessment? How is it documented?

3. Security plan, security procedures, crisis management

- Does a country security plan exist? If so, does it include a risk assessment for each location of operation/travel?
- Do Security Standard Operational Procedures (SOPs) exist? Are they described in line with the organisational principles and responsibility division as stated in the security policy? If so, are the SOPs described for the identified risks in the risk analysis (risks with the highest probability and/or impact)?
- Are they general (developed at central level) and/or local (specific for risks/risk mitigation at local level)?
- Are they clear and concise? Are staff briefed and/or trained in how to apply them? Is adherence monitored?
- Do Contingency Plans (CPs) exist? Are they described in line with the organisational principles and responsibility division as stated in the security policy? If so, are the CPs described for the major type of incidents?
- Are they clear and concise? Are staff briefed and/or trained in how to apply them? Is adherence monitored?
- Does a procedure for security crisis management exist? For which issues will the crisis team be operational? Does the organisation have any experience with major security crises?

4. Staff quality, security awareness and compliance

- Are sufficient and competent staff available at central and local level to perform the security duties?
- Are staff willing to take operational responsibility, even in difficult circumstances?
- Do (all) staff members comply with the SOPs and CPs?
- Do staff provide feedback when they see possibilities for improvement of the SOPs and CPs?
- Do staff have the appropriate security equipment to fulfil their duties?

5. Successful security implementation

- Does the international organisation or partner organisation have a track record of preventing incidents effectively, even in medium- and high-risk areas?
- Does the international organisation or partner organisation have a track record of managing incidents in an effective way?
- Does the international organisation or partner organisation have a track record of managing serious crises in an effective way?
- Does the international organisation or partner organisation have a positive image in the areas where they work among the various actors, resulting in a relatively low incident rate?

6. Assuring safety and security of international organisation staff when travelling with their partner organisation

- Does the partner organisation have a different security risk analysis and related risk-reduction measures for visiting (expatriate) staff compared to national/local staff?
- In the security policy/plan/procedures, does the partner organisation state a (different) approach to the security of visitors? Is this known by the relevant staff and adhered to?
- Is the partner organisation more risk averse in relation to visitors such as international organisation travellers than when considering its own staff? For what reasons?
- Do individual travellers receive any briefing before travelling with the partner organisation to potentially medium/high-risk areas?

Participants

Person	Organisation	Position
Euan Mackenzie	CAFOD	Global Security Coordinator
George Shaw	HIV/AIDS Alliance	Security Officer
Peter Crichton	Concern	Emergency Preparedness Coordinator
Mike Dell'Amico	UNHCR	Chief, Field Safety Section, Geneva
James Darcy	Overseas Development Institute	Senior Research Fellow
Kamran Saeed	Save the Children	Global Safety and Security Learning and Development Adviser
Tom Brabers	Oxfam Novib	Security Adviser
Alexander Hasenstab	UNDSS	Field Security Coordination Officer, Pakistan
Frédéric Bardou	Action Contre la Faim	Head of Safety and Security Service
Cat Mahony	CAFOD	Programme Officer
Tony Keating	Islamic Relief	Security Coordinator
Pervez Iqbal	WESS (partner with Concern)	Executive Director, Pakistan
Sicko Pijpker	ICCO	Security Adviser
Brian Kavanagh	WFP	Coordinator for Safe Distributions, Pakistan
Heather Hughes	Oxfam GB	Security Adviser
Christine Williamson	People in Aid	HR Services Manager
Elisabeth Baraka	Advocates for International Development (A4ID)	Lawyer
Sean Hardy	Mayer Brown International LLP	Lawyer
Maarten Merkelbach	Security Management Initiative	Project Director
Julian Sheather	British Medical Association	Ethics Manager
Oliver Behn	EISF	Former Executive Coordinator
Shaun Bickley	EISF	Former, Interim Executive Coordinator
Shawn Bardwell	USAID/OFDA	Safety and Security Coordinator
Joshua Kearns	USAID/OFDA	Safety and Security Specialist
Anthony Val-Flynn	ECHO	Security Coordinator
Jethro Kleibeuker	ICCO/ACT Alliance	Financial Officer
Bidyanath Bhurtel	ICCO/ACT Alliance	Programme Officer, Nepal / Pakistan
Paul Mausert Francois	Adema (partner with ACF)	Executive Director, Haiti
Adele Harmer	Humanitarian Outcomes	Partner, Humanitarian Outcomes
Michael O'Neill	Save the Children	Senior Director, Department of Global Safety and Security
Edward Kemp	12 King's Bench Walk	Barrister

Glossary

The legal terminology aside, explanations of the key terms employed are based on terminology used by the wider humanitarian community and draw on existing policy documents and reports. The latter include: *The Good Practice Review on Operational Security Management in Violent Environments* (GPR8 2010) and *To Stay and Deliver: Good Practice for Humanitarians in Complex Security Environments* (Egeland et al 2011). Where other sources are used, appropriate reference is made.

Danger habituation: a usually unconscious adjustment of one's threshold of acceptable risk resulting from constant exposure to danger; the result is a reduction of one's objective assessment of risk, possibly leading to increased risk-taking behaviour

Dual remit organisations: organisations working in both humanitarian and development contexts

Duty of care: a legal concept presuming that organisations are responsible for their employees wellbeing and must take practical steps to mitigate foreseeable workplace dangers (Claus 2010)

Extremely insecure context: increasingly marked by politicised targeting of aid workers where risks are high and threats may include kidnapping and the use of major explosives.

Free and informed consent: where choices have been made and agreements reached on the basis of (i) an understanding of the relevant facts and security risks involved and (ii) formal and voluntary acknowledgement of these

Highly insecure context: where risks are high but threats may be based more on economic or tangential military risks as opposed to political targeting

Liability: being responsible for loss or damage by act or omission as required by law and the obligation to repair and/or compensate for any loss or damage caused by that act or omission and/or other sanction imposed by a court (Kemp and Merkelbach 2011)

Mitigation measures: strategies devised to tackle security risks usually combining, to differing degrees: acceptance (obtaining actor consent and support for activities); protection (using procedures and devices to reduce and avoid vulnerability); and deterrence (using a credible counter-threat to reduce the risk)

Programme criticality: an approach that involves determining which programmes are the most critical in a given part of a country (in terms of saving lives or requiring immediate delivery) and therefore warrant accepting a greater level of risk or a greater allocation of resources to mitigate these risks

Remote management: programming where, as an adaptation to insecurity, international or other at-risk staff are withdrawn and programme responsibilities are transferred to local staff or local partners

Residual risk: the inevitable risk remaining after all appropriate risk-reduction and mitigation measures are taken (as no security approach can remove all risk)

Risk: the likelihood and potential impact of encountering a threat

Risk analysis: an attempt to consider risk more systematically in terms of the threats in the environment, particular vulnerabilities and security measures to reduce the threat or reduce vulnerability

Risk management: the attempt to reduce exposure to the most serious risks (including contextual, programmatic and institutional) by identifying, monitoring and tackling key risk factors. It also involves balancing risk and opportunity, or one set of risks against another. Risk management should be seen as an enabling process, not simply a precautionary one.

Risk transfer: when, because of insecurity, an organisation consciously seeks someone else to carry out certain activities in a highly insecure context

Security focal point: a staff member with some responsibility for safety and security

Security strategy: the overarching philosophy, application of approaches and use of resources that frame organisational security management

Strict liability: responsibility for loss or damage by act or omission without proof of intentional or negligent conduct (Kemp and Merkelbach 2011)

Threat: a danger in the operating environment

Threshold of acceptable risk: the point beyond which the risk is considered too high to continue operating; influenced by the probability that an incident will occur, and the seriousness of the impact if it occurs

Resource list

Action Contre la Faim (2010/2011). *ACF Partnership Policy and Guidelines* (internal document).

CAFOD. *Partner Organisational Profile and Security Assessment Annex* (internal document).

Christian Aid (2010). *Saving Lives Together: a review of security collaboration between the United Nations and humanitarian actors on the ground.* Christian Aid.

Claus, L. (2010). *Duty of Care of Employers for Protecting International Assignees, their Dependents and International Business Travellers.* White Paper: International SOS.

Egeland, J., Harmer, A. and Stoddard, A. (2011). *To Stay and Deliver: Good Practice for Humanitarians in Complex Security Environments.* OCHA.

The UK Clinical Ethics Network. *The four principles approach.* Extracted 03/06/11 from: http://www.ethics-network.org.uk/ethical-issues/ethical-frameworks/the-four-principles-approach

Finucane, C. (2011). *Responsibilities towards Local Partners.* Christian World Service Pakistan/Afghanistan.

GPR8 (2010). *Operational security management in violent environments.* Good Practice Review 8 (new edition). Humanitarian Practice Network. London: ODI.

HIV/AIDS Alliance (2011). *Security Policy* (internal document).

HPN (2011). *Humanitarian Exchange: Humanitarian Partnerships*, No.50.

HPN (2010). *Humanitarian Exchange: Humanitarian Security Management*, No.47.

Kemp, E. and Merkelbach, M. (2011). *Can you get sued? Legal liability of international humanitarian aid organisations towards their staff.* Security Management Initiative.

Klamp, C. (2007). *Duty of Care: Legal Liability in the Humanitarian Sector.* Safety and Security Review, No. 7. RedR

Oxfam International (2010). *Working with Partners in Humanitarian Response.* Oxfam International.

Oxfam (2007). *Oxfam Partnership Companion* (internal document).

Santa Clara University. *A Framework for Thinking Ethically.* Markkula Centre for Applied Ethics. Extracted 03/06/11 from: http://www.scu.edu/ethics/practicing/decision/framework.html.

Save the Children. *Partner Training Needs Analysis* (internal document).

Save the Children. *Partner's Safety and Security Assessment Form* (internal document).

Save the Children (2010). *Detailed Safety and Security Budget Template and Security in Proposals Guidelines* (internal document).

Stoddard, A., Harmer, A. and DiDomenico, V. (2009). *Providing Aid in Insecure Environments: 2009 Update.* HPG Policy Brief 34. London: ODI.

Stoddard, A., Harmer, A. and Haver, K. (2011a). *Aid Worker Security Report 2011.* Humanitarian Outcomes.

Stoddard, A., Harmer, A. and Haver, K. (2011b). *Annex 1 to: To Stay and Deliver. Good practice for humanitarians in complex security environments.* OCHA.

Stoddard, A., Harmer, A. and Renouf, J. (2010). Once Removed: Lessons in Remote Management of Humanitarian Operations for Insecure Areas. Humanitarian Outcomes.

UNHCR (2007). UNHCR Security Policy. Accessible at: http://www.the-ecentre.net/news/bulletin/1.%20UNHCR%20Security%20Policy.pdf

UN IASC (2011). Saving Lives Together: A Framework for Improving Security Arrangements among IGOs, NGOs and the UN in the Field. Endorsed by the IASC Principals in August 2011. Accessible from: https://dss.un.org/dssweb/LinkClick.aspx?fileticket=4oBzjRXhh_w%3D&tabid=1016&language=en-US

WFP (2005). WFP's activities: principles and NGO involvement. Section 3. Accessible at: http://one.wfp.org/aboutwfp/partners/documents /english/NGO_handbook_Section3.pdf

WFP (2010). WFP Security Report; Administrative and Managerial Matters: Agenda Item 13. Accessible at: http://documents.wfp.org/ stellent/groups/public/documents/eb/wfp234276.pdf

Other EISF Publications

Briefing Papers

Gender and Security: Guidelines for Mainstreaming Gender in Security Risk Management
September 2012
Christine Persaud (author), Hye Jin Zumkehr (ed.)

Engaging Private Security Providers: A Guideline for Non-Governmental Organisations
December 2011
Max Glaser (author), supported by the EISF Secretariat (eds.)

Abduction Management
May 2010
Pete Buth (author), supportedby the EISF Secretariat (eds.)

Crisis Management of Critical Incidents
April 2010
Pete Buth (author), supported by the EISF Secretariat (eds.)

The Information Management Challenge
March 2010
Robert Ayre (author), supported by the EISF Secretariat (eds.)

Reports

Risk Thresholds in Humanitarian Assistance
October 2010
Madeleine Kingston and Oliver Behn (EISF)

Joint NGO Safety and Security Training
January 2010
Madeleine Kingston (author), supported by the EISF Training Working Group

Humanitarian Risk Initiatives: 2009 Index Report
December 2009
Christopher Finucane (author), Madeleine Kingston (editor)

Articles

Incident Statistics in Aid Worker Safety and Security Management: Using and Producing them
March 2012
Koenraad van Brabant (author)

Managing Aid Agency Security in an Evolving World: The Larger Challenge
December 2010
Koenraad Van Brabant (author)

Whose risk is it anyway? Linking Operational Risk Thresholds and Organisational Risk Management (in Humanitarian Exchange 47)
June 2010
Oliver Behn and Madeleine Kingston (authors)

Risk Transfer through Hardening Mentalities?
November 2009
Oliver Behn and Madeleine Kingston (authors)
Also available as a blog at
www.odihpn.org/report.asp?id=3067

Forthcoming publications

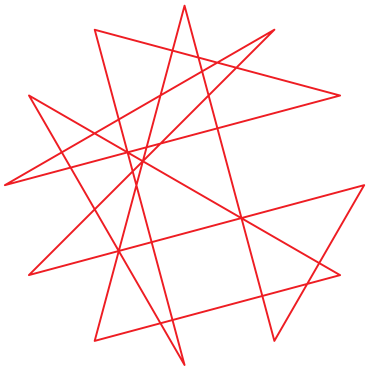
The Cost of Risk Management

Guide on Office Closure

Guide on Family Support in a Crisis

If you are interested in contributing to upcoming research projects or want to suggest topics for future research please contact **eisf-research@eisf.eu**.

eisf

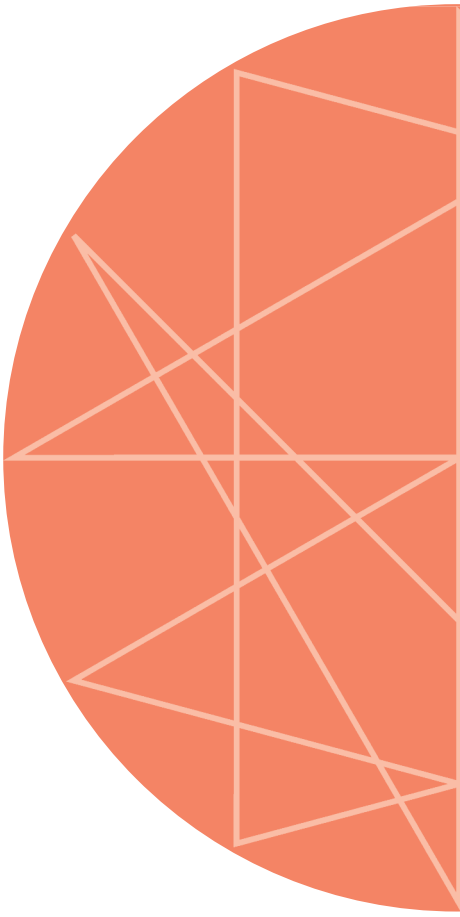


European Interagency Security Forum

EISF Coordinator
+44 7760 992 239
eisf-coordinator@eisf.eu

EISF Researcher
+44 7925 409 655
eisf-reseach@eisf.eu

www.eisf.eu



design and artwork: www.wave.coop

First published December 2012