

Generic Security Guide

for Humanitarian Organisations



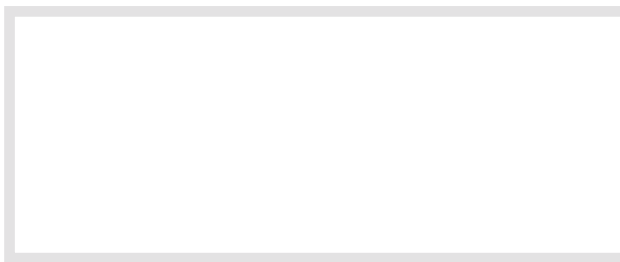
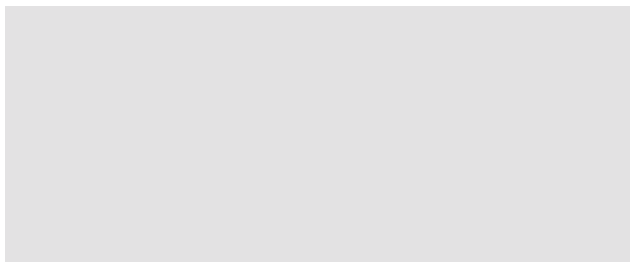
EUROPEAN COMMISSION



Humanitarian Aid

Commissioned by ECHO

2004



© Christian Aid / Peter Graystone



© Sean Sutton / Mines Advisory Group



© Action Contre La Faim

DISCLAIMER

This document is general in nature, and its contents may not be applicable in all situations. The advice it offers may be inappropriate in some circumstances and in some cases could even place people at risk of death or injury. Its contents should be modified and adapted as appropriate, to suit the needs of particular organisations and situations. It is not designed as a stand-alone document, but should be used by qualified and experienced managers who should exercise their judgement at all times as to the best course of action.

This document has been produced with the financial assistance of the European Commission's Directorate-General for Humanitarian Aid - ECHO. The views expressed herein should not be taken, in any way, to reflect the official opinion of the European Commission.

ECHO, The Evaluation Partnership and the author accept no liability whatsoever arising from the use of this document.

ECHO CONTACT FOR SECURITY MATTERS

The ECHO contact for security matters is:

E-mail: echo-ngo-security@ec.europa.eu

Web: <http://ec.europa.eu/echo>






TABLE OF CONTENTS

	1. Start Here	6		
	1.1 Aim of this Guide	6		
	1.2 What this Guide covers	6		
	1.3 What this Guide does not cover	6		
	1.4 If you are new to humanitarian work	7		
	1.5 If you are more experienced	8		
	1.6 If you are just visiting the field	8		
	1.7 A note for senior managers or security advisors	8		
	1.8 Do I really need a Guide this long?	9		
	1.9 How to use this Guide	9		
	2. Introduction to security	10		
	2.1 What is security?	10		
	2.2 Why is security important?	10		
	2.3 Approaches to security	10		
	2.4 Risk, Threat and Vulnerability	11		
	2.5 Definitions	11		
	3. Security preparation for the field	12		
	3.1 Security assessment before deploying	12		
	3.2 Prepare a security plan before deploying	12		
	3.3 Humanitarian space	13		
	3.4 Consider security aspects of proposed programmes	14		
	3.5 Selection of staff	14		
	3.6 Training	15		
	3.7 Briefing	16		
	3.8 Equipping	16		
	3.9 Preparing illiterate staff	17		
	3.10 Preparing security-related aspects of administration	17		
	3.11 Offices and warehouses	18		
	3.12 Staff accommodation	18		
	3.13 Standard documents and equipment	19		
	3.14 Personal preparation	19		
	3.15 Medical preparation	19		
	4. Security management in the field	20		
	4.1 Revised security assessment	20		
	4.2 Revised security plan	20		
	4.3 Information-gathering	20		
	4.4 Relations with the local population	21		
	4.5 Relations with other organisations	21		
	(a) Local authorities	21		
	(b) Local security forces	22		
	(c) Other humanitarian organisations	22		
	(d) The UN security system	23		
	(e) International military forces	23		
	(f) International police force	24		
	(g) Embassies	25		
	(h) Donors	25		
	(i) Local partners	25		
	(j) Security coordination between humanitarian organisations	26		
	4.6 The Field-Headquarters relationship	26		
	4.7 Reporting	27		
	4.8 Security aspects of programme design	27		
	4.9 Routine security management	28		
	(a) Teamwork	28		
	(b) Staff behaviour	28		
	(c) Female staff	30		
	(d) Rest and Recreation (R&R)	30		
	(e) Stress	30		
	(f) Discipline	30		
	(g) Checkpoints	31		
	(h) Weapons	31		
	4.10 Technical issues	31		
	(a) Telecommunications	31		
	(b) Vehicles	32		
	(c) Guards	33		
	(d) Fire safety	33		
	4.11 Administrative issues	33		
	(a) Financial security	33		
	(b) Information security	33		
	(c) Managing keys	34		
	(d) Identity badges	34		
	(e) Procurement	34		
	(f) Corruption	35		
	(g) Consider a "Get-you-in" team	35		
	4.12 Travel	35		
	4.13 Media aspects of security management	36		
	4.14 Visibility and security	36		
	4.15 Legal protection of aid workers	37		
	4.16 Reporting of war crimes	37		
	5. Security incidents	39		
	5.1 Security incidents: prevention and reaction	39		
	5.2 Reporting of incidents	39		
	5.3 Reporting 'near miss' incidents	39		
	5.4 Debriefing after an incident	39		
	5.5 Analysis of incidents and adjustment of procedures	39		
	5.6 Medical evacuation (Medevac)	40		
	5.7 Fatal incidents	40		
	5.8 Investigation of a serious incident	40		
	5.9 Media handling after a security incident	40		
	6. Suspension, Hibernation, Relocation, Evacuation	41		
	6.1 Deciding whether to suspend, hibernate, relocate or evacuate	41		

TABLE OF CONTENTS

	6.2 Suspension of programme activities	41	9.4 Learning from other agencies and networks	53
	6.3 Hibernation	42	9.5 Use of experienced staff as trainers, briefers, advisers, evaluators	53
	6.4 Relocation or reduction of staff	42	10. Donors	54
	6.5 Evacuation	42	11. Abbreviations	55
	6.6 Role of the United Nations in evacuation	43	12. Important information about this Guide	56
	6.7 Debriefing after an evacuation	43	12.1 Acknowledgements	56
	6.8 Media aspects of suspension, hibernation, relocation or evacuation	43	12.2 Authors and date	56
	6.9 Return after evacuation	44	12.3 Funding	56
	7. Closing a programme	45	12.4 Copyright	56
	7.1 Ending staff contracts	45	12.5 Software and languages	56
	7.2 Ending other contracts	45	12.6 Further copies	56
	7.3 Legal aspects of programme closure	45	12.7 ECHO contact	56
	7.4 Disposing of property	45	12.8 Photo credits	56
	7.5 Evaluation and inspection	45	Annexes: Checklists, Templates and Further Information	
	7.6 Handover of a programme	46	A1. Buildings and security	60
	7.7 Media aspects of closing a programme	46	A2. Checkpoints	62
	7.8 Farewell events	46	A3. Convoy procedures	64
	7.9 Debriefing after programme closure	46	A4. Corruption: avoidance and prevention	65
	7.10 Archiving documents after programme closure	46	A5. Cultural awareness	67
	8. Headquarters management of security	47	A6. Drivers: a basic checklist	68
	8.1 Responsibilities of Headquarters for security management	47	A7. Emergency contact card	70
	8.2 Hierarchy of documents: security policy, manual, plan	47	A8. Equipment for personal security	71
	8.3 Security advisor	48	A9. Equipment for team security	72
	8.4 Human Resources Management – security aspects	48	A10. Evacuation	73
	8.5 Serious or high-profile incidents	48	A11. Financial security	76
	8.6 International Humanitarian Law	49	A12. Fire safety	78
	8.7 Advocacy and humanitarian space: Headquarters aspects	49	A13. Guards and private security companies	80
	8.8 Archives	49	A14. Health and hygiene	83
	8.9 Discipline	49	A15. Information security	85
	8.10 Duty officer system	50	A16. Insurance for war risks	87
	8.11 Relating to the UN Security System	50	A17. International Humanitarian Law (IHL)	88
	8.12 Relating to donors	50	A18. Inventory control	90
	8.13 Codes and Standards	50	A19. Media and security	91
	9. Learning and training	52	A20. Medical evacuation (Medevac)	92
	9.1 Security lessons learned	52	A21. Next of Kin records	93
	9.2 Evaluations	52	A22. Next of Kin: procedure for informing them	94
	9.3 Training	52	A23. People In Aid Code: Principle Seven	96
	(a) Training for new field staff	52	A24. Radio procedures	97
	(b) Training for field managers	52	A25. Rest and Recreation (R&R)	100
	(c) Training for Headquarters managers	52	A26. Security assessment	101
			A27. Security briefing	105
			A28. Security incidents: prevention and reaction	107
			(a) Accidents	107

TABLE OF CONTENTS

	(b) Air attack	108
	(c) Air crash	108
	(d) Ambush	109
	(e) Arrest or detention	112
	(f) Assault	112
	(g) Bomb	113
	(h) Bomb threat by telephone	114
	(i) Chemical, biological or radiological attack	114
	(j) Crowds	115
	(k) Earthquake	115
	(l) Fighting	115
	(m) Fire	117
	(n) Flood	117
	(o) Fraud	117
	(p) Grenade	118
	(q) Hijack – vehicles	119
	(r) Hijack – aircraft	120
	(s) Kidnap	120
	(t) Looting	122
	(u) Medical emergency	123
	(v) Mines, booby traps and unexploded ordnance (UXO)	123
	(w) Rape and sexual violence	124
	(x) Robbery	126
	(y) Sexual harassment	126
	(z) Shooting	127
	(aa) Terrorism	127
	(bb) Weapon finds	127
	A29. Security incidents and ‘near misses’: report format	128
	A30. Security manuals	129
	A31. Security plan	130
	A32. Security policy	133
	A33. Shelters	135
	A34. Sitrep format	136
	A35. Stress	137
	A36. Syllabus for a basic security training course	139
	A37. Syllabus for a security course for field managers	140
	A38. Threat Impact Chart	141
	A39. Travel authorisation format	143
	A40. UN security procedures	144
	A41. UN-NGO Security Collaboration: Menu of Options	146
	A42. Vehicle equipment	147
	INDEX	148

FIND A SECTION QUICKLY

Click on a section heading in the Table of Contents, to jump directly to that section in the text.

To jump back to the Table of Contents, click on any page number.

The text of the Guide is cross-referenced. Where a word is underlined (for example [Annex 22](#)) click on it to jump directly to that Annex.

1. START HERE

- 1.1 Aim of this Guide
- 1.2 What this Guide covers
- 1.3 What this Guide does not cover

1.1 Aim of this Guide

The aim of this Guide is to help humanitarian organisations to manage their security well.

It does this by offering suggested guidance, tools and resources, designed to assist organisations to think through their security policies and procedures. It is intended to be adapted, by those responsible for security management, to suit the needs of a particular organisation and situation.

It does not cover every possible situation, organisation or eventuality. But since there are some common features to many insecure situations, a generic Guide of this kind can be helpful in suggesting, prompting, reminding and offering useful tools. It is not intended as a 'standard' or a requirement for any organisation.

The design of the Guide was decided after consultation with a wide range of humanitarian organisations. Accordingly, it aims to combine the following qualities:

- ▲ Highly practical guidance, avoiding theory, but with reasons given where this is helpful
- ▲ Bullet point checklists wherever possible, for ease of use
- ▲ Simple, clear language
- ▲ Accessible and easy to navigate, with detailed Table of Contents and Index
- ▲ Designed to be adapted by humanitarian organisations to their particular needs
- ▲ Illustrated, user-friendly layout
- ▲ Equal emphasis on nationally-recruited and international staff
- ▲ Step-by-step approach for all levels, with specific sections for new humanitarian staff all the way through to senior managers
- ▲ Existing documents and resources are referred to where these may be of further help

The Guide is complemented by a Report on the security of humanitarian personnel and a Security Training Directory.

While the primary intended audience is those responsible for the security management of an entire

humanitarian organisation, the Guide may also be of use, as a reference document, to:

- ▲ Field-based humanitarian managers
- ▲ Field-based humanitarian workers
- ▲ Visitors to the field
- ▲ Managers at Headquarters

1.2 What this Guide covers

This Guide aims to cover most aspects of security management and practice that are commonly thought relevant to humanitarian organisations working in emergencies in the field, in most parts of the world.

The Guide is based on existing good practice. It draws extensively from security manuals and other documents produced by a wide variety of humanitarian NGOs, UN agencies and the Red Cross / Crescent Movement.

National and international staff are covered equally in this Guide. Where a point refers to one or other group only, this is made explicit. Otherwise, all sections refer to all staff.

This Guide is about security rather than health and safety. But it would make little sense to manage security well while taking no fire precautions, for example. Accordingly, this Guide mentions basic fire precautions, and some other health and safety issues relevant to protecting humanitarian staff.

1.3 What this Guide does not cover

The Guide does not cover aspects of security management or practice that are specific to particular locations, cultures, or types of humanitarian operation. Instead it focuses on generic aspects that may be applicable in a wide variety of situations. It is always important to consider whether the generic points mentioned in this Guide need adapting to suit a particular situation.

The Guide does not aim to cover health and safety, except for a few selected issues which can pose serious threats to life. Readers should be aware that in

1. START HERE

1.4 If you are new to humanitarian work

many cases health issues pose the most serious risk to life, and should take precautions accordingly.

The Guide does not discuss the security or protection of local populations, refugees, children or other vulnerable people.

The Guide is aimed at humanitarian organisations, and therefore does not take into account the particular needs of those working on development programmes.

Most importantly, the Guide is no guarantee of security. Using the Guide does not replace the need for appropriate training, experience and judgement, coupled with the relevant equipment and procedures, applied as each situation demands. Please read and note the disclaimer, inside the front cover.

1.4 If you are new to humanitarian work

Benefits and risks

Humanitarian work, if done well, saves lives and relieves suffering. It is often also an enjoyable and rewarding experience for those who bring the assis-

tance. At the same time, in many countries there are serious threats to humanitarian staff.

The great majority of humanitarian staff carry out their work without coming to harm. But some have become sick, some have been injured, some have been held hostage, and some have been killed while doing their work.

Responsibility

Each individual is responsible for security. Humanitarian staff at every level are responsible for doing all they can to ensure their own security, as well as the security of their colleagues and others. The actions of one person can have an effect on the security of others in the same organisation, members of other organisations, and local people.

Line managers at all levels are responsible for ensuring the security of their team as a whole. To help them in this task, they may delegate some security-related functions, or take advice from a colleague who specialises in security matters. But the main responsibility for the team's security should belong to the line manager.

Reducing risk

It is not possible to eliminate risk, but it is usually possible to reduce it. A passenger in a car reduces risk by wearing a seatbelt and ensuring that there is a competent driver, but knows that some risk remains. In a similar way, humanitarian staff can take precautions to reduce risks, but can never reduce them to zero. In some cases, whatever precautions are taken, the risks remain high.

Humanitarian workers learn to balance risk against benefit. If the likely benefit of your work is great (for example, it will save many lives) and the risk is small, then you will probably decide to go ahead and do the work. But if the likely benefit is small and the risk is great, you will normally decide not to do the work, since it is not worth the risk.

As a new humanitarian worker, you will need to learn to assess risk, to assess the likely benefit that your work will bring, and to weigh the one against the other. The ability to do this is mainly learned by

The purpose of security management is to reach beneficiaries more effectively
© Christian Aid/Georgiana Treasure-Evans



1. START HERE

- 1.5 If you are more experienced
- 1.6 If you are just visiting the field
- 1.7 A note for senior managers or security advisors

experience in insecure situations in the field. Those with little or no such experience rely on their manager or supervisor to assess risk on their behalf. It is important for humanitarian staff at all levels to accept proper supervision in security matters, and to support managers in this task. It is also vital that managers and supervisors are fully competent to assess and manage risk on behalf of their teams.

Preparing for insecure situations

Those about to gain their first humanitarian field experience can and should do a great deal to prepare themselves for work in insecure situations. Preparation falls into three main categories:

- ▲ **Training** teaches you skills, and practises you in them until you can do them yourself.
- ▲ **Briefing** gives you information, for example about a particular country, culture, and security situation, about your organisation and about the humanitarian situation on the ground.
- ▲ **Equipping** provides equipment that you may need, to help enhance your security.

It is vital that new humanitarian workers make themselves available for training, briefing and equipping; read training and briefing materials thoroughly; and ensure that they understand them. Don't hesitate to ask your manager any questions you may have – it may save your life. If any part of security preparation appears to have been omitted, raise this with your manager. Busy managers can sometimes be tempted to make short cuts. Don't be afraid to insist on proper security preparation.

You will find more detail about appropriate training, briefing and equipping in Chapter 3 of this Guide. Further resources are available in the annexes.

Your organisation should provide you with a security manual or handbook and all other security-related information you need. If so, it should not be essential for you to read this Guide. But it may be useful as a reference manual, and to help to fill any gaps there may be in the guidance that you are given.

Your comments on this Guide, particularly on how it could improve in usefulness to new humanitarian

staff, are most welcome and should be addressed to the ECHO contact on security matters (see Section 12).

1.5 If you are more experienced

If you already have experience with a humanitarian organisation in an insecure location, this Guide may provide information or suggest ideas that are new to you, or remind you of points that you already know.

Your comments are most welcome and should be addressed to the ECHO contact on security matters (see Section 12).

1.6 If you are just visiting the field

Visitors to the field face as many threats as field-based staff, and sometimes more. It is vital that you ensure that you are properly prepared for your visit, and that an appropriate and competent person takes responsibility for your security.

Your comments on the Guide, particularly on how it could improve in usefulness to field visitors, are most welcome and should be addressed to the ECHO contact on security matters (see Section 12).

1.7 A note for senior managers or security advisors

This Guide is intended to help you. Your organisation may have appropriate security policies and practices in place, with field and Headquarters staff maintaining high standards of security. If so, you may wish to use this Guide simply as a comparison, or to double-check that nothing has been forgotten.

At the other end of the spectrum, your organisation may be conscious that it needs to make considerable improvements to its security management. The large number of procedures contained in this Guide may appear daunting or even unrealistic. If so, please be reassured by the following comments:

- ▲ Not all procedures are necessary for all organisations or all locations. The contents of this Guide should be adapted – and in some cases

1. START HERE

shortened – to meet your particular needs. Help is available, if you need it. Training organisations and consultants are two possible sources of help. (See the Security Training Directory which accompanies this Guide, for some examples of these).

If many changes are needed in your organisation, you may consider appointing a “change manager” to ensure that the improvements are made. This would free you and other senior managers to do your normal tasks.

- ▲ If the chief executive or board of directors supports good security management and allocates the necessary staff and resources, the task of implementing it becomes much easier. Take time to win their commitment.
- ▲ Finally, ask yourself if your organisation can afford **not** to manage security well? Lives are at stake. Your staff will do a better job if they are secure, leading to better assistance to those who need it.

A failure by management to address security, or health and safety risks, may expose you to legal action. This may carry a risk of your organisation being bankrupted by successful lawsuits.

1.8 Do I really need a Guide this long?

Security management should be kept as simple as possible, and yet there are many issues which need to be taken into account.

Your organisation should provide you with a security manual or handbook which meets your needs. If so, this Guide may be useful simply as an extra reference manual. Only use the sections which are helpful and relevant to your organisation and your situation, and adapt them as appropriate.

If you have no security manual, the idea is that the Guide should make it easier for senior managers to create a security manual of appropriate length and detail for their organisation. It should also help them to design relevant security policies, procedures

1.8 Do I really need a Guide this long?

1.9 How to use this Guide

and plans. How they do so is a matter for their judgement, and they will need to select, change, adapt and add to material found in this Guide.

Finally, there may be some immediate improvements you can make in the way that security is managed, or staff are prepared for their work. Don't let changes that will take longer prevent you from making those immediate improvements as soon as possible.

1.9 How to use this Guide

This Guide is intended to help humanitarian organisations to think through their security policies and procedures. Senior managers with security responsibilities may wish to use the whole Guide, to help them to design a security policy, a security manual and other procedures for their organisation.

Other users may prefer to use the Guide as a reference manual, to provide easily accessible help on a particular topic when the need arises. With this in mind, the Guide has several methods of finding the topic you are looking for:

- ▲ A table of contents
- ▲ A substantial index
- ▲ References and links within the text

In the Word and pdf versions, you can search for a particular word or phrase using the search facility provided by those programmes. Select 'Edit' then 'Find', or press Ctrl-F (i.e. hold down Ctrl and press F).

The Guide has a large number of annexes, containing helpful checklists, which can be adapted to your needs.

All users are welcome to use extracts from this Guide in their own documents, adapted as necessary to their own needs. This is subject to the disclaimer, to be found inside the front cover, and the copyright notice at section 12.4.

2. INTRODUCTION TO SECURITY

- 2.1 What is security?
- 2.2 Why is security important?
- 2.3 Approaches to security

2.1 What is security?

For the purposes of this Guide, security is the protection of humanitarian personnel and assets from violence and theft.

2.2 Why is security important?

Serious security incidents place humanitarian staff and property at risk. Any responsible employer will wish to take all reasonable steps to protect the lives of its staff, and to protect its assets.

Serious or unanticipated security incidents also place the provision of assistance at risk, with the danger that humanitarian assistance for needy populations may be curtailed or suspended. If humanitarian staff are secure, they are able to do a more effective job in bringing assistance to those who need it.

2.3 Approaches to security

Acceptance

Traditionally, humanitarian organisations have relied for their security on the goodwill of the local

population. This is still the favoured approach where possible. If the local population support the work that the humanitarian organisations are doing in their area, they will not threaten them but help them. This approach is often known as the "acceptance approach", since it depends on acceptance by the population.

To win acceptance, humanitarian staff may need to spend considerable time listening to local people, and explaining their role to local leaders and residents, both directly and via the media. This may include negotiation of access to areas of need; explanation of the humanitarian principles underlying the work; and response to rumours or accusations when they arise.

The acceptance approach is usually not enough on its own. Every society contains some people who resort to crime, and humanitarian staff and property may be targeted by criminals. The most frequent crime against them is probably theft, since they are sources of money and valuable goods in the midst of poverty. Sometimes they are the target of more serious threats such as assault, rape, kidnapping or even murder.

Protection

Therefore, even when there is wide local support for humanitarian organisations, they need at least some protection. Common protection measures include gates, guards, locks and safes. Other protection measures are decided on according to the threat in each specific context.

When there is not complete local support for the humanitarian organisations, a higher degree of protection is necessary if the work is to continue. In this case managers will usually consider whether the work should stop, either temporarily or permanently.

There may be some threats to humanitarian organisations which do not arise from the local community at all. These may include natural hazards such as disease, volcanic eruptions or floods. They may also include attacks from terrorist groups, whose decision-makers may be distant or even in a different country, orchestrating violence against humanitari-

Troops, civilians and aid workers frequently occupy the same space
© James Thurlow



2. INTRODUCTION TO SECURITY

2.4 Risk, Threat and Vulnerability

2.5 Definitions

an and other organisations for political reasons. If so, protection measures will need to take these threats into account.

Deterrence

Deterrence is a further security approach used by some organisations, notably the police and the military. They deter attack by threatening retaliation against anyone who attacks them. This is not an option available to humanitarian organisations, whose principles forbid them to attack anyone, or to threaten attack. The sole possible exception is when humanitarian organisations use armed guards, in extreme circumstances when there is no other way to protect staff and property (see Annex 13). A guard carrying a weapon is a type of deterrent: this is the only method by which humanitarian organisations may legitimately use deterrence.

Thinking long-term

Humanitarian managers try to keep in mind the long-term impact of their decisions about security. They aim to ensure that staff and property are safe, while upholding humanitarian principles¹, nurturing good relationships with local people, and bringing closer the day when outside assistance will no longer be needed.

2.4 Risk, Threat and Vulnerability

It can be helpful to distinguish between risk, threat and vulnerability by defining them as follows:

- ▲ **Threat:** a danger to you, your organisation or your property
- ▲ **Vulnerability:** your level of exposure to a particular threat
- ▲ **Risk:** the likelihood and impact of encountering a threat

For example, there may be a threat of theft. Your vulnerability to that threat depends on various factors including what money or valuable property you possess; whether potential thieves know about it; whether your neighbours will warn you of the potential for theft in the area; whether you have good locks and safes; whether you have efficient guards; etc. The risk that you will suffer from the

theft depends both on the level of threat, and your level of vulnerability to that threat. This is sometimes expressed in the relationship:

$$\text{Risk} = \text{Threat} \times \text{Vulnerability}$$

You may be able to do nothing about the level of threat around you, but you can probably do a great deal to reduce your level of vulnerability in two main ways:

- ▲ Reducing the chances of an incident happening (e.g. by driving slowly, improving locks, or introducing a neighbourhood watch system)
- ▲ Reducing the impact of an incident (e.g. by wearing seatbelts, or limiting the amount of cash held in the safe)

By reducing your vulnerability, you reduce the risk that the threat will become reality and have a serious impact on you. A major part of good security management is reducing vulnerability in every way possible.

2.5 Definitions

For the purposes of this Guide, the terms below are defined as follows.

Humanitarian space: The access and freedom for humanitarian organisations to assess and meet humanitarian need.

Security: The protection of humanitarian personnel and assets from violence and theft.

Security policy: A short document approved by the top management and board of trustees of a humanitarian organisation, setting out the organisation's overall approach and principles in relation to security.

Security manual: A handbook giving generic security procedures to be applied by all staff, but not including location-specific procedures. (The handbook may be a relatively long document.)

Security plan: A short document giving location-specific security information and procedures, that do not feature in the security manual. A separate security plan is produced for each field location.

Security incident: An event which threatens humanitarian staff or assets with violence or theft, or results in actual violence or theft against them.

¹ Humanitarian principles are summarised in the Code of Conduct for the International Red Cross and Red Crescent Movement and NGOs in Disaster Relief, available at <http://www.ifrc.org/publicat/conduct/code.asp>.

3. SECURITY PREPARATION FOR THE FIELD

- 3.1 Security assessment before deploying
- 3.2 Prepare a security plan before deploying

3.1 Security assessment before deploying

The team leader normally carries out a security assessment before a final decision is taken to deploy, and certainly before the arrival of the main team. It is done preferably by an assessment visit and, where a visit is not possible, by remote assessment.

If a team is already in the area, for example carrying out a development programme before the emergency began, then their existing security assessment should be used to inform the security assessment for the humanitarian team.

The aim of the security assessment is to understand the situation sufficiently to enable the team to plan their security measures appropriately.

Assessment visit

A security assessment visit should be long enough to achieve its aim. Factors influencing the length of the visit include:

- ▲ The level of insecurity
- ▲ The experience of the person/people making the assessment
- ▲ The number of people making the assessment
- ▲ Geographical size of the area
- ▲ Complexity of the political situation
- ▲ Weather
- ▲ Other local events, e.g. holidays, festivals
- ▲ Availability of key interlocutors such as local leaders
- ▲ Availability of transport
- ▲ Availability of good maps
- ▲ The severity of humanitarian need. If many people are dying, a more rapid security assessment may sometimes be necessary, to allow the programme to begin as soon as possible – but this is a matter for careful judgement since too rapid an assessment can be dangerous.

A security assessment can be combined with other aims, for example a needs assessment.

Remote assessment

A remote assessment (i.e. an assessment without visiting the area concerned), may occasionally be nec-

essary, if a visit is not possible. It should seek to answer the same questions as an assessment visit. It is much harder to do so because it is not possible to talk to the same people, or in the same way, if one is limited to telecommunications. A remote assessment is therefore much less reliable than an assessment visit, and is no substitute for a visit if possible.

A remote assessment should be checked and revised as necessary, as soon as the first staff deploy.

Assessment method

A suggested method for a security assessment is at Annex 26.

3.2 Prepare a security plan before deploying

A security plan should be produced, at least in outline form, before a team deploys to a new location. It should then be modified as the team gets to know the situation better.

Ideally, all staff should have an opportunity to contribute to the security plan. In practice this is not always possible. But experience has shown that staff who participate in the design of a security plan produce a better plan, and are more likely to follow it.

The aim of a security plan is to provide staff with a concise document which sets out the security rules and procedures applying to the location(s) where they are working. It must be short (many experienced field managers say it should be less than 10 pages, excluding annexes), otherwise it is likely that some staff will not read it.

Each organisation decides its own format for a security plan. A possible suggested format is at Annex 31. The security plan should give context-specific rules and procedures, and normally should not give generic security advice which would make the security plan too long.

Each literate staff member should have a generic security manual or handbook that has been approved by the employing organisation. This is a much longer document than a security plan. It gives detailed advice on a wide variety of security issues.

3. SECURITY PREPARATION FOR THE FIELD

3.3 Humanitarian space

All staff should be familiarised with the relevant parts of it as part of their security training, before they start work. See Annex 30 for examples of security manuals and handbooks.

In addition, guidance on the organisation's overall attitude to security should be written in a security policy. The hierarchy of security documents is thus:

- ▲ **Security policy** – giving overall policy and principles for the organisation (see Annex 32 for a suggested format for a security policy)
- ▲ **Security manual** – giving generic procedures for the organisation
- ▲ **Security plan** – giving detailed procedures for a specific location

3.3 Humanitarian space

For the purposes of this Guide, humanitarian space is defined as the access and freedom for humanitarian organisations to assess and meet humanitarian need.

In some situations it is necessary to negotiate with

leaders or local people to be allowed access to the areas of humanitarian need. When negotiating, it is important not to compromise on fundamental humanitarian principles, as set out for example in the Red Cross / Crescent / NGOs Code of Conduct². One objective of these negotiations will usually be to verify that local leaders and groups will do whatever is necessary to ensure the safety of humanitarian staff.

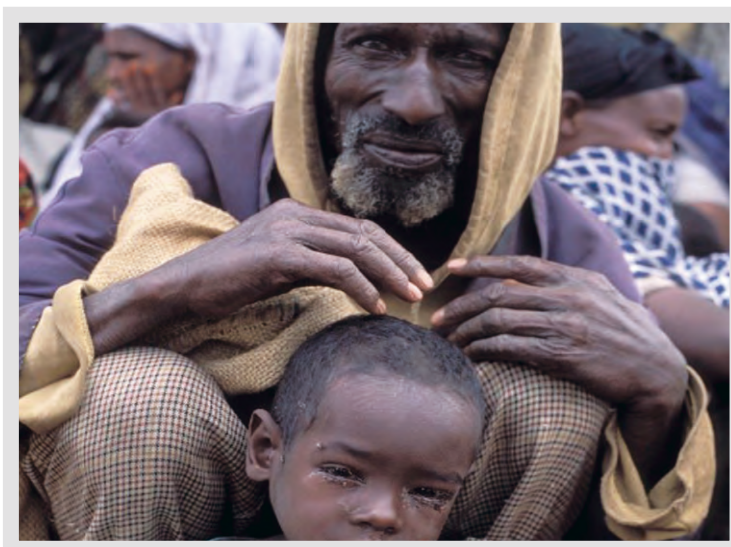
Sometimes humanitarian principles may conflict, for example if providing assistance on the basis of need alone is not in accordance with respecting local customs. In such cases, good judgement and common sense are needed, perhaps with advice from experienced colleagues.

If relief goods have to travel through areas which are not receiving assistance, in order to reach the most needy areas, local people in the areas being transited sometimes demand a share of the aid. Such demands can lead to violence if not well handled. They are best prevented by negotiations in advance with the representatives of those areas, ensuring that people understand the planned assistance and the reasons for it. Preventing misunderstandings is better than trying to resolve them once they arise. But if they do arise, quick action is necessary, to prevent an escalation of the problem.

Humanitarian organisations should always conduct negotiations with integrity. Bribes or other inducements should never be given in return for access. They are wrong in principle, and in practice usually lead to demands for further bribes. Instead, any group or individual denying access should be reminded of their responsibilities to allow humanitarian assistance to reach those who need it.

The actions of one humanitarian organisation often affect the work of other organisations. Consulting other relevant organisations is therefore essential, before negotiating with local leaders for access or wider issues of humanitarian space. In some cases a local code of conduct has been agreed among operational agencies so that everyone is working on the same agreed basis and can avoid being played off against each other.

Insecurity affects children and the elderly more than most
© Christian Aid/Jenny Matthews



² Available at <http://www.ifrc.org/publicat/conduct/code.asp>.

3. SECURITY PREPARATION FOR THE FIELD

Most importantly, the local population can be endangered by the actions of humanitarian organisations. For example, communicating the locations of refugees or going to help them might lead armed groups to them, who may then attack them. It is crucial to be aware of the local situation, and the aims of different leaders and groups, before negotiating with them.

3.4 Consider security aspects of proposed programmes

When preparing for the field, consider the security aspects of the programmes you expect to be involved in. A number of possible aspects are listed under "Security aspects of programme design" in Chapter 4.

3.5 Selection of staff

The quality and appropriateness of staff are probably the greatest single factors influencing the security of humanitarian work (and its effectiveness). Great care is therefore needed when selecting staff.

The same principles of staff selection apply both to nationally- and internationally-recruited staff, though their implementation may differ according to the post advertised, and local circumstances. Good selection makes security management much easier. Poor selection makes it more difficult to manage security well.

Rigorous checking of candidates' references is vital. It helps to ensure that those with a previous record of dishonesty, or other security-related problems, are identified and not employed.

In accordance with the principles of equal opportunity, the nationality or ethnic group of a candidate should normally have no bearing on whether he or she is employed. Nevertheless, if a team as a whole is perceived as having an unfairly high proportion of one nationality or ethnic group, some staff – and local opinion – may suspect that biased selection has taken place. That suspicion could in turn have an impact on staff security. This is a sensitive issue, which requires a clear and fair policy decision by sen-

3.4 Consider security aspects of proposed programmes

3.5 Selection of staff

ior managers, in line with applicable employment law. In some cases it may be legal, for example, to adopt a policy that for reasons of security and effectiveness, the staff team should reflect a reasonable mix of local ethnic groups, and to allow this policy to influence recruitment decisions.

In some situations, security may be enhanced by employing staff mainly from a particular ethnic group – for example if the programmes are aimed at displaced people from one ethnic group, who are in conflict with other ethnic groups in the area. If so, this consideration should be weighed against considerations of equal opportunity, and a careful decision made.

As a general rule, qualified national staff should be preferred for all posts unless there is a good reason to employ international staff for a particular post. This is likely to make the programme more sustainable, more culturally appropriate and more cost-effective, therefore more acceptable to local people and more secure.

Each situation will have its own characteristics. There have been examples where the government or a local political group have infiltrated NGOs by ensuring that their agents are recruited as national staff. This can have a serious effect on the real and perceived impartiality of the organisation, as well as its security. In other contexts, international staff of a certain nationality may be unacceptable for political reasons. Managers must try to be aware of such issues, and bear them in mind when recruiting.

Timely employment of the necessary staff is often a great challenge for humanitarian organisations. If key posts remain vacant it can cause dissatisfaction among other staff, or among local people as they see programme delays resulting. Risks to staff can then increase.

Proper recruitment is not easy during an emergency, and includes the following factors:

- ▲ Accurate job descriptions, including any security-related responsibilities

3. SECURITY PREPARATION FOR THE FIELD

- ▲ Accurate person specifications, including any security-related skills or experience that are required
- ▲ A fair and transparent recruitment process so that there can be no accusations of bias
- ▲ Adequate advertising of the vacancy
- ▲ Appropriate interviews and tests
- ▲ Rigorous checking of references before a contract is signed and before the candidate starts work. This is difficult to achieve, and sometimes impossible, during the height of an emergency. Be aware of the danger of employing someone who has been found to be dishonest, for example, by a previous employer. A follow up of references by phone or in person is often the most practical and effective way to check on a previous record.
- ▲ One issue that often leads to tension is failure to inform unsuccessful candidates
- ▲ Contract documents conforming to applicable laws and regulations, and meeting the needs of both the organisation and the employee. It is helpful if the organisation provides a standard contract text, which can be adapted to the local context and legal requirements. Without standard texts, writing contracts from scratch can be very difficult for hard-pressed managers in an emergency.
- ▲ In many cases it is advisable for humanitarian organisations to use a local employment lawyer to check contract terms, to advise on local employment practice and to assist in preventing or dealing with any employment disputes. Employment disputes and resulting legal action can be a very time-consuming distraction for humanitarian organisations, and can have security implications as disgruntled former employees, for example, resort to threats or violence.
- ▲ Emergency contracts are often short in duration. It is important to point out, and have written down, that an appointment may be temporary and there can be no guarantee of long term employment.
- ▲ Contracts should contain a clause stating that employment may be terminated at short notice, for example if insecurity forces a programme to close.

3.6 Training

- ▲ Check with employment laws about what severance payments are required, and make these clear in the contract
- ▲ Anticipate potential employment disputes before they arise so that you have at least the law and documentation on your side
- ▲ In some circumstances it may be necessary to have signed witnesses to contracts

3.6 Training

Perhaps the second greatest contributor to security, after the selection of high-quality and appropriate staff, is training.

It is a management responsibility to ensure that all staff have received any training that is necessary for their work. This requires careful judgement. Staff with significant field experience may need less training than staff who are new to insecure situations. But even experienced staff sometimes lack some elements of training which may be essential in the situation they are intending to work in.

New field staff who are due to work in an insecure situation will normally require training to a basic level in at least the following skills:

- ▲ The 'humanitarian system' including the UN agencies, Red Cross/Crescent Movement
- ▲ Assessing security threats
- ▲ Awareness of the most common types of security threat
- ▲ Understanding the 'acceptance approach' to security
- ▲ Respecting culture and custom
- ▲ Basic language skills, if possible
- ▲ Precautions at home and office
- ▲ Driving a 4-wheel drive vehicle
- ▲ Precautions when driving
- ▲ Procedures at checkpoints
- ▲ Reacting to the most common types of security incident
- ▲ Dealing with the military
- ▲ Dealing with rebel/irregular troops
- ▲ Radio handling and voice procedure
- ▲ Equipment that every vehicle should carry

3. SECURITY PREPARATION FOR THE FIELD

- ▲ Basic vehicle checks
- ▲ Changing a wheel
- ▲ Health and hygiene in the field
- ▲ Handling stress, including in a team context
- ▲ Programme suspension, hibernation and evacuation
- ▲ Medical evacuation

A Security Training Directory accompanies this Guide. A suggested detailed syllabus for a basic security training course is at Annex 36.

In a fast-moving emergency, there will be a limit to how much training can be provided in the field. This means that it may be very difficult to devote the time to train nationally-recruited staff in all of the above skills. The team manager's judgement will determine what topics are essential in the circumstances. He or she should ensure that enough time is set aside, with an appropriate trainer, to ensure that everyone has whatever training is necessary for their function. If there is no other option, in the last resort he or she should conduct the training, customised to the needs of the staff and the facilities available.

Unexploded shells on the ground pose a greater threat to civilians than the abandoned tank

© Sean Sutton/MAG



3.7 Briefing

3.8 Equipping

Internationally-recruited staff should either have received appropriate training before being employed, or should receive it once employed, before starting work in an insecure situation. There is often great pressure on humanitarian organisations to deploy staff quickly, and a shortage of available trained staff. Senior managers should predict their organisation's need for security-trained staff, and aim to ensure that enough staff are provided with security training in advance, to allow rapid deployment at the outset of an emergency.

See the Security Training Directory which accompanies this Guide, for information on security training providers, courses and resources.

3.7 Briefing

The aim of security briefing is to enable staff to understand the local situation sufficiently to live and work safely in it.

A security briefing should be given to all internationally-recruited staff before they travel to an insecure location. This briefing should be as thorough as possible, but usually can not be as detailed as a security briefing on the ground. It should be accompanied by at least basic written information, to remind them of points that they may not have taken in during face-to-face briefing.

On arrival, a further security briefing should be given which goes into greater detail and gives fully up-to-date information on the situation.

In addition to security training, nationally-recruited staff should receive a full security briefing before they start work.

In some circumstances it may be necessary to provide a security briefing to the family members of staff, either directly or through the staff member concerned.

A suggested checklist for security briefing is at Annex 27.

3.8 Equipping

The security equipment necessary will depend on the situation, and the type of work envisaged. A checklist of personal security-related equipment is at Annex 8. A checklist of team security equipment is at Annex 9.

3. SECURITY PREPARATION FOR THE FIELD

Both national and international staff should be provided with the equipment necessary for their security. A key item, in most contexts, is suitable vehicles. Whether owned or hired, they should be thoroughly checked by a competent mechanic, for roadworthiness and correct equipment. See Annex 42 for a suggested list of vehicle equipment.

Secure stores for equipment will be needed from the outset. Staff should be discreet about the presence of any valuable equipment.

Inventory control of equipment is necessary to reduce theft and loss – which result in considerable cost to humanitarian programmes. It is at the start of the crisis, and when the emergency is most pressing, that this issue becomes even more difficult than usual. A good system, prepared in advance, and a named staff member with the proper briefing and training, help to ensure good inventory control in even the toughest situations. Poor inventory control can have a direct impact on security, for example if vital communications equipment is lost or stolen. It is also an indicator of a poorly managed operation.

See Annex 18 for suggested inventory control procedures.

3.9 Preparing illiterate staff

Security preparation for illiterate staff should be adapted to their role, needs, skills and knowledge. Creative adaptation of training, briefing and equipping should ensure that they are well prepared to work in safety. The manager should decide which posts may be filled by illiterate staff, and which require literacy.

3.10 Preparing security-related aspects of administration

Certain aspects of administration have a bearing on security. These include:

- ▲ Creating and maintaining proper records, with copies both at Headquarters (HQ) and in the field, including:
 - Accounting records
 - Sensitive documents such as financial or personnel records
 - Up-to-date Next of Kin records
 - Copies of passports including visas
 - Copies of airline tickets

3.9 Preparing illiterate staff

3.10 Preparing security-related aspects of administration

- Health records of all staff, including blood groups
- Equipment inventory
- Full details including serial numbers of all high-value assets such as vehicles, computers and communications equipment. It may be necessary to take invoices or proof of ownership to the field, to present to customs authorities
- Staff contracts
- Other contracts
- Copies of staff driving licences
- List of addresses, phone numbers and radio frequencies
- ▲ Maintenance of up-to-date insurance (see Annex 16 for information on war risks insurance). All staff should receive a copy of the insurance policy, and understand its meaning and the level of benefits provided. Note that failure to maintain adequate insurance could lead to large claims being made against an employer, which in some cases could drive the employer into bankruptcy.
- ▲ Ensuring that recruitment and employment procedures follow all applicable laws
- ▲ Financial aspects:
 - Budgeting for security-related expenditure
 - Cash carriage and storage
 - How will money be handled? What quantity of cash will be needed, and how will it be kept safe?
 - Procedures for authorising expenditure and cash movement
- ▲ What communications equipment will be needed?
- ▲ What types and quantities of vehicles will be needed? What will they need to be equipped with?
- ▲ How many national staff drivers will be required?
- ▲ What skill and experience does the team need?
- ▲ Do any organisations need to be informed of our plans?
- ▲ What permissions do we need to obtain before deploying, or soon after deploying?
- ▲ What documents do staff members need?
- ▲ Creation of identity cards for staff, with expiry dates.
- ▲ Creation of information cards in local languages, explaining the mission and values of

3. SECURITY PREPARATION FOR THE FIELD

the organisation. These can be helpful for staff when crossing checkpoints, or meeting with local leaders or communities.

- ▲ Creation of emergency contact cards for staff, in relevant languages – see Annex 7 for an example.
- ▲ Keep track of which team members have received appropriate security training.
- ▲ Plan security briefing times for all team members and keep track of who has been briefed.

It is easy in an emergency for some of these aspects to be overlooked. Because of their potential impact on security, the manager should therefore take particular care to ensure that they are thoroughly planned and implemented. Relevant financial procedures should normally be made available to all international staff before deployment.

A critical requirement is that a properly trained and briefed bookkeeper, accountant or financial manager, appropriate to the size and type of programme, should be present from the start, including during the planning of the operation.

Annex 11 gives a basic checklist of financial security

3.11 Offices and warehouses

3.12 Staff accommodation

procedures, plus reference to further resources. Annex 21 provides a checklist on Next of Kin records. Annex 22 outlines a procedure for informing Next of Kin of an incident.

3.11 Offices and warehouses

Security at an office, warehouse or other building is made up of a number of factors including:

- ▲ General location
- ▲ Physical security of the building
- ▲ Local infrastructure
- ▲ Arrangements for receiving visitors
- ▲ Identity of the owner

Before deciding to use a building, it should be assessed for its security. For a checklist suggesting possible points to bear in mind when assessing or planning the security of a building, see Annex 1. Ensure that correct health and safety procedures are followed, particularly in warehouses.

3.12 Staff accommodation

Nationally-recruited staff may live in their own houses, or may move to live close to their work. They and their families may in some cases be attacked at their homes because of their employment. Thieves may think that they are wealthy. Violent groups may consider them a target for political reasons.

If a threat of this kind is assessed, the relevant manager should consider what help is appropriate. A simple example would be installing locks and grilles. Or it might mean giving an extra accommodation allowance. In extreme circumstances it might involve paying for the cost of relocating the entire family.

When considering accommodation for international staff, in addition to the checklist at Annex 1 it is wise to consider whether the building will be a restful or a stressful place to live. A comfortable home enabling genuine rest is important for staff efficiency, and ultimately will help the people they are trying to serve. Consider whether there is sufficient privacy, particularly if several staff will be living together.

While comfort is necessary, it is also important for

Local people benefit most from security
© Christian Aid/Georgiana Treasure-Evans



3. SECURITY PREPARATION FOR THE FIELD

3.13 Standard documents and equipment

3.14 Personal preparation

3.15 Medical preparation

international staff accommodation to be modest. If local people perceive that humanitarian staff live in luxury, paying excessive rents on unnecessarily lavish accommodation, not only will it damage the organisation's reputation but it may lead to greater insecurity for its staff, as local opinion turns against them. It is also wrong in principle for humanitarian funds to be used for unnecessary expenses.

3.13 Standard documents and equipment

It can save much time if some standard resources are available to a team when about to deploy to an emergency. They can also make security management easier. Examples of useful resources include:

- ▲ Standard contracts
- ▲ Other standard documents such as administrative procedures
- ▲ Common items of equipment, procured in advance and stockpiled
- ▲ Computer software, customised to the needs of the organisation

Some of the Annexes to this Guide may be helpful for suggestions, when designing standard documents or equipment lists for an organisation.

3.14 Personal preparation

In addition to training, briefing and equipping, staff should remember the following:

- ▲ Understand and respect the cultural and political environment in which you will be working. This may involve reading; being briefed; asking advice from nationals of the country concerned or from others who have lived there.
- ▲ Take all recommended health precautions
- ▲ Check that you have the recommended security-related equipment and are trained in how to use it

3.15 Medical preparation

Medical preparation is vital. Humanitarian staff are often exposed to serious medical hazards, some of them potentially fatal, which can usually be prevented by simple precautions.

All staff should normally undergo a medical examination before signing their contract. They should take

advice on the recommended vaccination and other medical precautions for the areas that they will be going to, and follow them scrupulously.

All staff should be aware of which local medical facilities are recommended, and which should be avoided. This implies that a qualified person should check the quality of local facilities.

Basic health and hygiene precautions greatly reduce the chances of illness. All staff should be briefed on these, and managers should check, as appropriate, that staff are taking the precautions. For a checklist of health and hygiene precautions, see Annex 14.

Decide how many staff will require first aid training, and ensure that it is carried out. The organisation should have a policy on first aid – see Annex 14. Identify what first aid kits, and other medical supplies, will be needed.

Medical evacuation (Medevac) procedures are discussed at Annex 20.

Check that appropriate medical insurance is in place. Many insurance companies have an arrangement with an emergency medical evacuation company. If your organisation has insurance providing this service, all staff should have the contact phone numbers on their person at all times. A simple way to achieve this is to print an emergency contact card with those and other emergency contact numbers, for staff to keep in their wallet or purse. See Annex 7 for suggested contents of this card.

It is good practice for staff to carry in their purse or wallet a record of basic medical data and any special medical requirements they may have, including:

- ▲ Blood group
- ▲ Allergies (e.g. to antibiotics)
- ▲ Any existing disorders
- ▲ Any medication currently being taken
- ▲ Vaccination record (note that some countries require certificates of vaccination as a condition of entry)

These details should be given both in an international language and in the local language if appropriate.

4. SECURITY MANAGEMENT IN THE FIELD

- 4.1 Revised security assessment
- 4.2 Revised security plan
- 4.3 Information-gathering

4.1 Revised security assessment

Even if a preliminary security assessment has been carried out, it will need to be updated and if necessary revised when the team deploys to the field. This is because the situation may have changed, or because the arrival of the team may itself have an impact on local perceptions and relationships, and therefore on the security of the team.

The security assessment should be further updated and revised whenever the situation demands it. Senior managers should be informed of any significant change in the assessment, and its implications for the staff and the programme.

4.2 Revised security plan

The security plan produced before deployment (see Chapter 3 above) should be reviewed in the light of experience on deployment, and modified if necessary. Annex 31 gives a suggested format for a security plan.

The security plan should be updated and modified

whenever required. Where possible, it should be the product of consultation with both national and international staff. This encourages a sense of ownership of the rules and procedures contained in the plan, and increases the willingness of staff to follow it, even when that may be inconvenient.

All literate staff should receive a copy of the security plan on their first day at work, as part of their initial security briefing. They should be required to read it immediately, and should receive any help they may need to understand it.

It is good practice to require staff to sign a statement within their first 24 hours in the field, that they have received a security briefing, have read and understood the security plan, and agree to follow it. Without such a system, many experienced managers report that new staff sometimes do not receive a security briefing on time, or do not actually read the security plan. This method also sends a signal that security is to be taken seriously, and produces a record for accountability purposes.

If staff begin to ignore a security rule or procedure within the plan, it may be because it is unrealistic and needs to be changed, or because they have not understood the reason for it, or because they do not feel sufficiently responsible. Whatever the reason, consulting them will help to identify the right course of action, whether it is to modify the plan or to keep it as it is while explaining the need for it and encouraging staff to take it seriously. Staff should understand that unless and until the plan is modified, failure to follow it is a disciplinary offence.

4.3 Information-gathering

Being well informed is one of the keys to security. This applies at every level: all staff should be aware of what is going on around them. Those responsible for the management of security should be especially well informed. Sources of information and topics of interest are similar to those given for a security assessment at Annex 26.

Both national and international staff should gather information and feed it into the team. National staff

During a crisis people need information – and aid agencies do too
© Jan Davis, RedR



4. SECURITY MANAGEMENT IN THE FIELD

are likely to have many sources of information that are not available to international staff. Regular information-sharing forums normally operate when there is more than one humanitarian organisation in the location: security-related information should be methodically shared and discussed at these.

Managers should disseminate security-related information to colleagues on a regular basis. A simple method is to include a short security update in all briefing meetings and in all reporting formats. Staff working in remote locations should also be kept up to date, and should supply the field office with any security-related information they themselves have received.

4.4 Relations with the local population

Relations with the local population, and any other local residents such as refugees, are probably the most important of all security measures. A detailed knowledge of them is vital for good humanitarian assistance, and for security. Relationships with leaders of all significant groups, and with ordinary people of all types, greatly increase the ability of organisations to meet humanitarian needs, and to do so in a way that is safe both for local people and for humanitarians.

Managers and their staff should normally spend a considerable proportion of their time meeting and talking with a representative variety of local people. There are many ways of doing this. Some of the most commonly used ways are:

- ▲ Regular conversations with nationally-recruited staff
- ▲ Regular meetings with local leaders of all significant groups
- ▲ One-to-one conversations with a balanced selection of leaders
- ▲ Random visits to homes in a variety of geographical areas, if appropriate in the local culture
- ▲ Visiting people living away from major towns, and away from major roads. (There is a tendency for busy humanitarian staff to visit people near easily accessible towns and routes far

4.4 Relations with the local population

4.5 Relations with other organisations

- more than those in areas off the beaten track.)
- ▲ Visits to religious leaders
- ▲ Attendance at social occasions, when invited
- ▲ Visiting areas inaccessible to vehicles, on foot if necessary
- ▲ Discussing and sharing information with other humanitarian organisations
- ▲ Reading local press and listening to local radio and TV

The pressures on a humanitarian manager's time are such that it is often difficult to visit local people as much as would be ideal. But it is essential that at least a basic minimum of visiting and discussion takes place. If it does not, the risks to programme quality and to security are likely to rise.

Nationally-recruited staff are a major source of local knowledge and opinion. Their advice should normally be asked on all significant programme and security decisions, unless to do so might place them or others in unacceptable danger. But the views of nationally-recruited staff are unlikely to be sufficient. They will not be able to represent the wide variety of perspectives held by different groups of local people. It also depends for each staff member on:

- ▲ The access they have to information about security (through friends, family, other contacts)
- ▲ Their ability to analyse this information to identify what may be important for you
- ▲ Their willingness to share this information

There is therefore no substitute for speaking with local people who have no connection with humanitarian organisations.

4.5 Relations with other organisations

(a) Local authorities

Humanitarian agencies normally establish early contact – preferably before deployment – with the government or other authorities of the area where they are working. The reasons for this include:

- ▲ Explanation of the organisation's role, to ensure that it is understood and not confused

4. SECURITY MANAGEMENT IN THE FIELD

- with any non-humanitarian organisations
- ▲ Making clear the humanitarian principles on which the organisation's work is based
- ▲ Explaining that donor interest is also a major factor in determining which programmes are run, and even whether the organisation can continue its presence in the area
- ▲ Increasing the organisation's security by winning greater acceptance for its work
- ▲ Obtaining any necessary permissions
- ▲ Establishing a mutually respectful relationship which may be helpful if lobbying is needed in future
- ▲ Obtaining any relevant information on the general situation

(b) Local security forces

It is often helpful to make contact with the security forces in the area (either military or police or both), for the following reasons:

- ▲ To explain the organisation's role, thus preventing any damaging misunderstandings
- ▲ To make clear the humanitarian principles on which the organisation's work is based
- ▲ To obtain their contact information, in case it becomes necessary to contact them in an emergency
- ▲ To obtain any necessary permissions
- ▲ To establish a mutually respectful relationship which may be helpful if lobbying is needed in future
- ▲ To obtain any relevant information, including on the levels and types of insecurity in the area

Humanitarian organisations should ensure that their contacts with the authorities, and especially with security forces, do not compromise their independence – either real or perceived.

If there is more than one security force, perhaps on different sides of a conflict, the team leader should decide whether to establish contact with all security forces, to show transparency and impartiality, or whether there is a good reason to avoid contact with one or more of them.

In cases where the security forces are oppressing the

4.5 Relations with other organisations

population or are unpopular for other reasons, local people should be given no reason to suspect that a humanitarian organisation is close to, collaborating with or tacitly supporting the security forces. In these cases it is usually wise to avoid frequent meetings, social contact, joint statements or any other activity with security forces which could cause misunderstandings – since misunderstandings of this kind could be very dangerous for the humanitarian organisation.

Humanitarian organisations are subject to the laws of the country in which they are present. Unless there are overriding reasons to disobey an unjust law, it is important that humanitarian organisations are rigorous in observing the law. This is not only right in principle; it can also help to protect the organisations from trouble including criticism, detention, harassment, attack or expulsion from the country.

There may be cases when the government or other authorities are committing crimes of such seriousness that humanitarian organisations decide to denounce them publicly. Public denunciations can have major consequences for the organisation making them, including sometimes severe consequences for the security of their staff. It can have an equally great impact on other similar organisations in the area – even those which have decided to stay silent. Any organisation intending to make critical public announcements should think through these potential consequences beforehand, and should wherever possible inform and consult those organisations likely to be affected.

(c) Other humanitarian organisations

Good relations with other humanitarian organisations in the area can help to enhance security, for at least the following reasons:

- ▲ Information-sharing: this is an important aspect of good security management. If possible, a systematic collation of security-related information, including security incidents, should be organised on a collaborative basis by humanitarian organisations. An inter-NGO security office may sometimes be helpful, along

4. SECURITY MANAGEMENT IN THE FIELD

- the lines of the recent Afghanistan NGO Security Office (ANSO).
- ▲ Discussion of security issues
 - ▲ A common position can sometimes be helpful on matters of principle or practice
 - ▲ Some organisations may be willing to share assets that are helpful to other organisations – for example, a radio network or the advice of a security advisor
 - ▲ Some organisations may have access to influential figures, including authorities, which could be used for the benefit of all humanitarian organisations

General humanitarian coordination meetings often include a discussion on major security issues. In some cases NGOs organise their own regular meetings to discuss security issues. Participation in such meetings is to be encouraged, for the reasons listed above. The meetings need to be frequent enough to be effective, yet not so frequent as to overload busy managers. They need to be skilfully chaired to ensure that discussions are efficient.

While good relationships with other organisations can be very helpful, it should remain clear that each organisation is responsible for its own security. Any lack of clarity about where this responsibility lies can be dangerous.

(d) The UN security system

In many humanitarian emergencies the United Nations plays a pivotal role in security management. Its resources and status often enable it to make available a security officer, a dedicated security radio channel, information, or other resources for the use of the whole humanitarian community.

Many NGOs cooperate with the UN on security matters, exchanging information and informing each other of security plans. It is therefore helpful for all humanitarian organisations to be aware of the UN security system. It is described at Annex 40.

(e) International military forces

In cases where a properly mandated international military force is present on the ground, it will usually be necessary for humanitarian organisations to have

4.5 Relations with other organisations

a means of dialogue with the force. At the simplest level, this may be only for information exchange, allowing the two sides to explain their role and activities. For the humanitarian agencies, such contact is often a useful source of information on the security situation.

Humanitarian organisations should take care that their contacts with any military force are not perceived as compromising their independence and impartiality. In most cases this will probably mean that contacts with any military body should have a low profile. Humanitarian organisations will wish to keep a distance from a military force, in order to maintain and demonstrate their independent humanitarian mission. Beware of giving or receiving information that is more than general in nature: the distinction between information and military intelligence can be a fine one, and it is important that there is no suspicion that you are involved in military intelligence.

If an international military force is or has been a belligerent in the conflict, or is perceived as such, the need for distance is still greater. However, some level of contact with or representation to them is likely to be desirable, to explain your position and, where necessary and appropriate, to remind them of their duties under international law.

Some humanitarian organisations believe that military forces should never provide any humanitarian assistance, or support to humanitarian organisations, on the grounds that this compromises humanitarian independence and confuses the military and humanitarian roles in the minds of the local population. Others believe that, in cases where humanitarian organisations are overwhelmed by serious need, it may be right for the military to support the humanitarian effort in order to save life and prevent suffering. The majority view is that military forces should only help with a humanitarian effort in urgent, life-saving situations where humanitarian organisations are not able to meet the needs.

Serious problems can sometimes arise because of a lack of understanding between military and humanitarian bodies. Humanitarian organisations which

4. SECURITY MANAGEMENT IN THE FIELD

4.5 Relations with other organisations

refuse any contact with the military may deprive themselves of important security information, and run into dangers that they could otherwise have avoided. The military may also see them as biased. Military personnel who act without regard for humanitarian organisations may endanger them, for example by wearing civilian clothes while carrying weapons, and calling themselves 'humanitarian' when meeting local people – thus causing confusion between military and humanitarian personnel and provoking attacks on the latter.

For all the above reasons, each organisation should give guidance on dealing with the military, in its security policy. See Annex 32 for a suggested format for a security policy.

If the military do provide support to the humanitarian effort, it should be:

- ▲ Defined in advance
- ▲ Clearly in support of humanitarian organisations
- ▲ Ideally provided at the request of the humanitarian organisations

This will help to reduce the risk of compromise and confusion, but will probably not eliminate it.

Whether humanitarian organisations request assistance from the military will depend on the circumstances, the level of and type of needs, and their capacities to meet that need. Local people's perceptions of the international military force will be an important factor, bearing in mind that those perceptions might change rapidly in future, if for example the military is required to take action which is unpopular.

International military forces have assisted humanitarian programmes in a number of crises, for example with:

- ▲ Rapid construction of refugee camps and associated facilities
- ▲ Protection of convoys
- ▲ Providing area security

- ▲ Responding to emergency security needs
- ▲ Logistics and transport assistance
- ▲ Mine clearance
- ▲ Immediate life-saving assistance during overwhelming crises, if humanitarian organisations do not have the capacity to meet the need

The UN has a procedure for deciding whether to make use of military assets in support of a humanitarian organisation. Among other criteria, using military assets should be:

- ▲ The option of last resort, indispensable and appropriate
- ▲ Not used if the offering military force is a belligerent in the conflict
- ▲ Limited in time and scale
- ▲ Not direct assistance to the population, if possible
- ▲ Assessed for its likely impact on the security of humanitarian personnel
- ▲ Assessed for its likely consequences for beneficiaries, other humanitarian actors, and humanitarian operations in the medium to long term
- ▲ Under military control, but the operation as a whole must remain under the overall authority and control of the responsible humanitarian organisation

For the full procedure and criteria, see the relevant UN document³.

(f) International police force

An internationally-mandated police force may in some cases have an executive policing role, providing police services directly to the public. Often it has no executive role, but may have – for example – a supervisory, monitoring, advisory or training role.

If the international police force has an executive role, humanitarian organisations will normally wish to make themselves known to the force, in case they need to call on them during an emergency. They should inform them of the locations of all offices and houses, so that if they need to call for urgent help, the police can find them quickly.

A common problem is for humanitarian locations, as

³ Guidelines on the use of military and civil defence assets to support United Nations humanitarian activities in complex emergencies, UN, March 2003, available online at <http://ochaonline.un.org/DocView.asp?DocID=426> or using a search engine.

4. SECURITY MANAGEMENT IN THE FIELD

4.5 Relations with other organisations

recorded by the police, to become out of date as organisations move offices and rent new houses, forgetting to inform the police of the changes. A named staff member should therefore be made responsible for keeping the police, and any other relevant bodies, updated on current locations.

If the international police force does not have an executive role, there may be little need for humanitarian organisations to be in contact with them unless the local police fail in their duty.

(g) Embassies

Staff of humanitarian organisations are advised to register their presence with their home country's local embassy. This is particularly helpful if embassies might have a role in providing consular protection services for their nationals, or in arranging evacuation if the security situation demands it. Embassies sometimes act as assembly points prior to an evacuation of their nationals. If so, assess it to ensure that it is an appropriate location: sometimes they are targets or the scene of rioting. Newly arriving staff should routinely be reminded by their manager to register with their embassy.

Contact with local and international security forces can be helpful. Humanitarian organisations should ensure that such contact does not compromise their independence. © RedR



In some cases contact with embassies may need to be low profile, especially if the embassy represents a country which has a partisan agenda in the area, or is perceived to have one.

(h) Donors

In general, donors do not provide direct security assistance other than funding for security measures. Direct contact between a field operation and a donor on security issues is therefore unlikely to be necessary while the operation is ongoing.

Donors' requirements on 'visibility' and its security implications are covered in the section "Visibility and security" below.

(i) Local partners

Many humanitarian organisations have partnerships with local bodies such as local NGOs, religious groups or community associations. Those organisations are usually responsible for their own security, since they remain independent while engaged in a partnership arrangement.

When negotiating the partnership agreement, both parties should consider what security implications there may be, if any. It may be that one or both sides will encounter greater or new types of insecurity as a result of entering into the agreement. The parties should agree any security measures at this stage, including any necessary training, briefing, equipping and funding.

These security measures may delay the start of partnership activities, leading to a temptation to cut corners. While emergency programmes should be launched as rapidly as possible, this should not be at the price of unacceptably high risk to life and property. This is a matter for managers' judgement in each case.

It will often not be necessary for local organisations to have the same security rules and procedures as international organisations. Different security measures are usually appropriate, since they belong to the culture, have great local knowledge, language and experience, and are well connected locally. In some cases, however, similar security measures

4. SECURITY MANAGEMENT IN THE FIELD

may be required. If so, they should not be overlooked.

(j) Security coordination between humanitarian organisations

Coordination with other humanitarian organisations is an important part of good security management. The actions of one can have an impact on the security of the others. Local people often draw little distinction between one humanitarian organisation and the next. All humanitarian staff should therefore strive for good coordination, so far as the situation and the mandate of their organisation allow.

Coordination on security can promote the following effects:

- ▲ Sharing information
- ▲ Agreeing common policy and practice, particularly on issues such as
 - Interfacing with military and belligerents
 - Use of armed guards
 - Use of private security companies
 - Salary and fee levels for services
- ▲ Sharing security training (two or more organisations can pool resources to carry out training, or the security officer of one organisation can train inter-agency groups)
- ▲ Learning from each other's experience and good practice
- ▲ Understanding the local situation better, resulting in fewer security-related errors
- ▲ Solidarity between humanitarian organisations, which can have further beneficial effects on the effectiveness of programmes
- ▲ Any organisation with particular weaknesses can receive friendly advice or warnings from stronger organisations
- ▲ Any organisation with particular strengths can have a positive influence on the whole humanitarian community in the area

Coordination on security often takes one or more of the following forms:

- ▲ Information-sharing meetings
- ▲ Liaison with a nominated security officer or security advisor (often the UN security officer)

4.6 The Field-Headquarters relationship

- ▲ An NGO security organisation. A recent example is ANSO, the Afghanistan NGO Security Organisation, which provides training, information, analysis, practical advice and coordination to the NGO community in Afghanistan. The model is being adapted for use in other countries.
- ▲ A dedicated security radio channel
- ▲ Regular radio checks for all humanitarian personnel
- ▲ Coordinated contingency plans
- ▲ Coordinated evacuation
- ▲ Joint lobbying of local authorities or other leaders
- ▲ Collocation of offices or accommodation
- ▲ Sharing of the costs of coordinated security measures, for example patrols by a private security company or the local police

Even though they coordinate, each humanitarian organisation remains autonomous, responsible for all of its security decisions. These will sometimes differ between organisations. It may be that some organisations decide to evacuate, for example, while others decide to remain. If possible, important security decisions should be taken after frank discussion between the organisations, to ensure that all are basing their decision on the fullest possible information.

4.6 The Field-Headquarters relationship

It is vital that the security-related responsibilities of HQ and field managers are clearly defined. The security policy should set out the responsibilities of each, and the limits of those responsibilities.

Security management should normally be delegated to the field manager, since he or she will have the best knowledge of the situation and will therefore be best placed to make good, timely decisions.

A relationship of confidence between HQ and the field will promote good security management. The field should keep HQ well informed of the situation. The HQ should support the field manager, providing good quality staff and other resources needed to manage security well. HQ managers should visit the

4. SECURITY MANAGEMENT IN THE FIELD

4.7 Reporting

4.8 Security aspects of programme design

field often enough to appreciate the situation, without burdening field staff unduly.

HQ managers should trust the field manager to make good decisions on security. In most cases the decision of a competent manager on the ground is likely to be better than a decision coming from a distant HQ. The field manager has more detailed and more current information, and can assess a number of intangible factors that may be impossible to report to HQ. As a general rule, HQ should aim not to overrule field managers on security issues, especially decisions to evacuate.

On the other hand, field managers can and sometimes do make mistakes. An alert manager at HQ should aim to discern when a mistake has been made, and should overrule if failure to do so is likely to threaten the safety of staff, local people or property. HQ managers will be more able to make these judgements, and will have more credibility in the eyes of their staff, if they themselves have had significant field experience during emergencies.

4.7 Reporting

Good reporting enables managers to make informed decisions, including decisions about security. It also helps accountability, by providing a record of what information is available and what decisions are made. This can protect both staff and managers in the event of an investigation.

The following types of report are commonly used:

- ▲ Situation reports (usually known as sitreps)
- ▲ Incident reports

Regular sitreps provide managers and other colleagues with important information that they need to do their job. The frequency of sitreps is for organisations to decide and will depend on the situation: daily sitreps may be needed at the start of a crisis, reducing to weekly, fortnightly or even monthly sitreps once the situation has stabilised. When circumstances demand it, a special sitrep is sent, to update managers or colleagues at a moment when no regular sitrep is due.

Sitreps should provide a concise, accurate snapshot of the current situation. Each significant aspect should be described. Often a single summary sentence can encapsulate the current status of one particular aspect of the situation. Each organisation will have a different view on the length and detail of sitreps, although in general short sitreps are preferred during emergencies. Longer sitreps are sometimes not read by busy staff.

It is helpful if sitreps have a standard format. This saves time and ensures that all topics which the organisation thinks vital are covered. It also allows flexibility, since additional topics may be added by the sitrep writer. A suggested format for a sitrep is at Annex 34.

For a suggested format for incident reports, see Annex 29.

Especially during a conflict, careful judgement is necessary to decide what information about the conflict should be included in reports. In general it is best not to include information which could be misunderstood by the authorities, could endanger staff or local people, or could result in accusations of spying or other offences. If it is vital to pass on such information, it is better done face to face, with no written record held in the country concerned.

Report writing is an important skill. Managers should ensure that this skill is nurtured among staff who have to write reports. Training in report writing should be provided when necessary.

4.8 Security aspects of programme design

When designing programmes or projects, consider the security aspects. These may include:

- ▲ How will the project or programme be designed? Will local people and/or respected leaders be involved in the design? (The Code of Conduct⁴ says that beneficiaries should be involved in the management of relief aid.)
- ▲ How will people be informed of the project or programme?
- ▲ Will local people have a means of making com-

⁴ Available at <http://www.ifrc.org/publicat/conduct/code.asp>.

4. SECURITY MANAGEMENT IN THE FIELD

- ments or complaints during implementation? How will these be handled?
- ▲ Might any groups of people misunderstand the plans, and gain false expectations of receiving aid? How could these expectations be managed?
 - ▲ Might your plans undermine or strengthen someone's power base? Who will gain and who will lose out, as a result of your plans?
 - ▲ Might any groups oppose the plans?
 - ▲ Will your plans be seen as fair and impartial?
 - ▲ What possibilities will there be for fraud or diversion of aid? How could these be guarded against?
 - ▲ How could false allegations, or the perception of fraud, be averted?
 - ▲ Will any goods or cash need to be secured?
 - ▲ Will any goods or cash need to be transported securely?
 - ▲ Will particular goods or assets required for the programme pose a valuable target for thieves, criminals or parties to a conflict?
 - ▲ What types of evaluation or audit will be needed?
 - ▲ Might the project or programme affect the security of beneficiaries, or other local people, or your organisation, or other organisations?

All minefields should be clearly marked – but they often aren't
© Sean Sutton/MAG



4.9 Routine security management

How will other organisations be informed of the plans? Will they have a chance to comment or advise on the plans before they are finalised, and in time for plans to be changed if necessary? (They may point out security or other issues which you are not aware of.)

- ▲ Will the plans need to be coordinated with other organisations' plans, from a programme or security point of view?

4.9 Routine security management

(a) Teamwork

Every member of the team should feel a responsibility for security. All appropriate staff should be involved in contributing to good security procedures. Discipline and mutual support are needed. Managers should build up team spirit, and demonstrate that they care for its safety.

Since the security situation evolves over time, and since staff come and go, security updates should be included regularly in staff meetings. Managers should consult the team when they reassess the security situation and when considering any changes to procedures. It may be helpful to delegate some specific security-related functions to one or more team members, while retaining overall oversight and responsibility.

Depending on the circumstances it is often wise to practise some security procedures as a team. Examples could include:

- ▲ Reaction to armed robbery attempt
- ▲ Passing through a checkpoint
- ▲ Sending an incident report
- ▲ First aid procedures
- ▲ Procedures for entering and leaving a house by car
- ▲ Fire drills

(b) Staff behaviour

The behaviour of humanitarian staff, both on and off duty, gives important signals to local people. If staff are consistently considerate, modest and interested in local people, that will promote the organisation's acceptance among those people. If staff appear arrogant, rude, immoral by local standards,

4. SECURITY MANAGEMENT IN THE FIELD

4.9 Routine security management

or express sympathy with one party to the conflict, the organisation's acceptance will diminish and so will its level of security. Annex 5 demonstrates the importance of cultural awareness.

Managers should explain these issues to staff as often as necessary, monitor staff behaviour and correct it when required.

Other points for staff to bear in mind include:

- ▲ Be friendly, respectful and tactful when meeting people. Get to know the culturally acceptable styles of greeting and conversation. Learn as much as you can of the language. Even a few words of greeting in the local language can make a big difference.
- ▲ Dress appropriately, bearing in mind the local culture.
- ▲ Build good relationships with local people, making sure that you show no bias towards one group or another. Get involved in community activities outside work.
- ▲ Respect security procedures in a methodical and disciplined manner. Use initiative and common sense if the situation demands it.
- ▲ Be aware of your surroundings and stay alert. Be suspicious of anything out of the ordinary.
- ▲ Check that you have and carry the recommended security-related equipment.
- ▲ Keep communications equipment well maintained and within reach.
- ▲ Vary the routes that you take to and from work, and the timing of your journey.
- ▲ Depending on the local situation, it is often good practice to lock the outside doors to your accommodation as darkness falls.
- ▲ Beware of common criminal tactics:
 - Keep your belongings with you and in view at all times – "A fool and his luggage are soon parted"
 - Carry bags in a secure manner
 - Do not accept 'sweets' or food from strangers in case it is drugged
 - Beware of jostling in a crowd, or being distracted by one person while his accomplice tries to pick your pocket
 - Do not accept lifts from strangers
- Avoid walking at night, or near bushes, dark doorways and other places of concealment. Keep to well-used roads
- If asked for directions by the driver of a vehicle, do not approach the vehicle. A common criminal technique in some contexts is to ask a potential victim to come closer to look at a map.
- If you think you are being followed, cross the road. If the person follows you, cross it again. If you are still worried, go at once to a place where there are lots of people, and tell someone what is going on
- Consider carrying a torch or whistle, or better still a very loud alarm
- Use an outside light when answering the door at night to illuminate your visitor. Do not turn on the interior light.
- ▲ In a hotel, consider staying on an upper floor if ground floor windows are accessible from the outside. Keep balcony doors and windows locked. Do not leave your key where someone can note your room number
- ▲ Lock your hotel room door even when you are inside the room. Use the chain on the door if you are not expecting a visitor.
- ▲ Avoid inappropriate sexual behaviour (e.g. use of prostitutes; sexual activity with those under the age of 18; sexual relationships with beneficiaries; other behaviour which is contrary to local customs).
- ▲ Be aware that drugs added to drink are sometimes used by criminals, who intend to commit theft, rape or other crimes. When at a bar, club or party, never leave your drink unattended, even when going to the toilet. If appropriate, nominate a friend to watch the drinks. Never accept a drink from someone you do not completely trust. If you begin to feel really drunk after only a drink or two, seek help from a trusted friend, who should get you to a place of safety as soon as possible. Remember that non-alcoholic drinks such as tea or coffee can also be targeted.
- ▲ Follow the Red Cross/Red Crescent/NGOs Code of Conduct⁵.
- ▲ Respect local laws.

⁵ Available at <http://www.ifrc.org/publicat/conduct/code.asp>.

4. SECURITY MANAGEMENT IN THE FIELD

4.9 Routine security management

- ▲ Don't request or accept personal favours of any kind from contractors
- ▲ Don't misuse the resources of your organisation
- ▲ Take all recommended health precautions.
- ▲ Keep fit and healthy.
- ▲ Take proper rest and eat properly.
- ▲ Do not use illegal drugs.
- ▲ Drink alcohol, if it is legal, only in moderation.

(c) Female staff

In many situations, women can be at risk from different or greater threats than men. The following personal security advice is likely to be applicable to all staff, but may be especially helpful to women. You should use your judgement as to which of them are applicable in your situation:

Some suggestions follow⁶:

- ▲ Know where you are going, and look as though you know where you are going. If you look confident (even if don't feel confident), you are less likely to appear vulnerable to attack.
- ▲ In public, dress and behave in an unobtrusive manner, bearing in mind local culture and gender roles. This does not necessarily mean international staff adopting local patterns of dress and behaviour, but acting in a manner that is seen by local culture as acceptable for expatriates, taking into account the expatriates' culture and the needs of their work. It can be a difficult balance to strike.
- ▲ If meeting someone you don't know well, inform a colleague of your plan. Consider meeting him/her in a public place where there will be other people.
- ▲ When meeting people, if there is any risk of misunderstanding about your intentions, speak up and communicate your wishes clearly.
- ▲ Listen to your instincts. If you are unsure about a location or a person, leave immediately.
- ▲ Do not use taxis unless the taxi driver and/or the taxi company is known and trusted. Agree the fare before beginning the trip.
- ▲ In many situations it may not be advisable to walk alone, or drive alone, particularly at night.

(d) Rest and Recreation (R&R)

During a high-pressure operation, staff are likely to need regular Rest and Recreation (R&R). Its purpose is to help prevent stress or illness, and to improve efficiency. R&R usually involves a staff member leaving the operation for a number of days, going to a location that is near enough to be inexpensive, but far enough from the operation to allow a sense of distance and freedom from pressure.

See Annex 25 for further discussion of R&R.

(e) Stress

Staff should be aware of the dangers of excessive or prolonged stress, and watch for signs of it in their colleagues. People suffering from stress are likely to manage their security less well, increasing the risks for themselves and their colleagues. Managers should aim to prevent excessive stress, and to spot early on when a colleague is suffering from it.

Be aware of the need to monitor your own stress levels and be prepared to acknowledge and do something about excessive stress. This is not only important for you but also your colleagues who may be relying upon you to perform well.

Different types of staff may show different signs of stress, because of cultural or personality differences. Their families may also be affected. Managers should set up work and living arrangements in such a way as to minimise stress and its effects. See Annex 35 for more details on prevention, diagnosis, treatment and management of stress.

(f) Discipline

At times it may be necessary to take disciplinary action against a staff member on security grounds. If a staff member causes a serious breach of security, or persists in insecure behaviour after being warned, formal disciplinary action is likely to be the most effective way to correct the behaviour and protect the team. Managers should not hesitate to take disciplinary action, up to and including dismissal, if the situation requires it.

(g) Checkpoints

Checkpoints are widely used in many countries.

⁶ Adapted from UNSECOORD/UNHCR *Security Awareness – An Aide-Mémoire*, 1995

4. SECURITY MANAGEMENT IN THE FIELD

4.10 Technical issues

Many checkpoints have a legitimate purpose, for example to prevent weapons from entering an area. Some checkpoints have little purpose other than to harass. Some checkpoints are used – for example by bandits or undisciplined soldiers – as a cover for ambush, theft or violence.

Staff should be trained and briefed on how to handle themselves at checkpoints. The best approach may vary from situation to situation. See Annex 2 for suggested checkpoint procedures.

(h) Weapons

Humanitarian staff should not carry weapons. Carrying a weapon is likely to damage the organisation's credibility as a neutral and humanitarian body. It may also increase the risk of violence, since someone with a weapon can be seen by armed groups or individuals as a threat, and since a weapon may be taken from you and used against you. Remember that a cosh, machete or stick is a weapon.

Humanitarian staff should never handle a weapon, even if simply offered the chance to hold one for a few seconds. All kinds of firearms, guns, mines,

grenades etc can fire or explode if not correctly handled by a trained person. Some may be booby trapped. A photograph of an aid worker holding a weapon could be used to damage your standing in the local community.

Aid workers have been known in the past to keep a firearm "under the bed just in case" without having consciously thought through the implications for themselves and their colleagues. If this may be a temptation for some staff, the field manager should consider explaining to the team the risks of possessing a weapon.

4.10 Technical issues

(a) Telecommunications

Communications equipment does not provide security. It is an aid to security, if properly used. The leader of a field team should ensure that the team's communications requirements are thought through in good time to allow the despatch of any vital equipment with the team as it deploys.

It is good practice, in insecure situations, for staff to have two independent means of communication (e.g. radio and satellite phone), so that if one breaks down communication will still be possible. In particular, avoid dependency on mobile phones. In a crisis a cellular telephone system is particularly vulnerable to becoming overloaded, damaged, or simply switched off by a belligerent.

Useful equipment may include:

- ▲ Hand-held radios
- ▲ Vehicle radios
- ▲ Base station radios
- ▲ Repeater stations (it may be possible to share repeater stations with other organisations)
- ▲ Satellite telephones
- ▲ Fax machines
- ▲ E-mail accounts, accessories and software
- ▲ Landline telephones
- ▲ Cellular (mobile) telephones
- ▲ Any necessary accessories, including battery chargers

Strong relationships with local leaders are vital for good security
© Christian Aid/Peter Graystone



4. SECURITY MANAGEMENT IN THE FIELD

4.10 Technical issues

From a security point of view, key questions requiring decision include:

- ▲ Who needs to be able to contact whom, and with what degree of reliability?
- ▲ Is it necessary to employ one or more dedicated radio operators, to ensure that someone is listening to the radio base station at all times, or during certain hours?
- ▲ Who will be 'on call' at all times in case of emergency? Is a duty officer system required, both at HQ and in the field, where several staff members rotate as the 'on call' person? Or should the manager (or a delegated colleague in the manager's absence) always be the 'on call' person?
- ▲ Do you need communications that will give an instant response? Do you need one person to be able to talk to several others at once (radio) or is one to one contact enough (phones)?
- ▲ What communications do other humanitarians in the area use, and do you need to be in contact with them?
- ▲ Is the use of certain kinds of communication equipment perceived as suspicious or a threat by any group? If so, how can you reduce or remove this suspicion?

Answers to the above questions will depend on the assessed threat. In most situations, it is not thought necessary or cost-effective to have all members of staff in constant contact, using mobiles phones or radios, though if this is necessary then it should be provided. The manager should decide on the basis of the likely threat to each staff member, regardless of whether they are national or international staff.

In many countries there is a legal requirement to obtain a licence to use radios that are capable of transmitting. Check the local regulations and abide by them. Some countries forbid NGOs to operate radios or satellite telephones.

Technical assistance will be needed to set up and programme radios. Check whether such assistance is available locally. If so, consider whether it would be safe to rely on local technicians, who may become suddenly unavailable in a crisis. It is also important to be confident that they can be trusted with the

knowledge of your communications arrangements: for example, could local military groups pressurise them into revealing sensitive information about your organisation?

Communications equipment is valuable and portable, attractive to thieves. This should be borne in mind when deciding where to locate communications equipment. Normally staff should sign for receipt of their communications equipment, and be held responsible for its safekeeping.

Staff should be trained to use all types of communications equipment that they may need to use. Remember that in a crisis the staff who are most skilled in using the equipment may not be available.

Annex 24 gives an introduction to basic radio use, and sources of further help.

No communications system is fully secure. All staff should be aware of the need for information security, and the risks that can arise from interception of communications. See Annex 15 for a discussion of information security.

(b) Vehicles

In most situations vehicles are an important aid to security. Vehicle management is therefore important, and should include:

- ▲ Maintenance
- ▲ Adequate fuel stocks
- ▲ Keeping all vehicle tanks at least half full
- ▲ Motor insurance
- ▲ Recruiting, briefing and managing good drivers
- ▲ Enforcing safe and considerate driving habits
- ▲ Enforcing the wearing of seatbelts
- ▲ Daily vehicle checks
- ▲ Vehicle log books
- ▲ Awareness of local driving rules and customs
- ▲ Always park facing outwards, to enable a quick departure
- ▲ A policy on carrying hitch hikers or other passengers
- ▲ A policy on whether military personnel, and/or weapons, may be carried

4. SECURITY MANAGEMENT IN THE FIELD

4.11 Administrative issues

- ▲ Training on vehicle-related security procedures including checkpoints, ambush, action in the event of an accident, under-vehicle search for bombs (in some contexts), etc

If possible, vehicles should be of a type and colour that cannot be confused with military, police or government vehicles. They should be clearly identified as belonging to a humanitarian organisation unless, in a specific context, it is assessed as safer for a vehicle to blend in with other vehicles and appear to be a normal civilian vehicle.

A list of possible vehicle equipment is at Annex 42.

Armoured vehicles are used by some humanitarian organisations, in extreme cases. They are expensive, heavy and require special training to drive. Most civilian armoured vehicles provide protection against only a limited range of threats. In most cases such vehicles are not necessary, and if they are necessary it may be best not to work in that area at all. Seek experienced advice before deciding to procure them.

(c) Guards

Guards are often needed at accommodation, offices and warehouses. Guards need careful briefing, equipping and strict management. Their instructions should be clear. Procedures should be in place for when a guard falls ill, or does not appear for duty, to ensure that buildings are never left unguarded. Annex 13 contains points to bear in mind when managing guards.

In some situations it can be appropriate to use private security companies. They may reduce the administrative and management burden and ensure continuity of cover. But there may be disadvantages or even dangers in using them. See Annex 13 for a discussion of the advantages and disadvantages of using private security companies.

In exceptional cases, armed guards may be necessary and appropriate, if there is no other way to protect life and property adequately. Annex 13 contains some points to bear in mind when considering the use of armed guards.

(d) Fire safety

Although fire safety is usually seen as a health and safety rather than a security issue, it would make no sense to manage security well without taking sensible fire precautions.

All buildings should be checked for fire safety, including ensuring that staff can exit easily. Simple fire safety measures such as smoke detectors and fire extinguishers save lives. See Annex 12 for suggested fire safety procedures.

4.11 Administrative issues

(a) Financial security

During a fast-moving emergency it is particularly easy for good financial procedures to be overlooked. This has often led to fraud, theft or mismanagement involving large sums of money. These problems can be greatly reduced by insisting on sound financial procedures from the start. The procedures should be simple, and designed so as not to impose delay on emergency programmes. If they do cause delay, field staff are more likely to ignore them.

A critical requirement is to ensure that a properly trained and briefed bookkeeper, accountant or financial manager, appropriate to the size and type of programme, is present from the start, including during the planning of the operation.

See Annex 11 for further information on financial security procedures.

(b) Information security

Humanitarian organisations need to store and transmit sensitive information. Examples may include:

- ▲ Financial records
- ▲ Requests for money transfers
- ▲ Information on persecuted individuals or groups
- ▲ Records of human rights abuses or war crimes
- ▲ Plans concerning staff movement through insecure areas
- ▲ Assessments of the political or security situation
- ▲ Personnel files

4. SECURITY MANAGEMENT IN THE FIELD

4.11 Administrative issues

Sensitive information should only be stored or transmitted if it is necessary to do so, in line with the organisation's mandate and programme. Holding or sending unnecessary sensitive information can place the organisation at greater risk. There have been cases of humanitarian staff being imprisoned for long periods because they were found with information on military movements or other subjects deemed to be incompatible with a humanitarian mandate.

Transmitting sensitive information brings added risks of it falling into the wrong hands. In many humanitarian crises, it would be surprising if all communications were not monitored by the authorities. Some organisations consider that the risks are so great that the team leader must authorise each communication before it is sent. Others rely on good training and briefing. Whichever procedure is adopted, all staff should understand that no communication system is totally secure, and be disciplined in following procedures. The most sensitive messages may in some cases have to be communicated face to face, and not entrusted to e-mail, fax, phone, radio or letter.

Normally, staff should be aware of sensitive information only on a 'need to know basis', meaning that a given piece of information is only shared with those staff who need to know it. In this way, other staff are protected, and the risk of information loss is reduced.

Files or computers holding sensitive information should be kept in rooms where visitors do not have access. Passwords should protect all computers. When travelling, staff should be briefed to keep any computers with them at all times, and not entrust them to others. All staff should be made aware that deleting files from a computer does not necessarily remove them from the hard disk.

A clear procedure for storing and transmitting sensitive information should be given to all relevant staff. See Annex 15 for a suggested checklist on information security procedures.

(c) Managing keys

Good locks are not effective unless keys are managed properly. All keys should be accounted for, with staff signing for receipt of each key. If a key is lost, locks should be changed.

(d) Identity badges

It is good practice to provide photo identification cards for all staff, and emergency contact cards for visitors. They can be laminated, two-sided cards with the applicable international language on one side and an appropriate local language on the reverse. They should clearly show an expiry date: this prevents former staff from continuing to use the badge, and limits the damage if a badge is lost or stolen.

(e) Procurement

The way in which humanitarian organisations procure goods and services can have security implications. Many serious attacks, including murders of NGO staff, have been related to procurement issues. Unless procurement is carried out fairly, and is perceived as fair, some local traders and others are likely to feel aggrieved. In some contexts, "fair" may be interpreted as buying from local traders, even if their prices are higher. Depending on the situation, these grievances can be expressed in a variety of

Road accidents are a leading cause of death and injury to aid workers
© James Thurlow



4. SECURITY MANAGEMENT IN THE FIELD

4.12 Travel

ways including threats to the safety of staff. They can also lead to costly and time-consuming legal action.

Great care should therefore be taken to ensure that procurement procedures are good, and followed. Retaining a good local lawyer can help in preventing problems and in defending against malicious or other claims.

(f) Corruption

The security of humanitarian organisations can be threatened by corruption. For example, paying a bribe can lead to a threat if a similar bribe is withheld in future. Yet if civil servants are receiving no salaries, reasonable fees for their services may be seen as legitimate income. Humanitarian organisations should have no involvement with corruption. They should take the local situation into account when deciding – preferably in a coordinated manner with a whole humanitarian community – whether certain fees are justified in a civil service or a commercial context.

All staff should be aware of the importance of avoiding corruption. Staff found to be involved in corruption should be disciplined. All relevant staff should be aware of practical ways of avoiding corrupt practices. Annex 4 contains some tips on how to avoid some common examples of corruption.

(g) Consider a “Get-you-in” team

Because of the heavy administration and management load when a team deploys, it can be helpful to deploy at the same time a “get-you-in” team whose task is to assist the field team in setting up the financial, administration, logistic and other systems necessary for an efficient field operation. A finance / administration specialist at this early stage is often particularly vital. The “get-you-in” team may only be on the ground for, say, one to four weeks, and would depart as soon as the field team can manage without them.

4.12 Travel

In many contexts, the majority of security incidents occur during travel. Some of the threats associated

with travel are:

- ▲ Accidents
- ▲ Ambush
- ▲ Robbery
- ▲ Aggressive behaviour of armed personnel at checkpoints

In insecure locations, all staff should be met on first arrival, and on subsequent arrivals if necessary. Those meeting staff should carry identification.

All relevant staff should be briefed, trained and equipped so that the risks from travel are minimised. A procedure for authorising travel should ensure that each journey is for a good reason, and that staff prepare properly. See Annex 39 for a suggested format for travel authorisation.

All vehicles used, including aircraft or boats, should be in good condition and operated by qualified personnel. All drivers should be required to carry out daily checks on their vehicles and should be tested in changing a wheel and other commonly-required tasks. See Annex 6 for a suggested checklist for drivers and Annex 42 for a suggested equipment list for vehicles.

Vehicle doors (including luggage or cargo doors) should be locked while driving. Leave space between you and the car in front, particularly at traffic lights or when the car in front has stopped. This gives you some freedom to manoeuvre.

Vary the time and route of any regular journeys you make, for example to and from the office. If criminals can predict where you will be and when, it is easier for them to target you.

In some circumstances it may be necessary to travel in convoy. See Annex 3 for suggested convoy procedures.

Vehicle accidents are a leading cause of injury and death to humanitarian staff. All managers and staff must insist on defensive, safe and considerate driving. Disciplinary action should be taken against drivers who persist in driving badly or whose driving may bring the organisation into disrepute.

4. SECURITY MANAGEMENT IN THE FIELD

4.13 Media aspects of security management

4.14 Visibility and security

Staff expected to drive 4x4 vehicles should be trained to drive them properly.

If permissions for travel are required by local authorities, leaders or groups, great care must be taken to ensure that those permissions are obtained, and the relevant documents carried by those travelling. In particular, clearance for flights, crossings of lines of conflict, and through insecure areas should be rigorously checked by a responsible manager before travelling. Humanitarian staff have in some cases been attacked simply because permissions had not been obtained, or there was a misunderstanding, or local officials or military had not been made aware of the intended journey.

4.13 Media aspects of security management

Use of the media can have security implications for humanitarian organisations. On the one hand, the local media can be helpful in informing local people of current and planned activities, and in winning local acceptance. On the other hand, the media can sometimes raise the profile of a humanitarian organisation to a level where it becomes a greater target for criminals or for violent groups.

In general it is likely to be better to give media interviews than to refuse them. But remember the journalists' mantra: "No news is bad news, good news is bad news... bad news is good news". There may be some circumstances where any use of the media may present a danger to humanitarian organisations or to local people – for example where media coverage of aid to a particular group may exacerbate ill-feeling towards that group or their helpers.

It is often necessary to manage local expectations. Local people may assume that newly-arrived humanitarian organisations will provide large quantities of aid to the whole population. Early explanation of the plans, including through local media, will help to ensure that expectations are more in line with reality. If this is not done, there will often be a high risk of disappointment, leading in some cases to increased security risks.

When giving media interviews, the most appropri-

ate staff member should be used. Often the manager will be the most appropriate. A nationally-recruited staff member (not necessarily the manager) may sometimes be able to give a more accurate and culturally appropriate message, enhancing local acceptance of the organisation, and therefore its security.

For tips on the security aspects of handling the media, see Annex 19.

4.14 Visibility and security

The 'visibility' requirements of donors may sometimes have security implications. Where the display of donor logos may result in danger to humanitarian staff or local people, visibility requirements should normally be waived. For ECHO, the following extracts from its Framework Partnership Agreement General Conditions are relevant:

Article 6.1 states:

The Humanitarian Organisation shall contribute to the visibility of the humanitarian Operations financed by the European Community, provided that this does not harm the Organisation's mandate or the safety of its staff.

Article 6.3 states:

In cases where equipment or vehicles and major supplies have been purchased using funds provided by the Commission and provided that this does not harm the Organisation's mandate or the safety of its staff, the Humanitarian Organisation shall include appropriate acknowledgement on such vehicles, equipment and major supplies, including display of the European logo (twelve yellow stars on a blue background).

Article 6.6 states:

The Humanitarian Organisation authorises the Commission to publish the following information in any form and medium, including via the Internet:

▲ The Humanitarian Organisation's name and

4. SECURITY MANAGEMENT IN THE FIELD

- official address
- ▲ The purpose of the grant agreement
- ▲ The amount granted and the proportion of the Operation's total cost covered by the funding

Upon a duly substantiated request by the Humanitarian Organisation, the European Commission may agree to forgo such publicity if disclosure of the above information would risk threatening the Organisation's safety or harming its interests.

Annex V (procedures for the award of contracts) makes certain visibility requirements, but also contains article 3.8 which states:

Upon a duly substantiated request by the humanitarian organisation, the European Commission may agree to forego such publicity⁷ if disclosure of the above information would endanger the organisation's safety or harm its interests.

ECHO partner organisations should be aware of these provisions and make use of them where appropriate. Other donors are likely to have equivalent

- 4.15 Legal protection of aid workers
- 4.16 Reporting of war crimes

rules: humanitarian organisations funded by other donors should be aware of and make use of these rules when necessary.

4.15 Legal protection of aid workers

The host government has primary responsibility for the security and protection of:

- ▲ Humanitarian staff
- ▲ Their dependants and property
- ▲ The property of humanitarian organisations

This responsibility flows from every government's duty to maintain order and protect people and property within its jurisdiction.

In the case of international organisations and their officials and property, the government is considered to have a special responsibility under the Charter of the United Nations or the government's agreements with individual organisations.

The Geneva Conventions⁸ provide further legal protection to certain carefully-defined categories of civilian medical and relief personnel, but this does not cover humanitarian staff in general. Staff of the ICRC are granted protection under the Geneva Conventions, as is the emblem of the ICRC.

The 1994 Convention on the Safety of UN and Associated Personnel⁹ provides protection to UN staff, and persons deployed by certain organisations with close contractual links to the UN or its agencies.

4.16 Reporting of war crimes

Humanitarian organisations should have a policy on the reporting of war crimes and/or serious human rights abuses that its staff may witness or find evidence of. Staff should be briefed accordingly.

The policy should take into account the threats that can face those who report war crimes, as those responsible for the crimes may seek to intimidate witnesses. There may be a need to balance the duty to report crimes with the risk of losing access to beneficiaries, and the risk of violence against staff. It

Mine-laying has had a devastating impact on civilians
© Sean Sutton/MAG



⁷ Ex ante and ex post publication

⁸ Available at www.icrc.org.

⁹ Available at <http://www.un.org/law/cod/safety.htm>.

4. SECURITY MANAGEMENT IN THE FIELD

may be possible to report indirectly or discreetly, and in such a way that it will not be deduced that your organisation did the reporting.

Staff should be trained in checkpoint procedures
© James Thurlow



5. SECURITY INCIDENTS

- 5.1 Security incidents: prevention and reaction
- 5.2 Reporting of incidents
- 5.3 Reporting 'near miss' incidents
- 5.4 Debriefing after an incident
- 5.5 Analysis of incidents and adjustment of procedures

5.1 Security incidents: prevention and reaction

Managers should ensure that their staff are properly prepared, both to minimise security risks and to respond to incidents. At Annex 28 are listed suggested ways of reducing the risk of different types of incident, and of reacting to incidents if they occur.

5.2 Reporting of incidents

Good reporting of an incident can reduce its consequences. It can result in quick reaction by the police or other organisations; it can warn colleagues enabling them to avoid the same incident; and can help to improve security procedures.

Incident reports are usually of the following kinds:

- ▲ Immediate incident report (sent by radio as soon as possible after the start of the incident, containing only a brief, urgent summary of what has happened)
- ▲ Updates (sent as often as necessary, while the incident or the response to the incident continues)
- ▲ Full incident report (usually written, sent once the incident has been stabilised or resolved)

Annex 29 contains suggested formats for each of these kinds of incident report.

It is good practice to establish a Security Incident File in each field office, held on paper or in electronic form. The incident reports of all security incidents are filed in it, to provide an instant overview of security incidents in a given period. This is preferable to searching through the e-mail or other archives to find the relevant reports.

5.3 Reporting 'near miss' incidents

'Near miss' incidents should be reported in the same way as real incidents. A 'near miss' is where it appears that a security incident came close to occurring. It may reveal a weakness in security procedures, or new information about security threats. It should be reported so that security procedures can

be reviewed in the light of it.

5.4 Debriefing after an incident

After a security incident, a debriefing should normally be held for all staff affected by it. This enables the facts to be confirmed, changes in procedures to be discussed, and helps morale.

Debriefing is usually also necessary on an individual basis for any member of staff directly involved. This has the same purposes as the group debriefing. It is also an opportunity for the person concerned to talk through their reactions to the incident. If they request counselling or medical help, or if the manager considers that either may be needed, the manager should seek professional advice.

Managers should note any signs of stress among staff, bearing in mind the possibility of Post-Traumatic Stress Disorder (PTSD) or other stress-related illness. If stress-related illness is suspected, professional advice should be sought – a stress debriefing conducted by someone who is not properly trained may do more harm than good.

5.5 Analysis of incidents and adjustment of procedures

After an incident, managers should think through the events and consider whether there are any lessons to learn. For example, should staff be better briefed? Should procedures be adjusted? Should a particular route be avoided? Should there be better liaison with the police? Should disciplinary action be taken against any member of staff?

Managers should consult relevant staff when considering lessons from an incident, to ensure that all possible lessons are identified and that staff support the conclusions reached.

Records of all security incidents should be kept, and analysed from time to time. Locations of incidents should be plotted on a map. What do the incidents reveal about the nature of the local situation and its threats? Is there a pattern? Can any trend be discerned? What action should be taken as a result?

5. SECURITY INCIDENTS

- 5.6 Medical evacuation (Medevac)
- 5.7 Fatal incidents
- 5.8 Investigation of a serious incident
- 5.9 Media handling after a security incident

It is vital to share reports of incidents with other humanitarian organisations, so that all can benefit from increased knowledge of the security situation. If there is a UN or other security officer in the area, he or she may coordinate the collation of information about incidents.

5.6 Medical evacuation (Medevac)

If a staff member is injured or falls ill and local medical facilities cannot provide sufficient treatment, medical evacuation (Medevac) may be needed. This normally happens only when a doctor advises that it is necessary. See Annex 20 for a suggested Medevac procedure.

Many humanitarian organisations insure against the costs of Medevac, and have arrangements with specialist Medevac companies. If so, it is vital that all relevant staff know the procedure for making use of these.

5.7 Fatal incidents

If a staff member dies, good practice normally requires at least the following procedures:

- ▲ Confirm the identity of the deceased (mistakes do happen)
- ▲ Inform the Next of Kin (see Annex 22 for suggested procedure for informing Next of Kin)
- ▲ Inform the local authorities
- ▲ Secure the body
- ▲ Post-mortem examination, if required
- ▲ Arrange for repatriation of the body. This can be a complex and difficult bureaucratic process
- ▲ Cooperate with local authorities, in the event of a police or judicial investigation
- ▲ Inform the media, if and when appropriate
- ▲ Ensure that any compensation or insurance payments are made swiftly
- ▲ Provide assistance if appropriate to the deceased's Next of Kin and/or dependents
- ▲ Investigation by the employing organisation into the events leading to the death. Depend-

ing on the circumstances, this may be conducted internally or independently

- ▲ Identify any lessons to learn from the incident and adjustment of policies or procedures as necessary

5.8 Investigation of a serious incident

Some incidents are so serious that they require a full investigation by a suitable person not connected with the incident. Precisely which incidents require such investigation is a matter for each organisation. They are likely to include:

- ▲ Death
- ▲ Sexual violence
- ▲ Serious injury
- ▲ Major fraud
- ▲ Major theft

Some serious incidents result from failure to follow agreed security procedures. Investigations should aim to identify what caused the incident, and should recommend any disciplinary action necessary. They ensure that there is accountability for serious loss or damage to staff or property, and are an important part of good security management.

5.9 Media handling after a security incident

The media may take a close interest in a security incident, particularly if it is serious. See Annex 19 for tips on media handling.

6. SUSPENSION, HIBERNATION, RELOCATION, EVACUATION

- 6.1 Deciding whether to suspend, hibernate, relocate or evacuate
- 6.2 Suspension of programme activities

6.1 Deciding whether to suspend, hibernate, relocate or evacuate

If the situation becomes too dangerous for humanitarian operations, work should be halted. Depending on the circumstances, the halt may be temporary or permanent. Stopping work temporarily is commonly known as suspension of the programme. Stopping work permanently and leaving the area is known as evacuation. A middle option, involving stopping work for a considerable time and keeping a low profile to allow the danger to subside, is sometimes known as hibernation. A final alternative is to relocate some or all staff, while remaining within the country.

Deciding to suspend, hibernate, evacuate or relocate is difficult. No formula can decide: only managers can decide, using their judgement and taking whatever advice they think necessary. Bear in mind that evacuation may expose staff to danger while they are evacuating. It is likely to be necessary when the current situation of staff is untenable, or where staff are already hibernating and the situation is expected to worsen.

The decision is normally taken by HQ, on the advice of the senior manager present in the field. If it is not possible to contact HQ, the senior manager present in the field should have the authority to decide to evacuate if a decision is urgently required. It may happen that HQ decides on evacuation against the advice of the senior manager present in the field, in which case the evacuation should normally still take place.

The essential question is: Do the potential risks of working outweigh the likely benefits? If they do, then the work should stop. If they do not, then the work should probably continue. Secondary questions may include:

- ▲ What are other humanitarian organisations planning to do? Will they suspend, hibernate or evacuate – or continue work? Will they take any new security measures? What is their view of the balance of risks and benefits? Be aware that actions by other humanitarian organisa-

tions may place you at greater risk.

- ▲ How is the situation likely to change in the near future?
- ▲ How are needs likely to change in the near future?
- ▲ What other security measures could we consider, which might enable the programme to continue?
- ▲ Rather than stopping work, might we consider reducing staff levels, reducing travel, or altering procedures so as to reduce risks?
- ▲ Is there any further information that we need in order to reach a decision?

Individuals should normally be free to leave if they consider the risks of continuing too great. Most humanitarian organisations have a policy that:

- ▲ Any staff member may choose to leave an insecure location, and that their decision to do so will always be respected; but
- ▲ If instructed by a manager to leave an insecure location, all staff must obey

6.2 Suspension of programme activities

Suspending programme activities may be necessary simply to avoid a threat which has recently emerged. It may be necessary in order to allow time for reflection on a changed security situation. It may also be used in order to send a signal to local authorities or to other groups that threats to humanitarian organisations are not acceptable.

Suspension is likely to be more effective if carried out by all humanitarian organisations at the same time, and for the same stated reasons.

Suspension may be announced in the media. Alternatively it may be unannounced, depending on the circumstances, the threats, and on the purpose of the suspension.

It is advisable to discuss the possible options for suspension with donors during the project design phase, so that funding problems are minimised if it becomes necessary to suspend activities.

6. SUSPENSION, HIBERNATION, RELOCATION, EVACUATION

- 6.3 Hibernation
- 6.4 Relocation or reduction of staff
- 6.5 Evacuation

6.3 Hibernation

A longer period of suspension, where staff remain at home or in a safe place for a considerable time in order to allow danger to subside, is sometimes known as hibernation. Ensure that sufficient resources are available for the duration of the hibernation period.

6.4 Relocation or reduction of staff

An alternative to suspension or hibernation is to relocate staff to a safer location, without leaving the country. A further alternative is to reduce the numbers of staff working, so as to reduce risk.

6.5 Evacuation

When the situation is too dangerous for humanitarian staff to remain in the area, evacuation is necessary. 'Evacuation' normally means the cross-border movement of staff. The decision to evacuate should not be taken lightly, since its consequences can be far-reaching and may include:

- ▲ Increased threats to your own or other humanitarian organisations
- ▲ Increase in workload for other organisations if they remain
- ▲ Misunderstanding by local people
- ▲ Increased needs among local population as the humanitarian programme ends
- ▲ Termination of employment for many staff
- ▲ Loss of property if looting or theft follows evacuation
- ▲ Difficulty in re-establishing a programme in the future

Evacuation is likely to involve most, if not all, of the following steps:

- ▲ Consult senior staff
- ▲ Consult HQ
- ▲ Decide to evacuate
- ▲ Inform all staff
- ▲ Inform relevant embassies, if appropriate
- ▲ Plan the evacuation (outline evacuation plans should already exist in the security

plan; these should now be adapted and made more detailed)

- ▲ Identify those staff who will leave and those who will stay (if any)
- ▲ Identify property that will leave and property that will remain; hide high-value property if possible
- ▲ Provide clear instructions for any staff remaining
- ▲ Provide pay and other money required by any staff remaining
- ▲ Inform local authorities of the evacuation if appropriate
- ▲ Inform HQ of detailed plan
- ▲ Carry out evacuation
- ▲ Inform HQ that the evacuation is complete
- ▲ Inform relevant embassies that the evacuation is complete
- ▲ Debrief staff after evacuation, and make counselling available if necessary
- ▲ Write post-evacuation report, including a detailed account of the position of all staff, property and money, and any issues still unresolved
- ▲ Keep in contact with remaining staff (if any)
- ▲ When appropriate, plan your return

Annex 10 contains a suggested checklist for points to consider when planning and carrying out an evacuation.

In most cases, humanitarian organisations have a stated policy that nationally-recruited staff are not normally evacuated from areas in which they live. Reasons given for this policy include:

- ▲ The prohibitive cost of evacuating and then providing for large numbers of nationally-recruited staff
- ▲ Nationally-recruited staff usually have families in the area and do not normally wish to leave them
- ▲ Nationally-recruited staff are in many cases not threatened as much as international staff

This policy is sometimes made explicit in the contracts signed by nationally-recruited staff. Nevertheless, it may be sometimes be appropriate and possible to relocate national staff and their families, within their country, or to provide them with the means to do so themselves.

6. SUSPENSION, HIBERNATION, RELOCATION, EVACUATION

In exceptional circumstances, where lives are at risk, it will be necessary to decide on a case-by-case basis whether to evacuate particular staff members and their families. There may be no legal requirement for organisations to do so (though the duty of care may constitute a legal requirement to evacuate staff in some situations), but in some cases a moral obligation may exist to protect staff when at grave risk.

In other cases nationally-recruited staff may continue running the programme, or a modified version of it, while the international staff are absent. This may be possible if the risks to nationally-recruited staff are significantly lower than to international staff. In this case, clear procedures and good communications with HQ are essential.

6.6 Role of the United Nations in evacuation

If the UN decides to evacuate, it is likely to play a leading role in the evacuation of other humanitarian organisations, if they decide to evacuate. The UN is under no obligation to assist another organisation, unless they have signed a Memorandum of Understanding with that organisation to include it in UN

Disciplined soldiers can provide a secure environment
© James Thurlow



- 6.6 Role of the United Nations in evacuation
- 6.7 Debriefing after an evacuation
- 6.8 Media aspects of suspension, hibernation, relocation or evacuation

security arrangements. See Annex 40 for further information.

6.7 Debriefing after an evacuation

After evacuation, the appropriate managers should debrief staff to ensure that any outstanding issues are resolved as far as possible. These issues may include, for example:

- ▲ Needs of the population left behind: are there any ways that they can be met, now that the programme has ended or been modified?
- ▲ Will the programme be re-established? If so, when, how and under what conditions?
- ▲ Should staff remain on contract so as to be able to re-establish the programme as soon as that becomes possible?
- ▲ Termination or renewal of contracts; reassignment to other tasks
- ▲ Continuing contact with staff whose contracts have recently been terminated
- ▲ Management of remaining staff
- ▲ Feelings of loss or disappointment
- ▲ Campaigning or lobbying
- ▲ Media interviews
- ▲ Pay
- ▲ Compensation for loss of property
- ▲ Stress
- ▲ Treatment of any staff needing medical attention
- ▲ Future plans for the team and for individuals
- ▲ Corporate and individual expressions of appreciation for the work done by staff: consider a ceremony of thanks or a farewell party

6.8 Media aspects of suspension, hibernation, relocation or evacuation

The media may take an interest in an evacuation. Some journalists may be tempted to give over-dramatic reports. If they decide to speak to the media about the evacuation, humanitarian organisations may wish to achieve one or more of the following objectives:

- ▲ Draw primary attention to the increased needs of the population after the closure or modification of humanitarian programmes

6. SUSPENSION, HIBERNATION, RELOCATION, EVACUATION

6.9 Return after evacuation

- ▲ Put across a true, factual account of the evacuation and the reasons for it, correcting any false accounts or rumours that may be circulating
- ▲ Call for action by governments, or other authorities or groups, to reduce the threats to humanitarian organisations, so that they may resume work
- ▲ Express the hope of re-establishing programmes in the near future

6.9 Return after evacuation

If it becomes possible to return to the area after an evacuation, a fresh security assessment (see Annex 26) will be necessary since the security situation is likely to have changed in important respects. Local relationships will need to be re-established, and it may take some time before there is sufficient confidence for programmes to be relaunched.

In some cases nationally-recruited staff may have continued running the programme throughout the period of the evacuation. Due recognition of their achievement is likely to be important for the cohesion of the team. In particular, international staff should be careful not to give the impression that everything came to a halt when they left.

7. CLOSING A PROGRAMME

- 7.1 Ending staff contracts
- 7.2 Ending other contracts
- 7.3 Legal aspects of programme closure
- 7.4 Disposing of property
- 7.5 Evaluation and inspection

The closure of a programme, for whatever reason, can have security implications. Staff are likely to be disappointed at losing their jobs. Local leaders, contractors, partners and beneficiaries may protest at losing the assistance that the programme brought. Care is needed to ensure that the closure is well managed and that security risks do not rise.

7.1 Ending staff contracts

The process of terminating contracts should be carefully planned and sensitively managed. Contracts should have been drawn up initially with the possibility of short notice being given in times of crisis, so that staff know what to expect. Ties of loyalty may have built up over time, and some staff may feel that their loyalty is not being rewarded. Other staff may be tempted to steal from the organisation, now that they know that they have no future with it. There are thought to have been cases of disgruntled staff threatening or carrying out violence as a result of losing their jobs.

Local employment laws and customs should be followed scrupulously. A good local lawyer is likely to be needed: his fees may be many times less than the cost of legal action which might result otherwise.

Above all, the process should be fair, and perceived to be fair. Managers should ensure that at all times there is clear communication about the process, and consultation where possible.

Redundancy payments and other compensation may be appropriate, or may be required by law. When considering such payments, organisations may wish to err on the side of generosity. This could be seen as a good security measure, encouraging departing staff to think and speak well of their former employer.

7.2 Ending other contracts

Contracts with local companies, owners of buildings, and others may need to be ended. In a known insecure environment where a crisis is likely to result in termination of contracts at short notice then clauses can be written into contracts at the outset to deal with such a situation. Transparency, fairness and

attention to detail are important. Once again, a local lawyer may be useful.

7.3 Legal aspects of programme closure

Any outstanding claims or legal cases should be resolved before the departure of the manager. To leave without such resolution could increase risks to staff and former staff, and to other humanitarian organisations. It would damage the reputation of the organisation, and make a future return difficult.

7.4 Disposing of property

Early decisions should be made on how to dispose of the organisation's property. Some may be sold. Some may be given to local organisations. Some may be taken out of the area by the organisation, for use in other programmes.

These decisions will depend on the requirements of donors, on the rules of the organisation, and/or on the judgement of the manager concerned.

Some governments have required departing humanitarian organisations to leave their property behind, arguing that, because the property was intended and funded for the benefit of local people, it should continue to be used for their benefit. This has sometimes included expensive items such as vehicles. The Red Cross/Crescent/NGOs Code of Conduct recommends that "Governments should not restrict the re-exportation of relief equipment at the end of a relief operation"¹⁰, but some governments may not wish to follow this recommendation. To avoid misunderstanding over this issue, it is best if organisations clarify the final destination of equipment with the local authorities, during the initial security assessment before the start of the programme.

7.5 Evaluation and inspection

Evaluations or inspections of programmes, including security management aspects, may be required by the organisation or by donors before the programme closes. These should be taken into account when planning the closure. In particular, will key

¹⁰ Available at <http://www.ifrc.org/publicat/conduct/code.asp>.

7. CLOSING A PROGRAMME

- 7.6 Handover of a programme
- 7.7 Media aspects of closing a programme
- 7.8 Farewell events
- 7.9 Debriefing after programme closure
- 7.10 Archiving documents after programme closure

staff be available for interview if required? If evaluations or inspections cannot carry out their work properly, an important element of security management will be lost.

7.6 Handover of a programme

In some cases a programme, or part of it, may be handed over to another organisation who will continue to run it after the departure of the organisation which launched it. Transparency, clarity, attention to detail and good communication with partners and beneficiaries are essential. Otherwise, misunderstandings and tensions may arise among local people, who may become hostile towards either organisation.

7.7 Media aspects of closing a programme

If media announcements are planned, they should be designed so as to give maximum clarity to local people about the programme closure, and to minimise any sense of disappointment.

7.8 Farewell events

Any farewell celebrations should be humble, if possible with local beneficiaries the centre of attention. All staff, particularly nationally-recruited staff, should be warmly thanked for their work. Any impression of self-satisfaction, complacency or arrogance is liable to reduce acceptance by local people, not only of your organisation but possibly of humanitarian organisations in general. That may indirectly increase threats to the organisation, or to humanitarian organisations in general.

7.9 Debriefing after programme closure

Senior managers at HQ should invite staff from the recently closed programme to a debriefing on the programme. Sufficient time should be set aside to do justice to the scale of the programme. Security aspects, from the earliest assessments to the closure of the programme, should be discussed. Senior managers should ensure that any lessons learned result in changes to security policy or procedures.

7.10 Archiving documents after programme closure

All security-related documents and reports should be archived properly. This enables accountability should any future investigation be made. It can also protect the organisation against any false claims.

Care should be taken when removing documents from the country. There have been examples of the authorities searching departing humanitarian staff, finding sensitive documents, and imprisoning the staff as a result.

Women and children depend on good security
© Christian Aid/Jenny Matthews



8. HEADQUARTERS MANAGEMENT OF SECURITY

- 8.1 Responsibilities of Headquarters for security management
- 8.2 Hierarchy of documents: security policy, manual, plan

8.1 Responsibilities of Headquarters for security management

Headquarters have important security responsibilities. They include the following:

- ▲ Setting the security policy for the organisation
- ▲ Producing generic security procedures for the organisation, which can then be adapted to each different field context
- ▲ Insurance
- ▲ Training policy
- ▲ Deciding on deployment or evacuation: HQ normally take the final decision on whether a team will deploy to a new country or region, and on whether a team will evacuate. HQ normally delegates authority to the field manager to evacuate if the situation is urgent and if he or she is unable to contact HQ.
- ▲ Providing competent field staff, particularly a competent and experienced field manager. This is one of the most effective contributions to good security management in the field.
- ▲ Preparation of field staff, through training, briefing and equipping
- ▲ Planning of field operations
- ▲ Allocating sufficient resources – financial and human – to ensure security, including security training
- ▲ Providing support to field managers and staff when required
- ▲ Overruling the field manager's decisions when necessary. This should only rarely be necessary if the field manager is competent, experienced and well prepared.
- ▲ Monitoring the effectiveness of security management in the field
- ▲ Ensuring lessons are learned from experience and that policy and procedures are updated accordingly
- ▲ Managing the security of HQ staff and property
- ▲ Ensuring that senior managers in HQ are well prepared to take timely security-related decisions when necessary. This includes the preparedness and implementation of a crisis management team for managing certain serious or high-profile incidents.
- ▲ Encouraging a culture of good security throughout the organisation

- ▲ Humanitarian organisations should be aware of the extent of their legal liability if various contingencies were to occur. In particular, liability for negligence can be considerable if it is shown that, for example, a staff member has been injured as a result of insufficient preparation for work in an insecure location. HQ should take legal advice on this question.

8.2 Hierarchy of documents: security policy, manual, plan

A recommended simple hierarchy of key security documents is:

- ▲ **Security policy** – giving overall policy for the organisation (see Annex 32)
- ▲ **Security manual** – giving generic procedures for the organisation (see Annex 30)
- ▲ **Security plan** – giving detailed procedures for a specific location (see Annex 31)

In this way the different purposes of each security document are clearly defined, and a proliferation of documents is avoided. The security policy and security plans should both be short, to ensure that they are read. The manual is likely to be much longer since there are many security procedures that can apply to a wide variety of different situations.

The security **policy** describes the organisation's approach to security and sets out general rules for security management.

A **manual** of generic security procedures is useful to field staff who should adapt procedures to suit the local context. This avoids the need to repeat generic procedures in the security plan for a particular location. Time is saved, and the security plan remains short and therefore more likely to be read by field staff. Other names sometimes used for a security manual include 'security handbook' and 'standard operating procedures' (SOPs).

If the organisation does not have its own security manual, it may find it helpful as an interim measure to use a manual produced by another organisation,

8. HEADQUARTERS MANAGEMENT OF SECURITY

- 8.3 Security advisor
- 8.4 Human Resources Management – security aspects
- 8.5 Serious or high-profile incidents

modified or with an addendum that meets the particular needs of the organisation.

Security **plans** are normally written by the field team leader, or other staff member who will be responsible for security management in a particular field location. If possible, they should be written in collaboration with all staff, national and international, who will be affected by them. It is good practice for a copy of each plan, and all updated versions, to be provided to HQ so that staff there can react appropriately in case of need.

8.3 Security advisor

Some humanitarian organisations employ one or more security advisors. The purpose of this post, whether at Headquarters or in the field, is to advise managers and staff on good security management, and to support them in their security-related duties.

The tasks of the security advisor should be clearly defined. They may include:

- ▲ Advising senior managers on security policy
- ▲ Drafting generic security procedures or a security manual, for approval by senior managers
- ▲ Assisting senior managers to monitor the effectiveness of security management
- ▲ Advising on the design and delivery of security training, briefing and debriefing. May also carry out training directly, particularly 'training of trainers'.
- ▲ Advising on the procurement of suitable security-related equipment and services, such as insurance and consultancy
- ▲ Assisting with recruitment of any security-related staff
- ▲ Reviewing security plans produced by field teams
- ▲ Collating information on security incidents and 'near misses'
- ▲ Collating organisation-wide lessons learned on security
- ▲ Assisting managers during security incidents

The security advisor is not responsible for security management – that rests with the line managers at each relevant level.

8.4 Human Resources Management – security aspects

Providing the right staff, with the right experience and training, on time, is one of the most important contributions to security management. Human resources managers need guidance and support from senior line managers if they are to succeed in this goal. Many humanitarian organisations have difficulty finding the emergency staff that they need. The result is often fewer staff, and lower quality staff, than life-saving programmes deserve.

For good security management, as for general management, it is important to plan for long term personnel needs and invest sufficient resources so that enough good staff will be available for emergency operations.

Organisations usually need to employ new staff for an emergency programme. The ability to recruit rapidly and effectively can make a great difference to the success, and the security, of the field team. Human resources managers have a role to play in checking that all staff are prepared for the field with the appropriate training, briefing and equipping.

Most field staff will require insurance cover. Human resources managers should check that there is appropriate cover, and that the cover does not exclude relevant risks. Note that failure to maintain adequate insurance could lead to large claims being made against an employer, which in some cases could drive the employer into bankruptcy. In addition, the duty of care is not absolved by monetary compensation, so lawsuits are possible even if there is adequate insurance, if the organisation has been negligent.

Human resources managers should ensure that staff performance appraisals include an appraisal of performance in security management, where appropriate.

8.5 Serious or high-profile incidents

A HQ is likely to play a role in managing certain serious or high-profile incidents, if the field team is unable to manage them alone. Senior managers

8. HEADQUARTERS MANAGEMENT OF SECURITY

- 8.6 International Humanitarian Law
- 8.7 Advocacy and humanitarian space: Headquarters aspects
- 8.8 Archives
- 8.9 Discipline

should be trained and prepared, as required, to handle such incidents. Examples may include:

- ▲ Death or serious injury to a member of staff
- ▲ Disaster affecting the ability of the HQ to function
- ▲ Mass casualties, in the field or at HQ
- ▲ Communications failure
- ▲ Major fraud
- ▲ Kidnap and ransom demand
- ▲ Compensation claim against the organisation arising out of a security incident
- ▲ Any incident which has generated or is likely to generate media interest

A crisis management team is likely to be necessary to handle such incidents. Such a team includes the necessary managers and support staff to manage a serious or high-profile incident for the whole of its duration.

HQ should ensure that contingency plans are in place for any eventuality that could have a high impact on the organisation or its work, including some of the above examples.

Trying to meet many needs can lead to high levels of stress among humanitarian staff

© James Thurlow



8.6 International Humanitarian Law

HQ may have a role to play in advising their staff on relevant provisions of International Humanitarian Law (IHL), and advocating for States or other parties to respect those provisions.

See Annex 17 for further information on IHL.

8.7 Advocacy and humanitarian space: Headquarters aspects

HQ should be ready to assist field managers in negotiating for humanitarian space, and in advocacy for any political or other initiatives that the situation may require. In some cases this may include campaigning, preferably in combination with other organisations, for a properly mandated military force to intervene. It may involve lobbying for proper distinctions to be preserved between military and humanitarian organisations, and their respective objectives.

HQ should be aware of the possibility of advocacy messages endangering field staff, local partners or local people. For this reason, field managers should control the development and delivery of advocacy messages.

Creative thinking and bold advocacy, based on well-researched evidence and mature reflection, can have a great and beneficial impact on the security of a humanitarian operation, and therefore on the safety of the local population.

8.8 Archives

HQ should ensure that archives are kept containing all relevant records from field programmes. This helps accountability, and can protect the organisation against false accusations in future. It also provides a back-up in case records are destroyed by fire or in conflict.

8.9 Discipline

A disciplinary system should only be needed rarely, but it is a necessary part of security management.

8. HEADQUARTERS MANAGEMENT OF SECURITY

- 8.10 Duty officer system
- 8.11 Relating to the UN Security System
- 8.12 Relating to donors
- 8.13 Codes and Standards

Staff should be aware that a breach of security procedures can be a disciplinary offence.

Managers should lead by example, and should check that staff do not take dangerous short-cuts with security.

8.10 Duty officer system

A duty officer system in HQ allows field managers and others to contact the HQ at any time of day or night, via a mobile phone or other communications method. The duty officer should have a full contact list and a briefing folder describing the actions to take in case of various contingencies. The system normally operates as a rota, with an alternative number to ring in case the main contact number does not respond.

8.11 Relating to the UN Security System

UN operational agencies are part of the UN Security System. Other humanitarian organisations are not part of the System but may wish to be in ongoing dialogue with the UN (UNSECOORD or another appropriate body) to promote good practice in security management by humanitarian agencies.

In 2002 the UN Inter-Agency Standing Committee, in consultation with NGOs, produced a Menu of Options for UN-NGO security collaboration. It is summarised at Annex 41. NGO HQs should be aware of this Menu of Options, and disseminate it to field managers.

8.12 Relating to donors

Many donors take an active interest in good security management and will wish to maintain an ongoing dialogue with HQ of humanitarian organisations. This enables informed funding and policy decisions to be made, which can be of value in supporting effective security management both in the organisation and more widely across the sector.

8.13 Codes and Standards

The Red Cross/Crescent/NGOs Code of Conduct

The Code of Conduct for the International Red Cross and Red Crescent Movement and NGOs in Disaster Relief¹¹ contains at least the following security-related points:

- ▲ “Host governments should facilitate rapid access to disaster victims” for Non-Governmental Humanitarian Agencies (NGHAs)
- ▲ “Donor governments should use their good offices to assist NGHAs in obtaining access to disaster victims. Donor governments should recognise the importance of accepting a level of responsibility for the security and freedom of access of NGHAs staff to disaster sites. They should be prepared to exercise diplomacy with host governments on such issues if necessary.”
- ▲ “Governments should facilitate the timely flow of relief goods and information during disasters”
- ▲ “Governments should not restrict the re-exportation of relief equipment at the end of a relief operation”
- ▲ Host governments “should authorise relief personnel to utilise all means of communication required for their relief operations”
- ▲ Host governments are urged to provide NGHAs with “information on potential security risks they may encounter”
- ▲ “Host governments are urged to designate, prior to disaster, a single point-of-contact for incoming NGHAs to liaise with the national authorities”
- ▲ “In the event of armed conflict, relief actions are governed by the relevant provisions of international humanitarian law”
- ▲ “Inter-Governmental Organisations (IGOs) should extend security protection provided for UN organisations, to NGHAs. Where security services are provided for inter-governmental organisations, this service should be extended to their operational NGHAs partners where it is so requested.”
- ▲ “IGOs should provide NGHAs with the same access to relevant information as is granted to UN organisations. IGOs are urged to share all information, pertinent to the implementation

¹¹ Available at www.icrc.org.

8. HEADQUARTERS MANAGEMENT OF SECURITY

8.13 Codes and Standards

of effective disaster response, with their operational NGHAs partners.”

People In Aid Code

Principle 7 of the People In Aid Code of Good Practice in the management and support of aid personnel¹² is entitled: “Health, Safety and Security”. It states:

“The security, good health and safety of our staff are a prime responsibility of our organisation. We recognise that the work of relief and development agencies often places great demands on staff in conditions of complexity and risk. We have a duty of care to ensure the physical and emotional well-being of our staff before, during and on completion of their period of work with us.”

Further detail is given at Annex 23.

Sphere Project

Some humanitarian organisations subscribe to the Sphere standards. Common Standard 7 of the Sphere Project Humanitarian Charter and Minimum Standards in Disaster Response¹³ requires that: “Aid workers possess appropriate qualifications, attitudes and experience to plan and effectively implement appropriate programmes.”

While this does not mention security explicitly, there is a clear implication that aid workers must be capable of managing their own security, and the security of their teams if they are managers, in situations of insecurity. Signatories of the Sphere Project should plan accordingly.

InterAction Field Cooperation Protocol

In 1996 a number of members of InterAction, the US NGO umbrella organisation, signed a Field Cooperation Protocol¹⁴. The signatories agreed to instruct their representatives engaged in disaster response to consult with other NGO representatives similarly engaged to try to reach consensus in dealing with a wide range of issues including security arrangements, and in particular:

- ▲ Hostage policy
- ▲ Payment of extraordinary fees
- ▲ Location of housing
- ▲ Communications channels and procedures
- ▲ Evacuation planning
- ▲ Convoy organisation and scheduling
- ▲ Protection of sensitive information

¹² Available at www.peopleinaid.org.

¹³ www.sphereproject.org.

¹⁴ Available at http://www.interaction.org/disaster/NGO_field.html.

9. LEARNING AND TRAINING

9.1 Security lessons learned

9.2 Evaluations

9.3 Training

9.1 Security lessons learned

At regular intervals during a programme, and after its closure, the programme manager and staff should identify lessons to learn relating to security.

A named manager at the appropriate level should be held responsible for ensuring that any security lessons identified are fed into policy, procedures or plans as required. He or she should compare lessons between operations, and share them with other organisations.

9.2 Evaluations

Evaluations should examine the effectiveness of security management as part of their terms of reference. They should also evaluate whether programmes were designed to take account of security considerations.

Evaluations should take place, if possible, during the lifetime of the programme, to ensure that relevant staff are available for interview.

A named manager at the appropriate level should be held responsible for ensuring that any security lessons identified in evaluations are fed into policy, procedures or plans as required.

9.3 Training

(a) Training for new field staff

Each humanitarian organisation has a duty of care to its staff. It is responsible for ensuring that staff who will be working in an insecure situation for the first time have at least a basic knowledge of how to stay safe. It is irresponsible and dangerous to send staff into insecure situations with little or no knowledge of the security risks and how to deal with them.

Organisations will have varying interpretations of what amounts to responsible security preparation for new staff, and how best to organise it. A suggested training syllabus for new field staff is at Annex 36.

Many of the above topics are best covered by training. Some may be covered by briefing. Relatively few of the above topics are covered by academic courses.

(b) Training for field managers

Field managers are responsible for ensuring the security of their team. They are likely to need training and briefing specific to this role. Annex 37 gives a suggested syllabus for field managers.

Again, a mixture of training and briefing is likely to be needed, to ensure that field managers have the necessary knowledge and skills for their job.

(c) Training for Headquarters managers

Some HQ managers have a vital role to play in security management. They are likely to need preparation for at least certain aspects of their responsibilities. The following are some examples:

- ▲ Assessing threats to the organisation
- ▲ Awareness of world trends affecting the security of humanitarian organisations
- ▲ Balancing the risks against the likely benefits of a programme

Mine Risk Education is vital in mine-affected areas
© Sean Sutton/MAG



9. LEARNING AND TRAINING

- 9.4 Learning from other agencies and networks
- 9.5 Use of experienced staff as trainers, briefers, advisers, evaluators

- ▲ Managing serious or high-profile security incidents, such as kidnapping
- ▲ Handling the media during a security incident
- ▲ Kidnap negotiations
- ▲ Dealing with mass casualties
- ▲ Security at HQ offices
- ▲ Standby arrangements if the HQ ceases to function
- ▲ Sharing knowledge and good practice on security with other organisations

Exercises or rehearsals may be necessary to prepare for some of the above tasks. Others may be covered by training or briefing.

9.4 Learning from other agencies and networks

There are a number of NGO networks, training organisations and other bodies actively engaged in improving security management. Humanitarian organisations may find it helpful to keep in touch with these. Examples include:

Bioforce – www.bioforce.asso.fr
 InterAction – www.interaction.org
 People In Aid – www.peopleinaid.org
 RedR – www.redr.org

A number of commercial companies provide training and other learning services such as management consultancy. The Security Training Directory accompanying this Guide has details of some of these.

9.5 Use of experienced staff as trainers, briefers, advisers, evaluators

Experienced field staff are a valuable resource for training and briefing current and future field staff. Some may have returned from the field temporarily or permanently, and may therefore have considerable time available. Humanitarian and training organisations may wish to make use of them for:

- ▲ Training current and future field staff
- ▲ Briefing on situations where they have recent experience or knowledge
- ▲ Advising on security policy or procedures
- ▲ Evaluating security management
- ▲ Assisting security assessments or other security tasks

10. DONORS

Donors are usually willing to provide funding for appropriate security measures, primarily field-oriented, that will improve the effectiveness of the team and its programmes. Some donors indicate that they are prepared to fund security measures to a greater extent than humanitarian organisations have requested in the past.

Normally, donors do not specify certain security measures or practices. In most cases, they do not have the time or detailed knowledge of a particular context to do so. Furthermore, the Code of Conduct for the International Red Cross and Red Crescent Movement and NGOs in Disaster Relief¹⁵ recommends (Annex II) that "Donors should provide funding with a guarantee of operational independence". Accordingly, donors form a view of the competence of the partner before funding, and rely on evaluations to verify that security, among other aspects of the programme, was well managed.

Good convoy procedures promote both security and efficiency
© James Thurlow



¹⁵ Available at <http://www.ifrc.org/publicat/conduct/code.asp>.

11. ABBREVIATIONS

The following abbreviations are used in this Guide.

ANSO	The Afghanistan NGO Security Office
CAP	Consolidated Appeal Process (UN)
DO	(UN) Designated Official for Security
DSA	Daily Subsistence Allowance (UN)
ECHO	European Commission's Directorate-General for Humanitarian Aid
ERW	Explosive Remnants of War
FM	Frequency Modulation (the normal radio type for local broadcast radio)
HF	High Frequency (long-range radio)
HIC	Humanitarian Information Centre
HQ	Headquarters
IASC	Inter-Agency Standing Committee (of the UN)
ICRC	International Committee of the Red Cross
IED	Improvised Explosive Device
IGO	Intergovernmental Organisation
IHL	International Humanitarian Law
Medevac	Medical Evacuation
MOSS	Minimum Operating Security Standards
MRE	Mine Risk Education
NGHA	Non-Governmental Humanitarian Agency
NGO	Non-Governmental Organisation
ODI	Overseas Development Institute
PTSD	Post-Traumatic Stress Disorder
R&R	Rest and Recreation
Sitrep	Situation Report
SMT	Security Management Team
SOP	Standard Operating Procedure
SRSR	Special Representative of the Secretary-General
UN	United Nations
UNHCR	UN High Commissioner for Refugees
UNSECOORD	UN Security Coordinator
UXO	Unexploded Ordnance
VHF	Very High Frequency (short-range radio)

12. IMPORTANT INFORMATION ABOUT THIS GUIDE

12.1 Acknowledgements

We gratefully acknowledge the help of staff and managers from ECHO, UN agencies and secretariat, the Red Cross/Crescent Movement and NGOs who were interviewed during the course of the preparation of this Guide.

Many existing manuals and handbooks were helpful to the preparation of this Guide. We particularly acknowledge the CARE International Safety and Security Handbook, to be published in the near future.

We also thank John Cosgrave and Jan Davis for their helpful comments on drafts. Finally our thanks go to Mrs Costanza Adinolfi, Acting Director-General, at whose initiative this Review was undertaken, and Peter Cavendish, Val Flynn and Siobhán Caughey of ECHO, who gave invaluable support.

12.2 Authors and date

The ECHO Security Review, of which this is part, was prepared by Katy Barnett, Barney Mayhew and Graham White of The Evaluation Partnership (www.evaluationpartnership.com), and submitted to ECHO in October 2004. The author of this Guide was Barney Mayhew.

12.3 Funding

ECHO provided full funding for this Guide.

12.4 Copyright

Copyright for this document is held by the European Commission's Directorate-General for Humanitarian Aid - ECHO. Copying of all or part of this document is permitted, subject to the disclaimer below the table of contents, provided that the source is acknowledged. This permission does not include the photographs used in this document, except when copied as part of this document. For permission to reproduce them separately, contact the copyright owners of the photographs, listed in this chapter.

12.5 Software and languages

This Guide is available in English in pdf and Word formats, and in French, Spanish and Arabic in Word format.

12.6 Further copies

Further copies of this Guide may be requested from echo-eval@ec.europa.eu or downloaded from ECHO's website: see the ECHO home page at <http://ec.europa.eu/echo>

12.7 ECHO contact

The ECHO contact for security matters is:

E-mail: echo-ngo-security@ec.europa.eu

Web: <http://ec.europa.eu/echo>

12.8 Photo credits

Cover page

Taking cover

© ECHO/François Goemans

Page 2

A head teacher and community worker at a school in Los Peres, Dominican Republic

© Christian Aid / Peter Graystone

Mine Risk Education supported by Mines Advisory Group, Cambodia

© Sean Sutton / Mines Advisory Group

Men with shotguns, Liberia

© Action Contre La Faim

Page 3

A Rwandan genocide widow with a counsellor from a local widows' association

© Christian Aid / Georgiana Treasure-Evans

Sick man being treated, Shawe IDP camp, Ethiopia

© Christian Aid / Jenny Matthews

Damaged building in Chechnya

© James Thurlow

12. IMPORTANT INFORMATION ABOUT THIS GUIDE

Kosovar refugees at tapstand, Macedonia
© Jan Davis, RedR

Mother and child. The mother is a voluntary elected president of a traditional Gacaca court in Rwanda
© Christian Aid / Georgiana Treasure-Evans

Page 4
Civilians, Oxfam staff and troops, Liberia
© James Thurlow

Kosovar refugee tracing, Macedonia
© Jan Davis, RedR

Kosovar boy, Macedonia
© Jan Davis, RedR

Young armed men, Liberia
© James Thurlow

Three men plus grenade launcher, Liberia
© James Thurlow

A soldier stopping a humanitarian agency vehicle, Liberia
© James Thurlow

Page 5
An ECHO-funded food convoy, Armenia
© James Thurlow

Booby-trapped grave, Chechnya
© James Thurlow

Armenian women looking through gate, asking for help
© James Thurlow

Truck passing checkpoint, Armenia
© James Thurlow

Burnt-out car, Liberia
© James Thurlow
Old man with child, waiting for food in Shawe IDP camp, Meda Wolabu, Ethiopia
© Christian Aid / Jenny Matthews

Page 7
A Rwandan genocide widow with a counsellor from a local widows' association
© Christian Aid / Georgiana Treasure-Evans

Page 10
Civilians, Oxfam staff and troops, Liberia
© James Thurlow

Page 13
Old man with child, waiting for food in Shawe IDP camp, Meda Wolabu, Ethiopia
© Christian Aid / Jenny Matthews

Page 16
Man inspecting unexploded shells and a destroyed tank, Kirkuk, Iraq
© Sean Sutton / Mines Advisory Group

Page 18
Mother and child. The mother is a voluntary elected president of a traditional Gacaca court in Rwanda
© Christian Aid / Georgiana Treasure-Evans

Page 20
Kosovar refugee tracing, Macedonia
© Jan Davis, RedR

Page 25
UN military officer and local armed group, Beni, D.R. Congo
© RedR

Page 28
MAG teams start clearing minefields around Bardarash village, Iraq
© Sean Sutton / Mines Advisory Group

Page 31
A head teacher and community worker at a school in Los Peres, Dominican Republic
© Christian Aid / Peter Graystone

Page 34
Road accident involving humanitarian agency vehicle, Chechnya
© James Thurlow

12. IMPORTANT INFORMATION ABOUT THIS GUIDE

Page 37

Son Phan was injured while clearing mines from around his house, Cambodia.

© Sean Sutton / Mines Advisory Group

Page 38

Truck passing checkpoint, Armenia

© James Thurlow

Page 43

A soldier stopping a humanitarian agency vehicle, Liberia

© James Thurlow

Page 46

Mother and child, Ethiopia: waiting for the clinic and food distribution

© Christian Aid / Jenny Matthews

Page 49

Armenian women looking through gate, asking for help

© James Thurlow

Page 52

Mine Risk Education supported by Mines Advisory Group, Cambodia

© Sean Sutton / Mines Advisory Group

Page 54

An ECHO-funded food convoy, Armenia

© James Thurlow

Page 59

Chey Ueith, Deminer and Minefield Surveyor, Mines Advisory Group, Cambodia

© Sean Sutton / Mines Advisory Group

Controlled detonation of cleared mines and unexploded ordnance

© Sean Sutton / Mines Advisory Group

Kosovar refugees in a camp, Macedonia

© Jan Davis, RedR

Young armed men, Liberia

© James Thurlow

Back cover

ECHO Flight

© ECHO/François Goemans

ANNEXES: CHECKLISTS, TEMPLATES AND FURTHER INFORMATION



© Sean Sutton/MAG



© Sean Sutton/MAG



© Jan Davis, RedR



© James Thurlow

BUILDINGS AND SECURITY

A1

By paying attention to a number of important details, you can greatly improve the security of your offices, warehouses and accommodation buildings. No building is totally secure, and most humanitarian organisations will not wish to live or work in a heavily fortified building except in extreme circumstances. Instead, it is often preferable to blend in with the local community, while taking discreet precautions to make your buildings as secure as possible. Each situation is different, and calls for careful judgement by an experienced manager.

Factors to bear in mind when choosing a building include:

General location

- ▲ Is it in a location that will enable your programme to run effectively? (Is it close enough to the beneficiary population? Does it have good access to routes and locations that are important for your programme?)
 - ▲ Is it in an area of relatively low crime?
 - ▲ Is it near the transport routes that are important to you, including potential evacuation routes?
 - ▲ Is the building accessible from many access points, or only one or two? (One or two may be easier to control.)
 - ▲ Is it discreetly located, or is it in a high profile location? Which is more beneficial to your security, in the current situation?
 - ▲ Is the building overlooked? Does that matter in the current circumstances?
 - ▲ Are access routes to the building free from places for people to conceal themselves? (Keep shrubbery and bushes around residences trimmed low.)
 - ▲ Are external electrical, telephone and gas supply boxes locked?
 - ▲ Is the building in an area prone to flooding, earthquake or other problems? If so, is it protected against these?
 - ▲ Are there any health risks in the area? (E.g. sewage or rubbish facilities)
 - ▲ If fighting were to break out, would the building be potentially exposed to direct fire?
 - ▲ Is the building close to a sensitive location? (E.g. a military or police barracks; a political party office; the house of a prominent politician, etc.)
- If so, might it embarrass your organisation to be associated in people's minds with that sensitive location? If a nearby location is likely to be targeted by violence, consider whether it might affect your building.
- ▲ Is the building close to a dangerous location? (E.g. a fuel store)
 - ▲ Are the police or other security forces within a reasonably short distance, so that if you need their help they will be quick to arrive?

Physical security of the building

- ▲ Are the walls strong enough to withstand likely threats?
- ▲ Are the windows barred?
- ▲ Are the doors strong? Check locks, hinges, bars.
- ▲ Is there a perimeter wall? How easy/difficult is it to surmount? Does it have barbed wire? Does it need barbed wire, or would that send the wrong signal to local people? Are its gates strong? Can a guard look through the gate without opening it?
- ▲ Is the roof difficult to access from the outside?
- ▲ Is there sufficient lighting, externally and internally?
- ▲ Is there a suitable location for a safe?
- ▲ Is there a suitable shelter, in case of armed robbery, attack or fighting in the vicinity? A shelter should preferably be behind thick walls and out of sight of any window. Sometimes a central room or inner corridor is suitable. (See Annex 33 for more details on shelters.)
- ▲ Is there storage for valuable items?
- ▲ Is there an alarm system?
- ▲ Are there sufficient fire safety measures, such as smoke alarms, fire alarm, primary and secondary escape routes? (See Annex 12 on fire safety procedures.)
- ▲ Are electrical installations sound and safe?
- ▲ Is there sufficient parking, and will vehicles be secure?
- ▲ If there is a threat of car bombs, is there sufficient distance from the building to the parking area?
- ▲ If there is a threat of any kind of bombs, consider measures such as concrete barriers, blast film for windows, police control of vehicle access. In such cases specialist advice on protection from

BUILDINGS AND SECURITY

A1

bomb threats should normally be sought.

- ▲ What improvements will you need to make before the building is secure enough for your use? How long will they take? What will they cost? For example, will blast film be needed for the windows? Do any walls need strengthening around the shelter?
- ▲ How many guards will be necessary? Is there a shelter for them?
- ▲ Will you place a sign on the building to show that it is occupied by a humanitarian organisation, and if so how prominent should it be? This depends on the local situation and the perceptions of local groups about your organisation.

Local infrastructure

- ▲ What is the state of the roads leading to the building?
- ▲ Is the power supply reliable? If not, how big a generator will you need?
- ▲ Is the water supply reliable? If not, will you need to install your own water system?

Arrangements for receiving visitors

- ▲ Is there a place where visitors can wait? Will it be easy to control visitors?
- ▲ Reception staff – where will they be and how many will you need?
- ▲ Can visitors be seen before the gate or door is opened?
- ▲ Which areas should be accessible to visitors?
- ▲ Will visitors need to be escorted within the building?
- ▲ Will visitors' identity badges be needed?
- ▲ Will designated visitors' hours be needed?
- ▲ Striking the right balance between security and courtesy: making visitors feel welcome without compromising security
- ▲ Location of meeting rooms

Identity of the owner

- ▲ Who is the owner? Is he or she reliable and of good reputation? Does he or she have connections that you should be aware of?

CHECKPOINTS

A2

Checkpoints are widely used in many countries. Many checkpoints have a legitimate purpose, for example to prevent weapons from entering an area. Some checkpoints have little purpose other than to harass. Some checkpoints are used – for example by bandits or undisciplined soldiers – as a cover for ambush, theft or violence.

Staff should be trained and briefed on how to handle themselves at checkpoints. The best approach may vary from situation to situation. Often the following points may be helpful:

- ▲ When approaching or leaving a checkpoint, inform base by radio. Do so in a discreet way, far enough from the checkpoint to avoid them seeing that you are using the radio.
- ▲ Turn the radio to low volume or off, to avoid it attracting attention at the checkpoint
- ▲ Observe the checkpoint from a distance, without stopping, to understand what is happening there. Does everything appear normal? Or are there signs that there may be a problem?
- ▲ If you suspect that there is a risk of violence or other serious problems, turn round and drive steadily away, if it is safe to do so
- ▲ All passengers should remove sunglasses before arriving at the checkpoint
- ▲ Keep valuables out of sight. It is best to travel without valuables, if possible.
- ▲ If it is at night, switch off headlights, leaving sidelights on, and switch on the interior light so that the checkpoint can see the vehicle occupants
- ▲ Approach the checkpoint slowly and stop several metres before the barrier
- ▲ Remain inside the vehicle unless you are ordered to get out
- ▲ Make no sudden movements. Even moving your hand to release the seat belt could sometimes be interpreted as reaching for a weapon – so announce what you are doing before you do it, and move slowly.
- ▲ If one person is asked to come away from the vehicle, for example to an office to check papers, consider whether it is safer for another person to accompany them
- ▲ Be ready to answer questions about the occupants, your journey, the vehicle and anything in it
- ▲ One person should be nominated to do the talking, on behalf of all the occupants, unless questions are put directly to other occupants
- ▲ Your manner and style are very important: be courteous and friendly, but not over-familiar. Treat the soldiers or police as human beings. They have a boring job to do, and are likely to give you an easier time if you show an interest in them. If appropriate, chat a little, perhaps about their family. If they ask you to do things that are incorrect (such as to give them a present), be politely firm in refusing, and use gentle humour if appropriate. (See Annex 4 for suggestions on how to avoid bribes.)
- ▲ Be ready to show any relevant documents including vehicle documents, authorisations, copies of passports and ID cards. If possible, avoid showing the original of your passport, to avoid it being stolen – but in some cases the original may be required. It may be helpful to keep your ID card on a chain around your neck so that you can show it without surrendering it.
- ▲ If you suspect that the checkpoint may have a hostile intention, depending on the circumstances it may be sensible to keep all doors including the cargo door locked, with windows more than half-way up. But in some circumstances this may anger soldiers or police, so use your judgement as to which is best.
- ▲ Allow the car to be searched if they insist on it
- ▲ Some organisations have to use sensitive documents for their work. Do not carry sensitive documents if you can avoid it. If you must carry them, and if you are searched, you may try to insist that they do not see them. But if they threaten you, you will have to give in. Therefore keep documents out of sight, so as not to attract attention.
- ▲ If threatened with a weapon, comply calmly with their instructions
- ▲ When leaving the checkpoint, turn the radio volume up and inform base that you have passed the checkpoint
- ▲ If not allowed to pass through, return to your base and report to your team leader. He or she is then likely to negotiate with relevant authorities for a resumption of free movement in the area.

CHECKPOINTS

A2

- ▲ Have a clear policy on giving lifts. Humanitarian staff are often asked to give lifts to soldiers at checkpoints, armed or unarmed. Most humanitarian organisations forbid giving lifts to any military personnel. Ensure everyone knows how to respond in such a situation as well as a situation when a soldier is injured and needs medical assistance. If necessary, be prepared to turn back.

CONVOY PROCEDURES

A3

A convoy is a group of vehicles travelling together. This can be advisable when individual vehicles are at greater risk of theft or violence. If required and if appropriate, a convoy may be escorted by a police or military escort. Humanitarian organisations will usually try to avoid the need for a military or police escort, because of the risk that it will compromise their independence in the eyes of local people. Instead they rely on negotiation with local leaders, while preferring that legitimate security forces provide security for the whole area rather than just a particular road.

See Annex 13 for some issues concerning armed guards, which may also apply to convoy escorts.

Convoy procedures should be adapted to the local circumstances. The following checklist may serve as a prompt of some major issues to consider:

- ▲ Communications arrangements
- ▲ How should vehicles and occupants react if they come under fire?
- ▲ What to do in the event of accident, incident, casualty or breakdown
- ▲ Checkpoints and roadblocks
- ▲ Identification of vehicles
- ▲ Number of vehicles (from 4 to 6 vehicles are easily manageable)
- ▲ Order of travel
- ▲ Spacing between vehicles
- ▲ Roadworthiness of vehicles
- ▲ Equipment for each vehicle
- ▲ Documents required
- ▲ Stop and check loads and tyres how often?
- ▲ Convoy leader normally in front vehicle
- ▲ Assistant convoy leader normally in rear vehicle
- ▲ Slow vehicles in front; fast vehicles behind
- ▲ All vehicles to travel at the speed of the vehicle following
- ▲ Speed
- ▲ Halts
- ▲ Leave at the office a travel authorisation form giving intended and alternate routes and expected arrival times
- ▲ Inform authorities, and warn checkpoints ahead
- ▲ Is there a need to send an advance party, to check the route and prepare reception of convoy?
- ▲ Liaison with security forces in escort, if applicable
- ▲ Plenty of time allowed
- ▲ All staff should be fully briefed on the convoy procedures and plan

CORRUPTION: AVOIDANCE AND PREVENTION

A4

Corruption can threaten security. This is obvious in the case of theft or fraud, two kinds of corruption. It is just as true, though sometimes less obvious, in the case of other kinds of corruption, such as bribery.

Any kind of corruption risks:

- ▲ Loss of goodwill from the local population
- ▲ Loss of honesty in relationships between colleagues or organisations, and therefore loss of reliability of information when passed between them
- ▲ Loss of trust between colleagues or organisations, and therefore loss of reliable allies when danger threatens
- ▲ Pressure and stress on staff, often particularly national staff

Reasons to avoid any kind of corruption include:

- ▲ It is usually against the law, and aid workers are bound by the law in the country in which they are working
- ▲ Corruption is something that hurts the poor by denying them free and fair access to the services that they are entitled to
- ▲ Humanitarian organisations are bringing in free help for people who need it, and it is morally wrong for officials to try to divert some of the resources intended for the needy
- ▲ Any corruption encourages more corruption

Even the perception of corruption, or false accusations of corruption, can cause the same negative effects as real corruption. Great care should therefore be taken not to allow any perception of corruption to arise in connection with humanitarian organisations.

In some countries the state has virtually ceased to function, and officials such as border police have received no salaries for months, sometimes years. In these cases a system of charges provides them with an income. Aid agencies will sometimes regard this as necessary and understandable. In this case they may discuss the issue together, and agree on a joint position that ensures that everyone pays the same charges for the same services, and gets a receipt for

any money paid. This compromise approach at least ensures that there is some accountability and transparency.

Anti-corruption measures include:

- ▲ Clear, open, honest relationships with all local groups, with the local authorities and with other humanitarian organisations
- ▲ Good financial procedures
- ▲ Appropriate, transparent rules for procurement
- ▲ Well-trained, experienced staff
- ▲ Good management of staff and projects
- ▲ Confidential, anonymous whistle-blowing channels (for the reporting of corruption)
- ▲ A common position among humanitarian organisations, if possible, on what 'informal fees' should be paid, if any
- ▲ A refusal to pay bribes at any time

Many experienced humanitarians have found it possible to work for years in countries that have serious corruption, without ever paying a bribe. There are respectful and courteous ways of doing this. Consider the following, if appropriate to your personality, to the context and the culture:

- ▲ In answer to the question: "Have you got a little present for me?" answer: "Yes – a smile" – and smile genuinely as you do so
- ▲ Good humour, the time to talk for a minute or two and have a joke together – these are some times quite sufficient to persuade a soldier at a checkpoint not to insist on a bribe. Often he is bored, and is grateful to be treated as a human being.
- ▲ Explain why you are not able to pay the bribe. Have various simple phrases that do not sound like an accusation of corruption for example: "My head office doesn't allow me to pay any fee that isn't official."
- ▲ If a soldier is insistent, say that you are not able to pay the bribe, but that you are willing to speak to his commander. (The soldier will often not want his commander involved.)

CORRUPTION: AVOIDANCE AND PREVENTION

A4

- ▲ Be prepared to wait. Patience cures many problems, while impatience often increases the pressure to pay a bribe. At a checkpoint when you have reached an impasse, be prepared to wait an hour or two, while you keep negotiating politely, if it's important to you to get through. Otherwise, consider turning back, and trying again another day. In the meantime, you could inform the higher military or police authorities of the problem that you faced, and get them to do something about it.
- ▲ The patience principle also applies to bureaucratic processes, such as NGO registration with the government authorities. In some countries this can take a year or more, leading to a temptation to try to hurry the process up.
- ▲ Remain courteous, respectful and – if possible – friendly. Some officials who normally insist on a bribe seem flattered and pleased when treated kindly, and waive the bribe as a result.
- ▲ Ensure that all your paperwork and documents are in order, and that you have copies of them with you at all times, so that if an official challenges you, the document is there to show. This may mean always having a bulky folder with you – a small price to pay to avoid the hassle that you might otherwise face.
- ▲ Keep some picture postcards with you, and give one of them as a “present” of minimal value
- ▲ Some people like to keep a packet of cigarettes on them – even if they themselves don't smoke – so that they can offer one (or two or five!) to the soldier at the checkpoint
- ▲ Ensure you or your driver knows the traffic rules and respects them. Otherwise it is an open invitation to a policeman or traffic warden to threaten dire penalties – unless you offer a bribe.
- ▲ Make sure that you and your colleagues respect the laws scrupulously, so that you are less likely to be accused of wrongdoing and therefore put in the power of law enforcement officials

Managers should lead by example in preventing and avoiding corruption, and should ensure that all staff follow this lead.

CULTURAL AWARENESS

A5

If staff are aware of the local culture or cultures in which they are working, they are likely to be more secure. They will understand more clearly what is happening around them. They will be able to show respect to local people and leaders, and communicate with them, more effectively. They will win greater local goodwill.

All international staff should be briefed on the culture(s) in which they will be working, preferably both before arrival and on arrival in the field. It can be very helpful to have a written brief on the local culture(s) to give staff before they deploy.

Often overlooked is that nationally-recruited staff also need to be briefed on the culture(s) of the international staff alongside whom they will be working, and on the culture of the organisation which is employing them.

There have been many cases of humanitarian staff becoming deeply frustrated with their colleagues, or with local people and leaders, essentially because they have not been properly briefed on their cultural differences. Humanitarian programmes run more efficiently, including their security aspects, when there is mutual understanding.

A few examples will serve to underline the importance of cultural awareness:

- ▲ In some cultures it is important to receive any gift with the right hand. Offence is caused if a gift is received with the left hand.
- ▲ In some cultures it is normal, and not impolite, for local people to:
 - Stop and stare at foreigners
 - Shout "foreigner" at foreigners they see in the street
 - Ask personal questions of strangers, such as how old they are, or how much they earn
- ▲ In some cultures two fingers held up in a V shape means "cool"; in others it means "victory"; in others it means you support one particular side in the conflict
- ▲ In some cultures it is insulting to show the sole of your shoe to another person, for example when your legs are crossed

- ▲ In many cultures it is important to take plenty of time to greet people, engaging in "small talk", before talking about work. In other cultures it is seen as a sign of inefficiency to "waste" time on small talk.
- ▲ The acceptable way to greet men and women differs greatly between cultures
- ▲ Sexual relationships between team members, or with individuals in the community, would in some cultures be offensive to local laws and customs, and in some cases could put the team at risk
- ▲ In some cultures it is not acceptable for female staff to work closely with male staff, or to travel alone with male colleagues
- ▲ In many cultures it would be unacceptable for a male aid worker, driving alone, to give a lift to a girl or woman: the aid worker would be suspected of wishing to exploit her

In almost all cases, it is important to take time frequently to chat to people, in their homes, on the street, in their offices, in the market. This helps your understanding of the whole environment, and so improves the likelihood of good programme and security decisions.

If staff turnover is rapid, particularly of international staff, it is more likely that they will have a weak understanding of the local culture(s). Programme and security decisions are therefore likely to be weaker. Greater staff continuity, in most cases, is likely to improve the standard of security management.

Equally, a thorough handover process between outgoing and incoming staff reduces the amount of knowledge and cultural understanding that is lost when a staff member leaves.

DRIVERS: A BASIC CHECKLIST

A6

Road accidents are one of the most common causes of death and injury for humanitarian staff. Good security procedures are seriously undermined if road safety is ignored.

Ensuring that drivers are competent and disciplined greatly reduces the risk of accidents. It is essential for managers to take sufficient time, especially at the outset of an operation, to make certain that drivers are aware of their duties, properly prepared for them, and are disciplined in carrying them out.

Stop to consider if a road journey is necessary. Can you do the same task using telecommunications or some other method? By cutting out unnecessary road journeys you reduce the risk of accidents.

In particular, anyone travelling in a vehicle which is being driven too fast should insist that the driver slows down to a reasonable speed.

Other causes of accidents include:

- ▲ Driver sleepiness
- ▲ Using a radio or telephone while driving
- ▲ Consumption of alcohol within 12 hours before driving
- ▲ Use of some medicines or other drugs
- ▲ Poor vehicle maintenance
- ▲ Poorly trained or inexperienced drivers
- ▲ Bad weather
- ▲ Time pressure – for example, when driving to meet a deadline such as a border or checkpoint closure, or a curfew time

It is good practice for drivers to have a checklist to help them remember their routine duties. Managers should hold drivers accountable for fulfilling the tasks on their checklist.

Local circumstances will dictate what the checklist should include. As an example, a checklist might contain:

Daily vehicle checks

- ▲ Fuel – preferably full. Always keep at least half-full in case of emergency.
- ▲ Oil
- ▲ Coolant

- ▲ Brake fluid
- ▲ Water
- ▲ Tyres
- ▲ Spare wheels
- ▲ Tools: tow-rope, jack, wheel brace etc
- ▲ Full vehicle equipment (see Annex 42 for a vehicle equipment checklist)
- ▲ Screen-wash fluid
- ▲ Wipers
- ▲ Lights
- ▲ Horn
- ▲ First aid kit
- ▲ Fire extinguisher
- ▲ Spare fuel
- ▲ Spare water
- ▲ Torch/flashlight
- ▲ Map, and compass if necessary
- ▲ Paperwork including vehicle log; vehicle registration and insurance documents (or copies, depending on local requirements); travel authorisation form
- ▲ Radios – working? Antennas in good condition?
- ▲ Winch (if fitted) – working?

Travel authorisation

- ▲ Get travel authorisation form signed
- ▲ Inform office on departure

Road safety

- ▲ Plan the journey
 - Not impaired by alcohol or drugs
 - Avoid driving when likely to be sleepy
 - Plan to share the driving if possible
 - Ensure you will be well rested
 - Book an overnight stop if necessary
 - Plan the route, and alternative routes if necessary
 - Plan when to take rest breaks – at least every 2 hours
 - Anticipate delays
- ▲ Safe and legal speed
- ▲ Defensive driving
- ▲ Know your location at all times
- ▲ Passenger comfort
- ▲ Consideration for other road users including pedestrians
- ▲ Particular care when children are nearby: slow

DRIVERS: A BASIC CHECKLIST

A6

- ▲ down and given them a wide berth
- ▲ If you start to feel tired, find somewhere safe to stop, nap for 15 minutes or more, take two strong caffeine drinks
- ▲ If the vehicle malfunctions, or you hear an unusual noise, stop and get a qualified person to check it. Driving on could seriously damage the vehicle.
- ▲ Do not give lifts to strangers, nor to military, police or armed personnel

EMERGENCY CONTACT CARD

A7

It can be helpful for staff in the field to carry a small emergency contact card in their wallet or purse. In most cases it is good practice for staff to carry the security plan with them at all times. But an emergency contact card may be easier to reach in an emergency, and can provide vital information such as telephone numbers if the security plan is lost. It can also be particularly helpful for visitors to the field.

An emergency contact card should be designed to suit the particular circumstances. Information on it could include, for example:

- ▲ Callsign of base station
- ▲ Radio calling channel
- ▲ Radio emergency channel
- ▲ Important phone numbers
- ▲ How to call for help in an emergency – brief summary
- ▲ Location and contact details of medical facilities
- ▲ Phone numbers and other instructions for Medevac

Ideally the card should be covered in plastic so that it is durable and waterproof.

EQUIPMENT FOR PERSONAL SECURITY

A8

Personal equipment that may enhance your security will vary depending on the circumstances. The following list gives a number of items that can often be helpful. Remember that any equipment needs to be properly used in order to do its job of enhancing security. In some cases this will require training or supervised practice.

Items that are usually essential in all environments are in **bold**.

- ▲ Adaptors for electrical sockets
- ▲ Alarm, such as a rape alarm or aerosol fog horn
- ▲ Body armour*
- ▲ **Clothing suitable to the environment you will be working in**
- ▲ **Documents** (carried in a durable document wallet) including:
 - Passport and/or identity card, driving licence and vaccination certificate (keep photo copies of these in a separate place, or carry copies and keep the originals in a separate place)
 - Copies of any important authorisation documents
 - The relevant security plan
 - Emergency contact details
 - Insurance certificate and emergency insurance phone numbers
 - Spare passport-size photos
- ▲ **E-mail communications** – typically a laptop computer and telephone landline, mobile or satellite phone
- ▲ **First aid kit** (see Annex 14 for information on first aid kits)
- ▲ Flashlight/torch
- ▲ Helmet*
- ▲ Insect repellent
- ▲ **Map**, preferably laminated or in a map case
- ▲ Map-marking pens
- ▲ Mobile phone and charger
- ▲ **Money belt**
- ▲ Mosquito net
- ▲ **Notebook and pens**
- ▲ Radio, short wave and FM, for listening to international and local news, plus spare batteries and/or charger
- ▲ **Radio, two-way**, plus spare battery and charger
- ▲ **Surge protector** (to protect electronic equipment when connected to unreliable power supply)
- ▲ **Watch** (robust and reliable, not valuable)
- ▲ Water bottle
- ▲ **Waterproof coat**
- ▲ Water purifying tablets
- ▲ Whistle

* Body armour and a helmet are normally only needed in high-risk circumstances. Many humanitarian organisations would assess that, if such protection measures are necessary, the situation is too dangerous for their staff to be present at all. Therefore these items are only rarely used by humanitarian staff.

EQUIPMENT FOR TEAM SECURITY

A9

Team security equipment will vary depending on the circumstances. The following list gives a number of items that can often be helpful. Remember that any equipment needs to be properly used in order to do its job of enhancing security. In some cases this will require training or supervised practice.

- ▲ Alarms – for issue to each building
- ▲ Battery chargers and other accessories
- ▲ E-mail system, tested and proven
- ▲ First aid kits (bear in mind the quality of local medical facilities when deciding what the first aid kits should contain)
- ▲ Foghorns (the aerosol can type, cheap and very effective)
- ▲ Generators
- ▲ Identifying stickers or flags, as appropriate
- ▲ Lighting equipment
- ▲ Maps of good quality and appropriate scale
- ▲ Money belts
- ▲ Padlocks
- ▲ Radios
- ▲ Safe(s) – should be capable of being fixed securely to floor or wall
- ▲ Security manuals or handbooks
- ▲ Smoke alarms
- ▲ Telephones: mobile or satellite. Remember that mobile phone networks may be shut down during emergencies.
- ▲ Torches/flashlights
- ▲ Vehicles, equipped as required (see Annex 42 for a suggested list of vehicle equipment). All vehicles used, whether owned or hired, should be thoroughly checked for roadworthiness and correct equipment by a competent mechanic.
- ▲ Vehicle spare parts
- ▲ Whistles for guards (or aerosol fog-horns)

EVACUATION

A10

The following suggested procedure may be of help in designing your own evacuation plans and procedures. It should be adapted as required by your particular situation.

PHASE ONE - PLANNING STAGE

Evacuation planning and rehearsals should be carried out regularly. History has shown that the safety and security situation can deteriorate rapidly, often without warning. The evacuation plan should be written, and an outline included as a section within the security plan issued to all staff. When writing the evacuation plan, at least the following issues should be considered.

Who will be evacuated - It is essential that all staff members clearly understand their and their families' eligibility for evacuation or relocation assistance. Each field team should determine which staff members are 'essential'; essential staff members are those required to conduct final coordination (Finance Officer for example), office closure, or limited, basic operations. Determine the evacuation order with Priority 1 evacuating first and Priority 4 last.

Priority 1 – International staff family members
Priority 2 – Staff members who are in immediate personal danger due to the conditions of the crisis
Priority 3 – Individuals other than essential staff
Priority 4 – Essential staff

Where will staff be evacuated to? Identify a first-choice destination and an alternate destination for evacuation or relocation. Determine visa requirements, and the logistics that will be needed upon arrival at the destination(s).

How will staff be evacuated? Establish a notification system to ensure everyone is informed of the impending evacuation. Determine and verify an assembly point where staff will gather after notification. Detail the method of evacuation (over land, by air or by sea). Identify potential evacuation routes to airports, seaports, or land borders. Check to ensure that these routes can be travelled under emergency conditions. Inspect border crossings and safe areas. Coordinate plans with embassies, UN agencies, and

other NGOs as appropriate.

What goes and what stays? Identify which documents, such as contracts, payroll records, etc., will be needed to re-establish operations once relocated or upon re-entry. Other documents should be marked for destruction, or left behind, as appropriate. Consider how evacuated documents will be perceived if seized by a particular person or group. They may contain information that could put the evacuating individual(s) at risk due to misinterpretation, and would be better destroyed or left behind.

Who is responsible for the various tasks during an evacuation? During crises key staff will be fully occupied so it is imperative that tasks and responsibilities for evacuation be clearly defined during the planning stage.

What will be the expected impact of evacuation on the operation? Will the office be closed and, if so, how? What are the policies and plans for continuing operations through national staff members acting on their own? Or through contractors, if feasible and appropriate?

PHASE TWO - ALERT

Mounting tensions and/or instability may lead the team leader, in consultation with HQ, to issue a recommendation to limit operations, increase security measures, and review the evacuation plan. Work outside the immediate vicinity of the field office may be suspended. Tasks during this stage include the following.

- ▲ Brief all national and international staff on the situation, if possible
- ▲ Communication systems for notification of staff should be finalized and tested. Consider tying into other systems, such as warden systems for other NGO, UN or embassy staffs.
- ▲ Prepare salaries and other money required by national staff
- ▲ Back up important files onto disks, delete sensitive files, and destroy sensitive documents. Be aware that deleted files still remain on a disk, and can be retrieved by computer specialists.

EVACUATION

A10

- ▲ Staff members and their family should check that they have personal documentation with them at all times
- ▲ Inventory all office equipment and assets. As appropriate, identify the equipment to be evacuated and responsibility for each item. Plan how high-value equipment which will remain should be hidden or protected.
- ▲ International staff families should be considered for an early departure
- ▲ Potential evacuees should assemble personal belongings to be taken during an evacuation, including:
 - Passport and visa
 - Driver's licence and other identification
 - Extra cash (convertible currency)
 - Hand-held radio with extra batteries
 - Contact list
 - Any medical essentials
 - Torch/flashlight with extra batteries
 - One bag of personal belongings not exceeding 15 kg
- ▲ Potential evacuees should ensure that they do not take with them any information or equipment that might be interpreted as incriminating (e.g. reports of military movements; pictures on disk or paper of any security-related subjects)
- ▲ Stock the assembly area with appropriate supplies, including the following:
 - Food
 - Water
 - Candles and matches
 - Toilet and related supplies
 - Power source
 - Communications equipment
 - Torches/flashlights
 - Cooking equipment
 - Reading material
 - Spare fuel for vehicles
- ▲ Assign each evacuee to a specific vehicle so that anyone missing may be readily identified, and ensure that all vehicles are ready

PHASE THREE - EVACUATION IMMINENT

The field office usually suspends the majority of normal operations to concentrate on evacuation prepara-

tions. Potential evacuees may be relocated to a pre-selected staging or safe area. Remote staff may be recalled or relocated. Staff currently outside the region should remain in a safe place. Non-essential personnel and family members may be evacuated. Tasks during this phase, which may last weeks or only a few hours, include:

- ▲ Keep all staff fully informed.
- ▲ Coordinate closely with embassies, other NGOs, the UN, and other agencies as appropriate
- ▲ Pay salaries to local staff, with salary advances if possible
- ▲ Hide high-value property which will remain. Options may include distributing among trusted staff if it will not put them at unacceptable risk; hiding in roof spaces; or burying. Remove logos from vehicles which may be stolen. Ensure you keep copies of serial numbers of high-value equipment.
- ▲ Give clear instructions regarding responsibilities and leadership roles to those staff staying behind. Establish a means of continued communication between remaining staff and those evacuating. Provide authorisation documents to key national staff, if necessary.

PHASE FOUR - EVACUATION

Once evacuation or relocation has begun, it should take precedence over all other activities. The field office may continue operations through national staff, or contractors if appropriate, or may close completely. Considerations during evacuation may include:

- ▲ If there is a risk of looting, consider disabling radios, equipment and vehicles. Empty and leave open all safes.
- ▲ Ensure effective communication with national staff left behind
- ▲ All evacuees move to pre-designated assembly area
- ▲ Evacuate by the safest means possible, maintaining good order and remaining in communication with all groups evacuating
- ▲ Keep in contact with key national staff, as far as possible

EVACUATION

A10

- ▲ Once evacuation is complete, inform HQ, relevant embassies, and key national staff

The evacuated personnel may manage operations from outside the country, communicating with and working through the national staff (or contractors) if possible. If a decision is made to close the office completely, care will be needed to ensure humane and correct termination or reassignment of staff contracts and the disposal of assets.

SPECIAL CONSIDERATIONS DURING EVACUATION

An evacuation is not easy for the evacuees or for those staying behind. It is a very emotional event, giving rise to feelings of guilt, hurt, frustration, and powerlessness. The departure of international aid agencies can have a variety of meanings to the local population, including the removal of a symbolic or real safety barrier. Thus, an evacuation is not a neutral act and may even aggravate a crisis. When a field team evacuates it should consider providing a statement for the media and others explaining the organisation's reasoning and any continuation or possible resumption of programmes.

Self-evacuation. Individuals that are working remotely from a local office, or who find themselves isolated during a crisis should use their judgement concerning the safety in their area. All staff members should be authorised to evacuate on their own authority, in accordance with established criteria and procedures, when they feel their safety is threatened. Every effort should be made to communicate with their manager during the process, and once in a safe area the individual must contact their manager or HQ immediately. No one may re-enter an area after evacuation without specific authorization from their team leader.

Evacuation refusal. Staff who are instructed to evacuate or relocate, and who refuse, may face disciplinary action including dismissal, depending on the policy of their employer. They are likely be considered as staying at their own risk, with their employer taking no further responsibility for their safety.

National staff evacuation or relocation. Most humanitarian organisations have a policy of only evacuating international staff. If the field manager believes that some or all national staff and/or their families face a direct threat, then they may be obliged to consider organising or assisting their evacuation or relocation.

Return and resumption of activities. This may occur soon after evacuation or take a long time. Re-establishing operations after an evacuation can be difficult. National staff who did not evacuate may have experienced hardship and threats to themselves and their families. They may resent this. Restoring relationships with staff, local authorities, beneficiaries, and the local population can be made easier if honesty, tact, and transparency are used prior to and during the evacuation, and on return.

FINANCIAL SECURITY

A11

Robust financial procedures are vital. Without them, fraud or theft are much more likely. If theft occurs, not only does the field operation suffer but there can be an increased risk of violence to staff, since thieves may use violence.

All humanitarian operations should include a manager able to manage financial procedures in the field, and to ensure financial security. He or she should be equipped with strong financial procedures, and trained in their use.

Good financial management is a large subject, beyond the scope of this Guide. Detailed advice on financial procedures, including simple guides to NGO accounting, can be found at www.mango.org.uk.

All field managers should be aware of the basics of good financial security. Points that they should watch out for include:

- ▲ A properly trained and briefed bookkeeper, accountant or financial manager, appropriate to the size and type of programme, should be present from the start, including during the planning of the operation
- ▲ Minimise the amount of cash held in the office, or carried by any staff member
- ▲ Reduce the use of cash to a minimum, preferring bank transfers or cheques where possible
- ▲ Require receipts for all cash movements in or out, however small. Ensure that all staff know the procedure, and understand the reasons for it. Take disciplinary action against any who do not follow it.
- ▲ Establish strict procedures for authorising expenditure, in accordance with the organisation's financial policy, and for depositing or withdrawing money from the bank or safe.
- ▲ Ensure that there is correct "separation of duties", as required by normal financial good practice. For example, different people should be responsible for ordering, receiving and paying for goods.
- ▲ Maintain proper cash control, including regular and frequent cash and bank reconciliations
- ▲ Secure the safe(s) by bolting them to wall or floor; locking the room in which they are kept; and restricting access to the building
- ▲ Insist on regular audits
- ▲ If large sums of cash are required on certain days, for example pay day, consider reducing the risk of theft by:
 - Bringing the cash from the bank on the day, rather than storing it overnight in the office
 - Varying the time and route used to bring the cash from the bank
 - Designating two or three staff members to withdraw the cash in two or three parts, bringing it to the office via different routes at different times
 - Storing the cash in several different locations, so that not all the cash is lost if there is a theft
 - Having more than one pay day per month, so that a smaller amount of cash is needed on each pay day
- ▲ Limit the amount of cash that can be carried by an individual
- ▲ Ensure that all staff know that they must not risk their lives to protect cash
- ▲ Staff should never talk or boast of their cash transfer experiences
- ▲ If large sums of cash have to be transported, ensure that the only people aware of this, including staff, are those who need to know, and who are trusted. If this is a frequent occurrence, vary the route, the timing and the method of travel so as not to create a predictable pattern.
- ▲ Procedures for changing money from one currency to another should be safe and legal
- ▲ Requests for money transfers should be kept confidential
- ▲ Beware of confidence tricksters. For example, check that someone claiming to represent an organisation to whom you are paying money, does in fact represent them.
- ▲ In general rushed financial transactions are more vulnerable to errors and fraud. Wherever possible, insist that all normal procedures are followed without exception.

If there is a serious failure in financial security, leading to a significant theft or fraud, it is essential that

FINANCIAL SECURITY

A11

the relevant staff – particularly the relevant managers – are held to account. It is difficult to hold them to account if they were never properly trained or equipped, which is one reason why good training and equipping are so important.

Any significant theft or fraud should be reported. It should be investigated by a manager senior to, and independent from, the team in which the incident occurred. He or she should produce a written report stating the facts, as far as they can be discovered; assigning responsibility, as far as it can reasonably be assigned; and making recommendations for improvements to financial systems and disciplinary action, where appropriate.

A procedure requiring such an investigation should be included in the financial manual of all humanitarian organisations. Failure to ensure full accountability in the event of a significant theft or fraud undermines the integrity of the organisation, and is likely to damage donor confidence.

FIRE SAFETY

A12

Good fire safety precautions include:

- ▲ Assessing all buildings for fire safety
- ▲ Ensuring there are sufficient fire escape routes
- ▲ Emergency exits should have emergency exit keys, preferably glassed-in in a box, near to the exit but hidden from exterior view
- ▲ Designating fire assembly points outside all buildings
- ▲ Fitting smoke alarms (smoke alarms are cheap – about US\$10 at the time of writing – and are an effective way of saving lives). Accommodation buildings should normally have smoke detectors in all rooms except bathrooms and kitchens.
- ▲ Equipping buildings, and vehicles where necessary, with fire extinguishers
- ▲ Training staff in the use of fire extinguishers
- ▲ Rehearsing an evacuation of the building
- ▲ Ensuring all staff know the procedure for calling for help in a fire (bear in mind that there may be no fire brigade)
- ▲ Storing flammable materials correctly, and away from buildings

Fire poses a significant risk to health and safety, especially in countries where there is no fire brigade, buildings are not built to minimize fire hazards, and few people have fire-safety training. Fires in offices, warehouses, and residences can prove catastrophic and the threat of fire should be addressed in all safety and security assessments. Most fires start small and can be extinguished if detected early. The best method for fighting fires is prevention through regular inspections, staff training and properly maintained fire-fighting equipment in all facilities.

IMMEDIATE ACTION FOR FIRE RESPONSE

It is important not to panic when confronted with fire. There are many things that can be done to prevent a fire from spreading and minimize damage and potential loss of life. The steps to take are:

- ▲ Sound the alarm. Shout for help, summon aid, activate the fire alarm. Do not attempt to fight the fire until the building evacuation is initiated.

- ▲ Determine the cause of fire and what is available to fight it. If it is an electrical fire, it is important to first turn off electricity, if possible.
- ▲ Attempt to fight the fire but under no circumstances risk injury in the process
- ▲ If successful, continue monitoring the site to prevent flare-ups until help arrives
- ▲ If unable to fight the fire, evacuate quickly, closing doors and windows, if possible, ensuring no one remains in the building
- ▲ Give information to and cooperate with the fire brigade when they arrive

FIRES IN BUILDINGS

Fires in buildings can spread quickly, trapping people inside. It is important to respond immediately to any fire alarm or evacuation order. Do not assume it is a practice drill. Staff should plan ahead and learn the emergency exit routes from residences and offices. In hotels or when travelling, look for the suggested evacuation route and rehearse it, if necessary. When evacuating a building remember the following:

- ▲ Think ahead what the route will look like – smoke may obscure vision
- ▲ Do not take the lifts/elevators – use the stairs
- ▲ Cover yourself with a non-synthetic blanket, coat or other cloth, preferably wet
- ▲ Before opening doors, feel the door for heat. There may be fire on the other side that will flare when the door is opened.
- ▲ Avoid routes that are exposed to falling objects
- ▲ Stay low and move as quickly as possible. It may be necessary to crawl to avoid smoke and heat.
- ▲ Jumping from more than two stories can be fatal and should only be a last resort. If unable to exit a tall building, make your way to the roof. Offices or residences should not be located in tall buildings that do not have adequate means of evacuation during emergencies.

If in a burning building, it is important that evacuation is not delayed for any reason. Remaining inside should only be an option when there is absolutely no means to escape. If unable to exit, prepare to remain in the building by doing the following:

FIRE SAFETY

A12

- ▲ Go to a room with an exterior window and mark it clearly to summon assistance. Stay in that room.
- ▲ Close the main entry door and any interior door to the room
- ▲ Place blankets and clothes at the base of the doors to keep smoke out. If possible, use wet cloth to make a better seal.
- ▲ If possible, wet non-synthetic blankets, coats or other clothes for possible use later
- ▲ Stay low near an open window and continue signalling for help
- ▲ If fire spreads to the room, get under two or more layers of blankets or clothes with the outer layers wet, if possible

IF A PERSON IS ON FIRE

If you or someone near you is on fire, remember - **stop, drop and roll.**

Stop. Don't panic and don't allow others to run about if they are on fire. Remove burning clothes, if possible.

Drop. Fall quickly to the ground or floor. If someone else is on fire, try to get them to do so. "Tackle" them only if you will not catch fire yourself.

Roll. Roll flat over and over (back and forth if in a room) until the fire is extinguished. The rolling will smother and scatter the fire in most cases. If someone else is on fire, have them roll. You can use water, sand, or a blanket to help smother the fire while they are rolling. Do not attempt to beat the fire out with bare hands; continue rolling instead.

Once the fire is extinguished, summon help and begin first aid.

GUARDS AND PRIVATE SECURITY COMPANIES

A13

Guards are necessary in many emergency relief situations. Humanitarian agencies have property that local criminals or armed groups, or simply hungry people, may wish to steal. There may also be risks to staff, who therefore need protecting.

A strong and happy team of guards can be a major help to the smooth running of a relief operation. Poorly managed guards can lead to theft, danger to staff, and extra burdens on managers. It is therefore worth investing time and effort to ensure that guards are managed well.

Recruiting

Recruiting good quality people is crucial to success. Do not take shortcuts: use the proper recruiting procedure. Insist on checking references before a new guard is allowed to start work. Make sure that the guards can speak the working language of the field team, so that all staff are able to communicate with them. It is good practice to agree pay scales for guards (and indeed other staff categories) with other relief organisations in the area, to avoid creating tension between guards working for different employers.

Induction

All guards should have a full induction, involving briefing, equipping, and training where necessary:

Briefing

Guards should be briefed clearly and thoroughly on their tasks. Do not assume that anything is obvious to them. Explain what the organisation does, and the values that it upholds. Describe the reputation that it wishes to have among local people. Make clear the importance of the guards, not only in protecting people and property but also in enabling the relief operation to help many others. Encourage them to feel part of the team.

Detailed briefing points should include:

- ▲ Most of the normal induction points that other staff would receive
- ▲ Their routine duties
- ▲ Hours and shifts
- ▲ The importance of remaining at their post even

if the guard due to take over from them does not appear

- ▲ How to communicate with their manager, and with other staff
- ▲ Action to take in the event of different types of incident
- ▲ How to deal with visitors
- ▲ The disciplinary system, and a warning that disciplinary action will be taken if a guard neglects his duties
- ▲ Guards should not risk their lives trying to protect property. Their role is to detect intrusion and to raise the alarm

Equipping

The appropriate equipment will vary according to the circumstances but may include the following:

- ▲ Identity card
- ▲ Torch/flashlight
- ▲ Whistle
- ▲ Aerosol fog horn or other loud alarm
- ▲ Radio and spare battery
- ▲ Battery charger
- ▲ Watch
- ▲ Coat
- ▲ Stick (if justified by the threat; locally appropriate; and if your organisation's policy allows it)
- ▲ Shelter
- ▲ Name badge
- ▲ Visitors' book

Recruiting a couple of dogs to accompany the guards can be a very effective deterrent to intruders, particularly in cultures where dogs are feared.

Training

Assess and provide for any training needs that the guards have. Radio voice procedure is likely to be one need. Rehearse with them the actions they should take in the case of the most serious security incidents such as armed robbery.

Managing guards

An experienced nationally-recruited staff member is likely to be the most appropriate line manager of the guards. He or she should keep a close eye on their performance, and should make random unan-

GUARDS AND PRIVATE SECURITY COMPANIES

A13

nounced visits to check that all is well.

In some situations it is almost standard practice for guards to sleep during the night. If this is the case, and if the security situation means that this would be dangerous, consider the following suggestions:

- ▲ Work out why they are falling asleep: for example, do they have a second job? Are their shifts too long? Do they have a long journey to and from work? Are they eating enough?
- ▲ Put two or more guards on duty overnight
- ▲ Appoint an overseer and hold him accountable for ensuring all guards stay awake
- ▲ Remove anything that could be used as a bed
- ▲ Summarily dismiss any guard found asleep on duty
- ▲ Shorten the length of shifts
- ▲ Visit guards unannounced in the middle of the night, so that they resist the temptation to go to sleep for fear of being caught

Private security companies

Many humanitarian organisations engage a local security company to provide guards. This is likely to be more expensive than employing guards directly. If the company is good, it can have several advantages including:

- ▲ Reduced administration: you do not need to recruit or manage guards
- ▲ Greater reliability: the company ensures that the guards are well trained and equipped, and turn up on time
- ▲ Replacement guards immediately available if one is sick or absent
- ▲ In many cases a quick reaction force is available, to respond to emergency calls (check whether the quick reaction team is armed, and if so, what you should do when you call them – e.g. lie on the floor, stay away from windows, etc.)
- ▲ Flexibility: easy to increase or decrease the number of guards, as the needs of the operation change
- ▲ No need to make guards redundant at the end of the operation

It is vital to check the reputation and efficiency of a private security company before making an agreement. Are their procedures suitable for an organisation like yours? Will they use force only when necessary? Who is liable for harm done when they do? What kind of arms do they use? Is the company, or is any of its owners, connected to individuals or groups that you do not wish to be associated with? Are they honest?

There can be disadvantages in using private security companies. They usually cost significantly more than employing your own guards, while paying their guards less than a humanitarian organisation would pay if employing them directly. Private security guards sometimes have no training for their role. Their presence can give the impression that a humanitarian organisation is cutting itself off from local people. In some cases the loyalty of their staff can be weak. Consider these and any other possible disadvantages before making your decision.

Armed guards

In a few extreme and exceptional cases, armed guards may be necessary and appropriate, if there is no other way to protect life and property adequately and if the humanitarian need justifies the continuation of the relief operation. Recent crises where most humanitarian organisations have used armed guards include Somalia and Chechnya.

If some humanitarian organisations use armed guards but others do not, those that do not can become greater targets while those that do can become associated with an implied threat of violence, and with a greater isolation from the local community. In a few situations, it may look 'out of place' **not** to have armed guards. If possible, all humanitarian organisations should reach the same decision on armed guards by consensus. They should consider how to minimise any negative local perceptions that might result.

In each case where armed guards are used, organisations should have a clear policy on their use. In particular, instructions for opening fire should be very clear to all concerned. Management of armed guards needs to be especially strict, with severe

GUARDS AND PRIVATE SECURITY COMPANIES

A13

penalties for misuse of weapons.

Because of the risk of misuse of weapons, some humanitarian organisations prefer never to employ armed guards directly, but instead to engage a private security company to provide them. See the discussion on private security companies within this Annex.

In some cases no security company is available, in which case the local police, military or paramilitary authority may provide them. If so, the question may arise whether they should be paid. There are differing views on this: some say they may need to be paid, particularly if they receive no salary and their commitment needs to be assured. Others say that any payment to police, military or paramilitary guards compromises independence, and/or may become a protection racket. The best answer will depend on the situation and the judgement of an experienced manager.

It is vital that the organisation supplying armed guards is reputable and reliable, and perceived as so among the local population. Check whether the organisation is connected to individuals or groups that you do not wish to be associated with.

In all cases, a senior manager at HQ should take the decision whether to deploy armed guards, and should do so having consulted with any other humanitarian organisations working in the same area. Before making the decision, managers must be convinced that armed guards will reduce rather than increase the risks to the organisation.

Other issues to consider include:

- ▲ Checking that the guards are capable of doing their job
- ▲ Strict discipline, including a ban on the use of drugs or alcohol
- ▲ What happens if and when the need for armed protection ends?
- ▲ What happens if a guard injures or kills someone?

HEALTH AND HYGIENE

A14

Healthy staff tend to be more efficient, alert and safe. Common illnesses among humanitarian staff include potentially fatal infections such as malaria. It is vital that humanitarian staff take good care of their health, and are rigorous about hygiene and other preventive measures.

All staff should normally undergo a medical examination before signing their contract. They should also undergo a medical examination after completing their contract. This both ensures that any medical problems can be dealt with, and helps to protect the organisation from false claims concerning medical problems resulting from the employment. It can also result in lower insurance premiums.

Staff should take qualified medical advice on health and hygiene precautions. Some of the most common are:

Health precautions

- ▲ Malaria precautions are essential, in areas where malaria is a risk. Malaria can kill, and often does. Take care to prevent mosquito bites. Precautions against malaria include:
 - Wear long sleeves, trousers and socks in the late afternoon and evening, to prevent bites
 - Wear insect repellent on any exposed areas of skin
 - Use a mosquito net correctly when sleeping
 - Burn anti-mosquito coils or tablets to kill mosquitoes inside buildings
 - Fit anti-mosquito netting to doors and windows
 - Take the appropriate malaria prophylaxis, on the advice of your doctor
 - Site buildings away from mosquito-breeding areas
- ▲ Vaccinations against serious diseases. Some countries do not admit foreigners without a certificate of vaccination.
- ▲ Verify the quality and capacity of local medical facilities. Ensure that all staff are aware of which medical facilities can be trusted, and their locations. A medical NGO may be able to provide emergency cover.
- ▲ First aid kits should be available in each building and vehicle, and may need to be carried by

staff. It is important that first aid kits are appropriate to the situation and kept up to date by a qualified person.

- ▲ Precautions against HIV/AIDS, including:
 - Availability of clean needles and syringes for medical purposes
 - Appropriate and responsible sexual behaviour
- ▲ Protection against the sun. Wear a hat, long sleeves and long trousers or skirt, and use sun protection cream.
- ▲ Avoid dehydration: drink enough. Carry a water bottle if necessary.

Hygiene precautions

- ▲ Clean water supply. If clean water is not guaranteed, filter water and boil for 5 minutes to make it safe for drinking.
- ▲ Keep a spare stock of water in case of failure of supply
- ▲ Keep a stock of water purification tablets
- ▲ Ensure food is sourced and prepared correctly
- ▲ Wash hands frequently, and before meals
- ▲ Ensure cooks wash their hands frequently while preparing meals
- ▲ Ensure kitchen, washing and latrine areas are kept clean
- ▲ Dispose of rubbish effectively
- ▲ Avoid eating fruit or vegetables that have not been thoroughly washed in clean water

First aid precautions

It is advisable for humanitarian organisations to have a policy on first aid, including:

- ▲ What level of first aid training should be required in field teams
- ▲ Which field staff should have first aid training
- ▲ What type of first aid kits should be held as standard procedure in:
 - Accommodation buildings
 - Offices
 - Warehouses
 - Vehicles

For advice on health, hygiene, first aid or any medical matter, always consult your doctor. Further information is available from:

HEALTH AND HYGIENE

A14

- ▲ World Health Organisation: see the section on International Travel and Health at www.who.int/ith
- ▲ Helpful travel health information website from the UK National Health Service, at www.fitfortravel.nhs.uk - see particularly the A to Z Index there
- ▲ *Travellers' Health: How to stay healthy abroad*, a book edited by Dr Richard Dawood¹⁶
- ▲ *The Traveller's Good Health Guide*, a book by Dr Ted Lankester¹⁷. Aimed particularly at aid workers and others planning an extended trip overseas. Includes information on preparation, precautions, treatment and 'reverse culture shock' on returning home.

¹⁶ Oxford University Press, 2002, available from bookshops or from www.amazon.com.

¹⁷ Sheldon Press, 2002, available from bookshops or from www.amazon.com.

INFORMATION SECURITY

A15

Information security is ensuring that important information is not lost, and that confidential information remains confidential.

Filing system

An efficient filing system is essential. Without it, information will be lost, and will require considerable time and effort to find or re-create.

Security of files

Files should be kept in rooms not accessible to the public. Sensitive or confidential files should be clearly marked as such, and kept in unmarked, locked filing cabinets.

Backing up files

Any files whose loss would be costly or damaging should be copied ("backed up"), and the copies kept at a different location from the originals. It may be necessary to send the copies to HQ for safekeeping. Such files might include financial information, personnel files, and any files which will be required for reports to donors.

Files for evacuation

If evacuation is a possibility, a list should be made of the files which should be taken with the team when evacuating. In this way, the necessary files can be gathered quickly when the evacuation is decided on. Such files may include personnel files, financial files and inventories of equipment or stock, for example.

Note that it may be dangerous to take certain types of information with the team when evacuating, as the team may be searched when attempting to leave the area. There have been instances of humanitarian staff being arrested, tried and imprisoned for long jail terms because they were found to be in possession of sensitive information, while evacuating.

It is wise to prepare a draft authorisation document, which can be rapidly signed in the event of evacuation, giving authority to the senior national staff member to represent the organisation and to manage its operations.

Computer security

Information held on a computer is vulnerable to

damage and theft, even if passwords are used. Files remain on computer disks and can be read, even once they appear to have been deleted. Disk corruption, viruses and other types of computer attack can damage or remove information.

Managers should ensure that all staff using computers regularly back up important information held on computers. Back-up disks should be held in a different location. All computers should if possible be locked to a fixed point, to make theft more difficult.

Radio, telephone and e-mail security

All radio and telephone conversations, and all fax and e-mail, can be listened to or read by others, even if encryption is used. There is no such thing as a totally secure encryption system. That said, some encryption systems are very good, so that it would require a highly trained specialist, and considerable time, to decode a message.

Satellite phones are also not secure. There have been instances of military forces apparently discovering the locations of refugees by listening to the satellite phone conversations of humanitarian managers who thought they were talking on a secure system. The military then went to the refugees' location and killed them.

The simple way to avoid giving away sensitive or confidential information is not to send it. It is often possible to take the information in person, and communicate it directly to the person who needs to know it. This may take longer, but is it essential that that person knows the information quickly?

It may sometimes be unavoidable to send sensitive or confidential information. In these cases, be aware of the risks (to you and others, including local people) and weigh them against the benefits.

Many experienced humanitarian managers strongly advise against the use of encryption by humanitarian organisations. In some countries, a licence is required by organisations using encryption. Although some encryption systems are very good, there is no such thing as 100% secure communica-

INFORMATION SECURITY

A15

tions. In the case of encrypted e-mail, the computers which send and receive messages contain decoded versions of the messages: if the computers are seized, those messages can be read.

A further argument against encryption is that its use may be likely to attract attention from intelligence agencies who may wonder why encryption is necessary. Aid workers have been imprisoned in the past when their computers or documents were found to contain sensitive information. Sending non-encrypted messages, with no highly sensitive content, helps to avoid this potentially serious problem.

Information that should not be recorded

Humanitarian organisations should avoid recording any sensitive information that they do not need to record. In particular, they should not record any information that might give the impression that they are spying, or gathering information that might compromise the security of a local authority or a party to a conflict.

For example, humanitarian organisations need to know the general security situation around them, and the threat (if any) posed by military forces. But they probably do not need to know or record the precise locations of troops, trenches, heavy weapons, and current military operations unless they are threatening an area where humanitarian staff are working. (An evacuation from that area is then likely to be necessary.) Recording inappropriately detailed military information can put the organisation at great risk. If found with such information its staff could be attacked or imprisoned on suspicion of spying.

INSURANCE FOR WAR RISKS¹⁸

A16

Many humanitarian organisations find it necessary to obtain “war risks insurance” for field staff working in insecure locations. This is similar to travel insurance in the benefits that it can pay out, but unlike normal insurance does not exclude risks arising from conflict.

It can be hard to find war risks insurance at a reasonable price. It is vital to check the wording of any policy very carefully before buying it. Are any risks excluded? Are any countries excluded? Is the level of benefits sufficient? Are any other conditions imposed? Contact other experienced humanitarian organisations and ask them which insurers they use.

Benefits to consider include compensation for:

- ▲ Medical costs
- ▲ Repatriation costs, in the case of illness or injury
- ▲ Repatriation of mortal remains, in the event of death
- ▲ Temporary partial disability
- ▲ Temporary total disability
- ▲ Permanent partial disability
- ▲ Permanent total disability
- ▲ Loss of life
- ▲ Employee replacement costs
- ▲ Personal or organisational liability
- ▲ Loss of property
- ▲ Are dependants covered?

Exclusions that an insurer may seek to impose include:

- ▲ Cover only during work assignment (possibly excluding time on holiday, or time on Rest and Recreation (R&R), or time away from the duty station)
- ▲ Cover only during working hours
- ▲ Cover excluding war zones (check the definition of war zone)
- ▲ Cover only if the organisation has written security guidelines, or if they are enforced, or if they were being followed at the time of the incident
- ▲ Cover only if the organisation provides security training for all staff without exception
- ▲ Cover only for the duration of the contract (so, what happens if effects of an incident appear after the end of the contract?)

Staff should check to see if other personal or corporate insurance currently in force may be invalidated by travelling to a high-risk area. Sometimes life insurance policies or policies connected with a mortgage, among others, can be invalidated in this way.

Both national staff and international staff should be insured, if the organisation is not able to self-insure. The level of benefits should be set by a clearly thought-through policy that staff see as fair. All staff should receive a copy of the insurance policy, and understand its meaning and the level of benefits provided.

Note that failure to maintain adequate insurance could lead to large claims being made against an employer, which in some cases could drive the employer into bankruptcy.

Some insurance companies will offer significantly lower premiums if those covered have received proper security training.

For further information, see *Under Cover? Insurance for Aid Workers*¹⁹, a report produced for People In Aid.

¹⁸ Adapted from Annex 6 of K. Van Brabant (2000) *Operational Security Management in Violent Environments* published by ODI Humanitarian Practice Network as Good Practice Review No. 8. Available as free download from www.odihpn.org.

¹⁹ S. Davidson and J. Neal (1998). Available as a free download from www.peopleinaid.org.

INTERNATIONAL HUMANITARIAN LAW (IHL)

A17

International Humanitarian Law (IHL) is the body of rules which, in wartime, protects people who are not or who are no longer participating in the hostilities. Its central purpose is to limit and prevent human suffering in times of armed conflict.

International humanitarian law covers two areas:

- ▲ The protection of those who are not, or no longer, taking part in fighting
- ▲ Restrictions on the means of warfare – in particular weapons – and the methods of warfare, such as military tactics

A major part of international humanitarian law is contained in the four **Geneva Conventions of 1949**. Nearly every State in the world has agreed to be bound by them. The Conventions have been developed and supplemented by two further agreements: the **Additional Protocols of 1977 relating to the protection of victims of armed conflicts**. These documents can be found at (www.icrc.org/eng/ihl).

Other agreements prohibit the use of certain weapons and military tactics and protect certain categories of people and goods. These agreements include:

- ▲ The 1954 Convention for the Protection of Cultural Property in the Event of Armed Conflict, plus its two protocols
http://portal.unesco.org/culture/en/ev.phpURL_ID=8450&URL_DO=DO_TOPIC&URL_SECTION=201.html
- ▲ The 1972 Biological Weapons Convention
http://www.unog.ch/disarm/distreat/bac_72.htm
- ▲ The 1980 Conventional Weapons Convention and its four protocols
<http://www.un.org/millennium/law/xxvi-18-19.htm>
- ▲ The 1993 Chemical Weapons Convention
<http://disarmament.un.org:8080/TreatyStatus.nsf>
- ▲ The 1997 Ottawa Convention (on anti-personnel mines)
www.un.org/Depts/mine/UNDocs/ban_trty.htm

- ▲ The 2000 Optional Protocol to the Convention on the Rights of the Child on the involvement of children in armed conflict
www.unhcr.ch/html/menu2/6/protocolchild.htm

(If any of the above web addresses become unworkable, use a search engine to find the document you need.)

International humanitarian law applies only to armed conflict; it does not cover internal tensions or disturbances such as isolated acts of violence. The law applies only once a conflict has begun, and then equally to all sides regardless of who started the fighting. If not all the parties have ratified the Geneva Conventions, Customary Law still applies, with similar effect - the ICRC can advise on this if necessary.

For example, the principle of non-refoulement (refoulement is the forcible return of people to countries where they face persecution) is part of customary international law and is binding on all states. Therefore no government should expel a person in those circumstances²⁰.

The International Committee of the Red Cross (ICRC) has been appointed by the international community as the promoter and guardian of IHL. The ICRC is ready to assist if there are questions about IHL or its application. It gives a large amount of useful information on IHL on its website at www.icrc.org.

Humanitarian managers should have at least a basic familiarity with key provisions of IHL, for several reasons including security. For example:

- ▲ If an armed group is threatening or attacking humanitarian staff, after taking any necessary immediate action to secure their staff, humanitarian managers may think it appropriate to remind the armed group of their responsibilities under IHL, including their responsibility not to threaten or attack humanitarian staff. Normally the ICRC will remind all relevant authorities of this, but in some cases the ICRC may not be present, or it may be necessary to apply further pressure. Diplomatic channels may also be used to bring pressure to bear, provided that they do not compromise the impartiality (real

²⁰ Source: UNHCR. There are some exceptions to this rule. For more information, see UNHCR's website at www.unhcr.ch.

INTERNATIONAL HUMANITARIAN LAW (IHL)

A17

and perceived) of humanitarian organisations.

- ▲ If anti-personnel mines are being laid, humanitarian managers should be aware that they are illegal, and if it is safe to do so should report the fact to ICRC or another appropriate body
- ▲ If child soldiers are in evidence, perhaps posing a threat to humanitarian organisations, humanitarian managers should consider discussing the issue with the ICRC or Unicef who may be able to take appropriate action

Reporting a breach of IHL, or a war crime or a serious human rights abuse, may place the organisation and its staff in danger. Yet if crimes are committed with impunity, insecurity usually increases. It may be necessary to report confidentially, in such a way that the source of the information is never identified or guessed by potentially hostile groups.

For further information on IHL, see the ICRC brochure: "International Humanitarian Law: Answers to your Questions", available on the ICRC website at www.icrc.org.

Other organisations involved in the promotion of IHL include:

- ▲ United Nations High Commissioner for Human Rights www.unhcr.ch
- ▲ Human Rights Watch www.hrw.org
- ▲ Amnesty International www.amnesty.org

UN Human Rights Treaties (not the same thing as IHL), together with relevant explanation and a description of remedial mechanisms are made available at www.bayefsky.com.

INVENTORY CONTROL

A18

Theft and loss of goods are common problems in humanitarian operations. When large quantities of goods are moving rapidly through an area in crisis, it is inevitable that some theft and loss occurs. But the scale of theft can be greatly reduced by good management, and particularly by inventory control procedures.

All goods and property should be logged in an inventory. A staff member should be assigned responsibility for establishing and maintaining the inventory. There may be a need for more than one inventory – for example, one for the organisation's equipment, and another for goods in the warehouse. It is vital that inventories are kept fully accurate and up to date, from the outset of the operation. Indeed, it is at the outset that many losses tend to occur, because of the greater confusion that is usually present.

The principles are simple (although in a fast-moving situation it can be hard to keep up). All incoming goods or equipment should be signed for using a **receipt form**, and then entered on the **inventory**. All outgoing goods or equipment should be signed for using a **despatch form**, and removed from the inventory.

When an item of equipment is issued to a staff member for his or her use, he or she should sign for it on an **issue form**. When the equipment is returned, the person receiving the returned equipment should sign to acknowledge its receipt, in a separate column on the issue form.

In a warehouse, once goods have been received and placed in the inventory, they are normally also allocated to a particular stack of goods. Each stack has a **stack card**, on which the goods should also be recorded when they arrive or leave.

The names of the forms may vary between organisations, but the basic principles remain the same. Without a system of this kind, used by all staff in a disciplined manner, there is a much higher risk of theft, loss and inefficiency.

A manager should regularly check that the inventory control system is functioning properly. Frequent checks may be needed at the start of an operation, as systems get up and running. Checks should include unannounced visits, and random verification of goods or equipment and their related paperwork.

Any significant theft or loss should be reported. It should be investigated by a manager senior to, and independent from, the team in which the incident occurred. He or she should produce a written report stating the facts, as far as they can be discovered; assigning responsibility, as far as it can reasonably be assigned; and making recommendations for improvements to inventory control systems and disciplinary action, where appropriate.

A requirement for such an investigation should be included in the logistics procedures of all humanitarian organisations. Failure to ensure full accountability in the event of a significant theft or loss undermines the integrity of the organisation, and is likely to damage donor confidence.

MEDIA AND SECURITY

A19

The media can sometimes have an impact on the security of humanitarian staff. By reporting details of a sensitive operation they may arouse the anger of groups who wish to see the operation stopped. They may attract the attention of hostile armed forces. They may simply alert criminals to the presence of high-value goods to steal.

On the positive side, the media can enhance security by reporting accurate information about a humanitarian operation, winning local goodwill. After a security incident, the media can be used to disseminate accurate reports, thus squashing exaggerated rumours that may be circulating.

Humanitarian managers should therefore be aware of media reporting, and able to use the media effectively when appropriate. Points to bear in mind may include:

- ▲ Know what message you want to get across, and ensure that you do so during the interview. Be able to express it briefly and clearly. In the Western media, expressing your message in a 'sound bite' of 8 seconds or less greatly increases the chances of it being broadcast.
- ▲ Ensure that you always tell the truth. This is right in principle, and wise in practice. It builds up a reputation for honesty, and false information is usually found out in the end.
- ▲ If you are not sure of a fact, don't publish it. If you don't know the answer to a question, say you don't know. If you have to publish unconfirmed information, state clearly that it is unconfirmed.
- ▲ After a major security incident, consider making an early statement to the media as soon as you have some confirmed facts to tell them. This will help to prevent false rumours from growing.
- ▲ It is not usually a good idea to say "no comment" to a question from the media. This looks defensive, and leaves an information gap that they may try to fill with less reliable information.
- ▲ If you become aware of a false rumour concerning your organisation, consider how best to correct it. Assess whether it could become the cause of an increased threat to your organisation if it is left uncorrected.
- ▲ Give clear instructions to your staff as to who may speak to the media, and who may not. For those who are not to speak to the media, explain to them the reason for it (e.g. it helps prevent confusion if there is only one spokesperson), and let them know what they should say if approached by the media (e.g. politely refer them to the spokesperson).
- ▲ In general, openness works better than a defensive attitude towards the media. They have a legitimate job to do, and they can help your operation. An ideal working relationship will be respectful, professional and open but not too familiar, since the media may be tempted to take advantage of too close a relationship.
- ▲ Remain aware of what the local media are saying. If they use a language which you do not speak, nominate a colleague who does speak the language, to monitor the media and to summarise it to you. This enhances your understanding of the local situation, and enables you to assess the evolving security environment.
- ▲ Avoid commenting on the government, political or military situation unless there are overriding reasons to do so

MEDICAL EVACUATION (MEDEVAC)

A20

A humanitarian organisation's security plan should detail the procedure for medical evacuation (Medevac). If the organisation has contracted a medical evacuation company (usually in conjunction with an insurance policy), then the procedure agreed with that company will apply. Typical requirements include:

- ▲ A doctor who has examined the patient must sign a certificate stating that Medevac is necessary. This certificate must be faxed to the insurance company.
- ▲ All staff must know the procedure for calling in the medical evacuation company, including up to date phone and fax numbers, and certificate numbers if necessary
- ▲ There should be clarity as to which staff are entitled to Medevac, and what medical arrangements are available for any staff who are not entitled to Medevac

It is a good idea to telephone the number for the medical evacuation company when you are setting up your programme, to check that you have the correct number and to verify that they recognise you as a client.

Medevac routes should be checked. Will the roads you intend to use be open if there is a deterioration in the security situation? What alternative routes are there? Will the local airfield or airport be open, accessible, and secure? What alternative airfields are there?

A medical NGO operating in the same area may be able to help during medical emergencies. Discuss this possibility with them before an emergency arises.

NEXT OF KIN RECORDS

A21

A Next of Kin record enables an organisation to inform a staff member's family or close friends, in the event of an accident, injury, illness or death. An up to date Next of Kin record of all staff (both nationally-recruited and international) should be held at all times at HQ or in the field: preferably in both locations in case records at one location are lost.

A Next of Kin record is likely to contain at least the following information:

Staff Member

- ▲ Full name of staff member
- ▲ Date of birth of staff member
- ▲ Home address and telephone numbers of staff member

Next of Kin

- ▲ Full name of Next of Kin
- ▲ Relationship to staff member (e.g. father, wife, friend, etc)
- ▲ Address
- ▲ Telephone numbers
- ▲ E-mail address
- ▲ If this person cannot be contacted, is there another person who should be contacted? If so, provide full name, their relationship to you, and full contact details.

NEXT OF KIN : PROCEDURE FOR INFORMING THEM

A22

If an accident, injury, illness, death or other serious event happens to a staff member, and if that person is unable to contact their Next of Kin, in most cases the employing organisation has at least a moral duty to inform them. This is obviously a very sensitive process, and it is important to have a clear procedure for it.

The procedure is likely to include at least the following points:

- ▲ Who should inform the Next of Kin? In serious cases such as death, it should usually be a senior manager who informs the Next of Kin, to show the importance that the organisation attaches to the event, and to supporting the family and friends of the staff member.
- ▲ By what means should the Next of Kin be informed? If the staff member has died or is seriously ill, a personal visit is likely to be essential. In some cases, for example where the Next of Kin lives in another country, a rapid personal visit may not be possible, in which case a senior manager should decide whether a telephone call is appropriate.
- ▲ Advice to those who have to communicate the news to the Next of Kin

Communicating with Next of Kin

The following tips may be helpful:

- ▲ If you do not speak the same language, ensure that a good interpreter is available, and consider whether a colleague who does speak the same language would be more appropriate to break the news
- ▲ (If visiting) Dress respectfully. If the Next of Kin is a woman, ensure that the visit is by a woman, or if there is more than one visitor, at least one of them is a woman – and *vice versa*.
- ▲ (If telephoning) Ask the person if they are alone. If they are not, request that they go to a room where they can be alone.

- ▲ (If visiting or telephoning) In the case of death or other serious event, you may wish to have a trained counsellor take part in the visit or call
- ▲ Say that you have some bad news. Invite them to sit down.
- ▲ Look at them directly (if visiting). Tell them simply and clearly what has happened to the person concerned. For example, "I am very sorry to say that John is dead." This is usually far better than a longwinded sentence, or delaying the moment when they hear the bad news. They have probably guessed it already.
- ▲ At this point, be prepared to offer support to the person. Their reaction may take many different forms, ranging from silence all the way through to hysterical grief or even violence. What is important is that you remain calm, supportive, sympathetic and gentle. Depending on their mood, a physical sign of support may be appropriate, from someone of the same gender: for example, an arm round the shoulder. It is helpful if you come with a supply of handkerchiefs.
- ▲ If and when they wish to hear the whole story, tell it simply and clearly, preparing to pause if they cannot hear any more
- ▲ Use your judgement as to whether it is appropriate to tell them a long version of the story, or a shorter version. A shorter version inevitably is more selective, but it may be all that they can cope with at this stage.
- ▲ Make sure that everything you say is truthful. If you don't know the answer to a question, say that you don't know. It can be very damaging for relatives to discover later that they were misled, whether intentionally or unintentionally.
- ▲ Once they understand the situation and are calm enough to think of practical matters, inform them what action the organisation has taken (e.g. taken the injured person to hospital; recovered the dead person's body, etc). Suggest

NEXT OF KIN : PROCEDURE FOR INFORMING THEM

A22

what action they might wish to take (e.g. fly out to see the injured person). Say what help the organisation will give (e.g. pay for airfare; ensure that any insurance payment happens rapidly – but check that you only give totally accurate information on financial matters, and make no promises that you cannot keep). Take plenty of time to reassure them as much as possible.

- ▲ Ask if they have family or friends who can provide emotional support, and offer to contact them on their behalf
- ▲ If they need you to stay for a long time, be prepared to do so. If the news is of a death, they should not normally be left alone; instead, wait until a friend or family member has arrived to support them. Once they are ready for you to leave, express your sympathy again, and reassure them that you will help in every way possible. Give them your name and full contact details. Give them the name and contact details (including evenings and weekends) of the person who will be their main contact within the organisation (if it is not you).
- ▲ Ensure that you (or the main contact person) contacts the Next of Kin the next day, and as frequently as appropriate thereafter. Organisations sometimes find it easier to offer immediate support, but harder to remember the ongoing support that is vital – both for the good of the Next of Kin, and for the reputation of the organisation. The family of a dead staff member is likely to make severe criticism of any employer who appears to forget them.
- ▲ Verify what financial and other help is due from the organisation, or from an insurance company, to the Next of Kin. Ensure that this is communicated with total accuracy, and without delay, to the Next of Kin. Arrange for this help to arrive as soon as possible.
- ▲ A senior manager should remain in charge of the whole process, to ensure that high standards are maintained

PEOPLE IN AID CODE: PRINCIPLE SEVEN

A23

Principle 7 of the People In Aid Code of Good Practice in the management and support of aid personnel²¹ is entitled: "Health, Safety and Security". It states:

The security, good health and safety of our staff are a prime responsibility of our organisation. We recognise that the work of relief and development agencies often places great demands on staff in conditions of complexity and risk. We have a duty of care to ensure the physical and emotional well-being of our staff before, during and on completion of their period of work with us.

The following indicators are attached to the principle, to assist aid agencies in assessing how well they measure up to it. They are:

Written policies are available to staff on security, individual health, care and support, health and safety.

Programme plans include written assessment of security, travel and health risks specific to the country or region, reviewed at appropriate intervals.

Before an international assignment all staff receive health clearance. In addition they and accompanying dependents receive verbal and written briefing on all risks relevant to the role to be undertaken, and the measures in place to mitigate those risks, including insurance. Agency obligations and individual responsibilities in relation to possible risks are clearly communicated. Briefings are updated when new equipment, procedures or risks are identified.

Security plans, with evacuation procedures, are reviewed regularly.

Records are maintained of work-related injuries, sickness, accidents and fatalities, and are monitored to help assess and reduce future risk to staff.

Workplans do not require more hours work

than are set out in individual contracts. Time off and leave periods, based on written policies, are mandatory.

All staff have a debriefing or exit interview at the end of any contract or assignment. Health checks, personal counselling and careers advice are available. Managers are trained to ensure these services are provided.

In the case of staff on emergency rosters, managers should ensure that health clearance, immunisations and procedures for obtaining the correct prophylaxes and other essential supplies are arranged well in advance.

²¹ Available at www.peopleinaid.org

RADIO PROCEDURES

A24

Radios should only be used if they are necessary: in some situations other methods of communication are sufficient. It takes time to learn to use a radio well. All staff should be taught basic radio use as an essential aid to security, in those field operations where radios are necessary.

Types of radio

Long-range radios are High Frequency (HF) radios, which can communicate several hundred kilometres and in some circumstances several thousand.

Short-range radios are usually Very High Frequency (VHF) radios. They can usually communicate a few kilometres directly, but using a repeater station (on a hilltop or a high building) can sometimes communicate several tens of kilometres. Typical ranges²² for VHF radios are:

- ▲ Handheld to handheld: 2 – 5 km
- ▲ Vehicle unit to vehicle unit: up to 20 km
- ▲ Base unit to handheld: up to 15 km
- ▲ Base unit to vehicle unit: up to 30 km
- ▲ Base unit to base unit: up to 50 km

Some VHF radios are hand-held, with a small antenna: these are often carried by humanitarian staff. Larger radios, either VHF or HF, are mounted in vehicles or in buildings, with larger antennas.

Care of a radio

A radio battery needs to be recharged regularly. Some kinds of batteries should be fully discharged before they are recharged, or the life and power of the battery will be reduced. It is good practice to carry a spare battery, fully charged, to enable an immediate change of batteries when the first one runs out.

Radios are expensive items, attractive to thieves and to unscrupulous soldiers. All staff should sign for receipt of their radio and be warned to keep it with them at all times.

Programming radios

Many modern radios need to be programmed before they can be used. A technician will normally do this. The radio is tuned to the frequencies in use

by humanitarian organisations in that area, plus one or more frequencies specific to your organisation.

Often, humanitarian organisations will share one or more radio channels. A UN agency may make available two or more of its channels, for use by all humanitarian organisations. If so, one channel is likely to be designated as the 'calling' channel, and another may be designated as the 'security' or 'emergency' channel.

Procedure for speaking on the radio

It is important to follow the standard procedure for speaking on the radio. Only one person can speak at one time, and while doing so he or she prevents anyone else from speaking. Unlike a telephone, anyone with another radio can hear what you are saying. Therefore bear in mind the following principles of radio use:

- ▲ Clarity
- ▲ Brevity
- ▲ Security

Do not use the radio like a telephone. Work out what you want to say before transmitting. The following procedure words (known as prowords) are some of those commonly used:

Proword	Meaning
HELLO	I am calling (then insert the callsign of the person or station you are calling)
CALLSIGN	The 'radio name' of a person or station. (Usually composed of letters and numbers, e.g. A21 (pronounced "Alpha Two One"). Actual names of people or organisations are not used.)
THIS IS	My callsign is...
I SAY AGAIN	I am repeating what I have just transmitted
READ BACK	Please read back this entire transmission exactly as you heard it
ROGER	I understand what you have just said
SEND	Please send your message

²² Source: *Safety First: a field security handbook for NGO staff* by Shaun Bickley, revised version published 2003 by Save the Children UK. Available from www.plymbridge.com.

RADIO PROCEDURES

A24

OVER	This is the end of my transmission and I expect you to reply
OUT	This is the end of my transmission and I do not expect you to reply. ("OVER AND OUT" is never used.)
WAIT	I must pause for a few seconds. Please wait. (Other users should not use the radio channel in the meantime.)
WAIT OUT	I must pause longer than a few seconds; I will call you back. (Other users can use the radio channel in the meantime.)
CORRECT	What you have just transmitted is correct
WRONG	What you have just transmitted is incorrect
CORRECTION	What I have just transmitted is incorrect – and the correct version is...
BREAK – BREAK	This is an emergency and I need to interrupt a radio conversation to send my message

Calling another person

- ▲ Ensure no one else is transmitting at the same time. Wait for ongoing discussions to finish completely before beginning transmission.
- ▲ Make your message brief but precise
- ▲ Use the standard procedure words
- ▲ Use call signs instead of personal names. Do not identify organisations or personnel by name over the radio.
- ▲ Begin by pressing the 'transmit' button and saying: "Hello [their callsign] this is [your callsign] over". Then release the 'transmit' button immediately.
- ▲ After they respond (perhaps by saying "[Their callsign], send over"), you press the 'transmit' button, say your callsign again, send your message, and end with "over" or "out". Release the 'transmit' button.

- ▲ After the initial call in a conversation, it is normal for each transmission to begin with the callsign of the person speaking, but in some cases this is not necessary. Local practice varies.
- ▲ Break the message into sensible passages with clear pauses between
- ▲ Maintain clear speech with normal rhythm and moderate volume
- ▲ Hold the microphone approximately 5 cm from your mouth
- ▲ Avoid excessive calling. Use radios for work-related purposes only.
- ▲ Never transmit specific security-related information or travel plans or discuss transfer of cash or goods

Phonetic alphabet

When spelling letters on the radio, or using letters in callsigns, the international phonetic alphabet is used. All radio users should know this alphabet by heart:

A	ALFA
B	BRAVO
C	CHARLIE
D	DELTA
E	ECHO
F	FOXTROT
G	GOLF
H	HOTEL
I	INDIA
J	JULIET
K	KILO
L	LIMA
M	MIKE
N	NOVEMBER
O	OSCAR
P	PAPPA
Q	QUEBEC
R	ROMEO
S	SIERRA
T	TANGO
U	UNIFORM

RADIO PROCEDURES

A24

V	VICTOR
W	WHISKY
X	X-RAY
Y	YANKEE
Z	ZULU

Power supply

Radios cannot operate without power. In most humanitarian situations, mains electricity supply is either non-existent or unreliable. Therefore you are likely to need a generator and a fuel supply for the generator, to power larger radios directly and to power battery chargers for battery-powered radios.

Ensure you keep all your batteries fully charged so that, if an emergency occurs, all power fails and your generator breaks down, you can still communicate.

Generators should be sited far enough away from offices and accommodation to reduce the noise disturbance that they cause. If they can be housed in an outhouse with sufficient ventilation, or a wall built around them, so much the better. They are valuable, so secure them with strong locks and prevent public access to them.

When using unreliable mains electricity or a generator, electronic equipment can be damaged or destroyed by power surges. It is vital to connect a surge protector between the power supply and your radios, battery chargers and computers.

Generators need regular maintenance from a competent technician.

In emergency

The standard radio emergency call, primarily used for shipping or aircraft, is "MAYDAY MAYDAY MAYDAY", followed by your callsign three times, followed by your location, a brief description of the emergency, and what assistance you need. In practice aid workers rarely use this procedure, but use plain language and/or an immediate incident report (see Annex 29).

Duress codes

Duress code words are generally innocuous words or phrases selected for use over the radio or telephone

to indicate that the speaker is in a threatening situation but not free to communicate. All staff should be informed of the duress code word(s).

Do

- ▲ Get trained in radio use before starting – practising with a colleague can help
- ▲ Think before you speak
- ▲ Be very brief
- ▲ Only use a radio when there is no other suitable method of communication
- ▲ Know which is the calling channel and which is the emergency channel

Don't

- ▲ Don't mention sensitive information on the radio
- ▲ Don't touch an antenna when a radio is transmitting (there can be a risk of burns)
- ▲ Don't use a radio close to fuel when it is exposed to the air, for example when filling up a vehicle (there can be a risk of igniting the fuel)

REST AND RECREATION (R&R)

A25

During a high-pressure operation, staff are likely to need regular Rest and Recreation (R&R). Its purpose is to help prevent stress or illness, and to improve efficiency. R&R usually involves a staff member leaving the operation for a number of days, going to a location that is near enough to be inexpensive, but far enough from the operation to allow a sense of distance and freedom from pressure.

The location for R&R should be as stress-free as reasonably possible. It should preferably be somewhere where the person's language is understood. Accommodation should be comfortable, without being luxurious. Some staff will prefer to have company; others to be alone.

How much R&R is needed will depend on the circumstances and the resources available. In the most serious phase of a major crisis, some organisations provide a week's R&R every six weeks or so. In subsequent, less serious phases, the frequency may reduce to eight or twelve weeks, or longer.

Once an R&R procedure has been decided for an operation, it is good practice for it to be mandatory. This is because the most motivated staff are likely not to take R&R if it is optional – and this is likely to result in stress, illness or inefficiency.

In the past, R&R has been almost only provided to international staff, on the grounds that they are working in a foreign country, away from their families and normal support structures. Yet in some circumstances, nationally-recruited staff may be under just as much pressure as international staff. In these cases, wise managers will consider what R&R is appropriate for nationally-recruited staff: because of the presence of their families it is likely to be a different format from international staff.

For further information, see People In Aid's Guidelines on *Setting up a Policy on Rest and Relaxation*, 2002, at www.peopleinaid.org.

SECURITY ASSESSMENT

A26

The aim of a security assessment is to understand the security situation sufficiently to enable the team to plan their security measures appropriately.

The team leader normally carries out a security assessment before a final decision is taken to deploy, and certainly before the arrival of the main team. It is done preferably by an assessment visit and, where a visit is not possible, by remote assessment.

A security assessment visit should be long enough to achieve its aim. Factors influencing the length of the visit include:

- ▲ The level of insecurity
- ▲ The experience of the person/people making the assessment
- ▲ The number of people making the assessment
- ▲ Geographical size of the area
- ▲ Complexity of the political situation
- ▲ Weather
- ▲ Other local events, e.g. holidays, festivals
- ▲ Availability of key interlocutors such as local leaders
- ▲ Availability of transport
- ▲ Availability of good maps
- ▲ The severity of humanitarian need. If many people are dying, a more rapid security assessment may sometimes be necessary, to allow the programme to begin as soon as possible – but this is a matter for careful judgement since too rapid an assessment can be dangerous.

The most important requirement of a security assessment is to talk to the people who will best explain the security situation. These may be many different types of people, for example:

- ▲ Ordinary residents, selected at random in a representative variety of locations
- ▲ Local leaders, such as mayors, elders, village heads, governors, politicians
- ▲ Women: often a special effort is needed to meet with women (separately from men, if possible, since their opinions and information may be significantly different from those of men)

- ▲ Religious leaders
- ▲ Staff of local NGOs
- ▲ Staff of international humanitarian organisations (both national and international staff)
- ▲ Business people
- ▲ Diplomats
- ▲ Other knowledgeable people, such as former humanitarian staff, academics, etc

Informal conversation often yields the most useful information, although with local leaders a more formal style may be appropriate, depending on the culture. The person assessing will wish to know the answers to a large number of questions, including:

General situation

- ▲ What is happening in the political arena?
- ▲ What is the economic situation? What are the main sources of income? How much poverty is there, and what causes it? Is there high unemployment?
- ▲ What is the social make-up of the area?
- ▲ What local religions are there, and how many people follow them?
- ▲ What is the history of the area?

Threats

- ▲ What are the main threats to humanitarian organisations in this area?
- ▲ What types of crime are there, and how much?
- ▲ Do these threats vary by area, or by type of humanitarian organisation?
- ▲ Do they vary at different times of day, or times of the year?
- ▲ Are different types of staff threatened in different ways? (E.g. national, international, male, female, or staff of a particular ethnic group.)
- ▲ Are some threats different for nationally-recruited staff and their families?
- ▲ What security incidents have there been in recent months and years?
- ▲ Have any of these incidents involved humanitarian or other international organisations?
- ▲ Are there any threats originating from outside the area? How can one get information about these?
- ▲ Are there any terrorist threats? If so, are they serious enough that specialist advice on anti-

SECURITY ASSESSMENT

A26

terrorism security measures will be necessary?

Local attitudes

- ▲ What are the most appropriate ways of winning acceptance from local people?
- ▲ How well is the work of humanitarian organisations understood by local people and leaders?
- ▲ What is the attitude of local people, and local leaders, to humanitarian organisations at present?
- ▲ What rumours are circulating? Is there truth in them? What do they reveal about local attitudes?
- ▲ Are any local groups or individuals hostile to humanitarian organisations?
- ▲ How would my particular organisation be viewed locally?
- ▲ What would be the best ways for us to explain our role to local people and leaders?
- ▲ What impact would our arrival have on local opinion?
- ▲ What impact would our presence have on the security of local people?
- ▲ Would our work be valued by local people and leaders?
- ▲ How would international staff (of various kinds and nationalities) be viewed?
- ▲ How would national staff (of various kinds) be viewed?
- ▲ Are there any cultural practices or issues that we should be aware of?
- ▲ Are there any corruption issues to consider? Will we be able to work here without paying bribes?
- ▲ Are any nationalities or ethnic groups especially vulnerable in the local context?

Local authorities

- ▲ Do local authorities require humanitarian organisations to register? What conditions are imposed, if any?

Our organisation's profile

- ▲ Should we adopt a low, medium or high profile when we deploy?
- ▲ Are there suitable places for our offices, warehouses and accommodation?
- ▲ Are there any issues that might affect our impartiality? For example, will we need to

work on both sides of a front line, or among several ethnic groups, to demonstrate our impartiality?

- ▲ How can we ensure that we remain independent, and perceived as such? For example, should we locate our office or accommodation deliberately far from the residence or office of prominent local leaders?

Protection

- ▲ What protection measures are we likely to need?
- ▲ Will we need to use armed guards (normally only in extreme circumstances – see Annex 13)?
- ▲ What security-related equipment will we need?

Influential people and groups

- ▲ Who are the most influential leaders locally?
- ▲ What ethnic groups are there, where are they, and who are their leaders?
- ▲ What other organisations (e.g. military, police, civil, political, business, religious, cultural) have influence locally?
- ▲ What are the aims of these groups?
- ▲ Where do these groups draw their power from?
- ▲ How are they perceived by local people?
- ▲ What are the relationships between all these groups?
- ▲ What permissions, from whom, will we need to do our work? How long will it take to get those permissions?

Staff

- ▲ Are there any issues concerning recruitment of national staff? Will there be any problems finding people of the right abilities? Will a fair recruitment process be possible?
- ▲ Will national staff face risks because of their work?
- ▲ What security measures would need to be provided for national staff homes, and for their travel to and from work?
- ▲ Is it more appropriate to use national or international staff? Male or female? In what proportions?
- ▲ What key posts are essential to security? Will we be able to fill them?

SECURITY ASSESSMENT

A26

Movement and access

- ▲ How much freedom of movement is there for humanitarian organisations?
- ▲ Will we have access to the areas we plan to work in?
- ▲ Is there a curfew in place? Give clear details of times for different locations.
- ▲ Are there feasible evacuation routes?

Property

- ▲ Will the organisation's property be safe?
- ▲ What risk is there of the organisation's goods contributing to violence? (If, for example, they are stolen and sold.)
- ▲ What is the attitude of the authorities towards the property of humanitarian organisations when a programme closes?

Insurance

- ▲ Is there a reputable local insurance provider?

Site security

- ▲ Will it be possible to have a secure office, accommodation and other sites?

Security forces

- ▲ How well does the local police function?
- ▲ How disciplined are the local armed forces?

Overall

- ▲ Does the likely benefit of our work outweigh the security risk?
- ▲ Will the organisation's presence endanger others?

It is important to be aware that some information may be inaccurate, either deliberately or accidentally. Checking key information with a variety of sources should help to minimise this risk.

Documents may be available which help to answer the above questions. Relevant documents may come from a wide variety of sources, including:

- ▲ UN or NGO reports, and old archives
- ▲ Media reports and articles – local and international
- ▲ Academic papers
- ▲ Government publications

Many useful documents are available on the internet. Some useful sources include:

- ▲ ReliefWeb www.reliefweb.int
- ▲ UN Integrated Regional Information Network (IRIN) www.irinnews.org
- ▲ UN Humanitarian Information Centres (HICs) www.humanitarianinfo.org
- ▲ International Crisis Group www.crisisweb.org
- ▲ AlertNet www.alertnet.org

It is essential during an assessment visit to get a feel for the area. How best to do this depends on the area. It may be helpful, if it is safe to do so, to:

- ▲ Walk through various parts of the main town(s)
- ▲ Visit markets and chat to traders and customers
- ▲ Drive down important roads, stopping to talk to people from time to time
- ▲ Visit out-of-the-way villages and talk to people

In some cases, it may not be safe to do some or all of these things. Since you are on an assessment and may not know the area well, it will be necessary to take advice from a trusted source on what is safe to do – and preferably to be accompanied by a reliable person who is familiar with the area and can help ensure that you stay safe.

When talking with local people during an assessment visit, there is a danger of causing misunderstanding. Depending on the culture and context, your short visit may be taken as a promise to return, bringing aid with you – even if you clearly explain the reason for your visit and are careful to make no promises. This could cause problems for you or for other humanitarian workers.

If you are not familiar with local customs, it can be easy to cause offence without realising it, particularly when asking questions. If your visit is quick, that alone can cause offence in some cultures, where taking time to greet and talk is an important part of politeness.

These considerations should be taken into account when planning an assessment – and may result in deciding not to visit certain locations or people but

SECURITY ASSESSMENT

A26

to find out security-related information in another way.

Ideally, the assessment should be written. This allows senior managers to check and approve it. It enables easy dissemination to other team members. It also leaves a record on file, for evaluation and accountability purposes.

A possible outline structure for a security assessment is as follows:

- ▲ Location, date and author
- ▲ General situation
- ▲ Local authorities
- ▲ Threats
 - List of threats
 - The likelihood of each threat occurring
 - The likely impact of each threat, if it occurred
 - Threats can helpfully be plotted on a chart – see the end of this Annex
- ▲ Our vulnerabilities to the threats
- ▲ Security measures needed to minimise those vulnerabilities
- ▲ What liaison will be required with other organisations
- ▲ Conclusion:
 - Does the likely benefit of our work outweigh the security risk?
 - Will the organisation's presence endanger others?
 - Recommendations

If the humanitarian need is very urgent there may not be time to write the assessment in full: in this case a summary should be written. In extreme cases, where action is required in a matter of hours, senior managers may give permission for the security assessment not to be written. In this case they should normally record this decision, with their reasons, in order to explain why normal good practice has not been followed.

See also the Threat Impact Chart in Annex 38.

SECURITY BRIEFING

A27

The length and content of security briefings will vary according to the situation, and according to the job that the particular staff member is doing. But in general, most initial security briefings are likely to cover at least the following topics:

- ▲ Local geography: major features; centres of population; routes; condition of roads; natural hazards such as flood, earthquake, eruption; any other aspect that may affect security. Considerable effort should be made to obtain good maps of the area to permit effective briefing.
- ▲ History of the area, particularly as it affects the current political and security situation
- ▲ Political situation and any political trends, issues or sensitivities
- ▲ Ethnic groups in the area, their different histories, characteristics and aspirations
- ▲ Culture and custom in the area, including acceptable methods of greeting, languages used, actions and phrases to avoid
- ▲ Key local personalities, including political and other leaders
- ▲ Local laws, as they affect humanitarian organisations
- ▲ Local police and other relevant officials
- ▲ Armed forces and other armed groups in the area
- ▲ Driving rules and customs
- ▲ Likely threats to humanitarian organisations
- ▲ Procedures and other advice for responding to those threats
- ▲ Recent security incidents
- ▲ Location of local medical facilities
- ▲ Evacuation routes
- ▲ Other humanitarian organisations in the area
- ▲ Phone numbers and/or radio channels and call-signs to call in an emergency
- ▲ The background to the organisation's current humanitarian programme
- ▲ Authorisations necessary for humanitarian organisations
- ▲ Issue of identity documents and explanation of when they are required
- ▲ Security plan, including all security-related rules and procedures
- ▲ Enough time for any questions to be fully answered

Nationally-recruited staff will already be aware of some of the above information: it will be for the manager to judge which parts of the briefing should be omitted for them.

It is highly desirable, indeed essential if circumstances permit, to brief international staff fully on the general situation, and not only on the security-specific aspects of the situation. This will help them to understand the environment in which they will be working, which in turn can help them to make good security decisions. It may be helpful for a manager to prepare a written orientation briefing document, containing some basic information on the situation. It may contain, for example:

- ▲ Name of Head of State
- ▲ Name of Prime Minister
- ▲ Governing Party/Parties and their leaders
- ▲ Government in force since [date]
- ▲ Government mandate expires on [date]
- ▲ Opposition Parties and their leaders
- ▲ Local government authorities relevant to humanitarian work; their functions; names of key officials; their contact details
- ▲ Description of the conflict, if any
- ▲ Description of local crime situation
- ▲ Names of military, paramilitary or bandit forces in the area
- ▲ Contact details of local Embassies or Consulates

National staff may have little or no need to be briefed on the local situation. But they will need to be briefed on the organisation which is employing them. Contents of such a briefing may include:

- ▲ Brief history of the organisation
- ▲ Aims of the organisation
- ▲ Areas where it works
- ▲ Number of staff
- ▲ Sources of funds
- ▲ Names of Chief Executive and other senior managers
- ▲ Name of desk officer for this area
- ▲ Location and contact details of HQ
- ▲ Relevant policies and regulations of the organisation
- ▲ The culture of the organisation
- ▲ The organisation's plans in this area

SECURITY BRIEFING

A27**Notes:**

- 1.** The aim of security briefing is to enable staff to understand the local situation sufficiently to live and work safely in it.
- 2.** A security briefing should be given to all internationally-recruited staff before they travel to an insecure location. This briefing should be as thorough as possible, but usually can not be as detailed as a security briefing on the ground. On arrival, a further security briefing should be given which goes into greater detail and gives fully up-to-date information on the situation.
- 3.** Nationally-recruited staff should receive a full security briefing before they start work.
- 4.** In some circumstances it may be necessary to provide a security briefing to the family members of staff, either directly or through the staff member concerned, and to give them written instructions or an edited version of the security plan, if necessary.

SECURITY INCIDENTS: PREVENTION AND REACTION

A28

Managers should ensure that their staff are properly prepared, both to minimise security risks and to respond to incidents. Below are listed some suggested ways of reducing the risk of different types of incident, and of reacting to incidents if they occur. The points below will not apply in all situations: the best response will depend on the particular circumstances. But they may serve as helpful suggestions, to be adapted as appropriate.

Security incidents and some health and safety incidents are included in the same list, for ease of reference.

(a) Accidents Vehicle accidents

In many cases, driving is the most dangerous activity that humanitarian staff do. While accidents are not strictly a security issue, they are mentioned in this Guide because of the large number of humanitarian staff killed and injured while driving. Great effort should be made to ensure safe driving, and well-maintained vehicles, so that accidents are avoided as far as possible.

Once an accident has happened:

- ▲ Stop quickly and safely. Pull off the road if it is safe to do so. Note: in some cultures it is not safe to stop if you have just been involved in an accident, since onlookers are likely to beat or even kill the occupants of any vehicle they think has caused the accident. In these cases it is normal to drive on, even if there have been casualties, and seek help from the police or other responsible authority. But in many cultures it is imperative to stop immediately, indeed is a criminal offence not to do so. This underlines the importance of good local knowledge, and briefing for new staff.
- ▲ Prevent further danger. It is vital to prevent further danger to passengers, onlookers and other road users, after an accident has happened. This may involve:
 - Removing from vehicles any passengers who are in imminent danger
 - Putting out warning signs. Warning triangles should be placed far in front of the accident, facing towards oncoming traffic in both

directions. If a warning triangle is not available, improvise an alternative (e.g. place a person there to signal to traffic, or use a warning known to local people, such as twigs and leaves on the road).

- Putting out a fire, or preventing a fire if one is likely (e.g. if there has been a fuel spill)
- Directing traffic past the accident, if necessary
- Directing pedestrians and any onlookers out of the way of traffic and other hazards
- ▲ Give first aid to any who need it
- ▲ Call an ambulance if necessary, or if an ambulance is not available, make other arrangements to take casualties to the nearest emergency medical facility, perhaps using your own vehicle
- ▲ Call the police
- ▲ Take the names and addresses of any witnesses
- ▲ Exchange contact details with any other parties involved in the accident
- ▲ If you have a camera, take photographs of the positions of the vehicles after the accident, and any other relevant items, if doing so will not antagonise bystanders
- ▲ On the arrival of the police, cooperate fully with them
- ▲ Show courtesy and respect to all parties. If anyone has been injured in the accident, even if the fault was not yours, consider visiting them and/or their family, bringing a small present if appropriate. This helps to build local goodwill and can therefore be helpful to your security.
- ▲ After the incident, make a detailed record of it. Identify any lessons to learn, and ensure that any necessary changes in procedures are made. If disciplinary action is appropriate, ensure that it is taken swiftly and fairly. Proper accountability is particularly important relating to road accidents, because of the large numbers of deaths and injuries they cause to humanitarian staff.
- ▲ Record the incident in the organisation's accident book

Non-vehicle accidents

Humanitarian staff are at risk of a variety of hazards not involving vehicles. Examples include:

SECURITY INCIDENTS: PREVENTION AND REACTION

A28

- ▲ Electric shock
- ▲ Natural hazards such as rock falls or mudslides, floods or earthquakes
- ▲ Tripping, slipping or falling
- ▲ Drowning
- ▲ Burns

Managers should ensure that staff exposure to these hazards is minimised and that appropriate measures are in place to limit the impact of such incidents or to speed recovery from them.

It is good practice for all field locations to maintain an accident book. All accidents should be reported to managers and recorded in the accident book. 'Near misses', i.e. cases where an accident was only narrowly averted, should be recorded in the same way. The book should be inspected regularly by senior managers in order to ensure that any necessary lessons are learned.

In industrialised countries, it is estimated that 70% of workplace accidents could be prevented if employers put proper safety control measures in place²³. A full discussion of health and safety measures is beyond the scope of this document, but it is clear that good security management which fails to take account of non-security hazards amounts to an unbalanced approach to staff safety.

(b) Air attack

There are several kinds of air attack including:

- ▲ Bombing
- ▲ Gunfire
- ▲ Missiles

As with all other threats, it is vital to assess the threat of air attack. In particular:

- ▲ Is an air attack likely?
- ▲ If there is an air attack, is it likely to be aimed at you?
- ▲ What are the likely targets of an air attack? Are any of them near to you?
- ▲ If there is an air attack, what kind is it likely to be?
- ▲ In view of all the above, what security measures should you put in place? What kind of shelter do you need? If the risk of air attack is high,

should you even be present in the area?

For information on shelters, see Annex 33.

In the event of an air attack, the correct action will depend on the type of attack and your location. The following procedures may be appropriate, depending on the circumstances:

- ▲ Drop instantly to the ground. Lie completely flat.
- ▲ If it is possible to roll or crawl into a ditch, into a building or behind a wall without raising your profile, do so. This may give you some protection. Otherwise, remain still. Most blast and shrapnel fly upwards from the site of the explosion in a cone shape, so your best defence is to stay as low as possible. In this way it is often possible to survive explosions that are very close by.
- ▲ Observe what is happening
- ▲ Do not move until you are confident that the attack has finished. Beware: it may appear to have finished when in fact a second wave of attacks may be about to start. If there is a security officer for the humanitarian organisations, he or she may be able to announce the "all clear" by radio – but often this is not possible. You may therefore have to wait a long time before you can be reasonably confident that no more attacks are coming.
- ▲ If you are in a building, drop to the ground and move away from windows. Many injuries and deaths are caused by shattering glass. If it is safe to do so, move into the pre-designated shelter, without raising your profile.
- ▲ As with all incidents, do not use the radio unless it is absolutely necessary. Do not call your colleagues to check if they are safe: if they need help, they will call you. Keep the radio channels clear so that those who have emergency needs can use them.
- ▲ Report the incident as appropriate

(c) Air crash

Although aircraft crashes are usually seen as a health and safety rather than a security issue, they have accounted for a significant number of humanitarian staff deaths in recent years. For this reason the topic

²³ See RoSPA website at <http://www.rospace.com/CMS/index.asp>.

SECURITY INCIDENTS: PREVENTION AND REACTION

A28

is included in this Guide.

Humanitarian managers are able to reduce the risk of air crash in some respects, including:

- ▲ The choice of airline or air charter company
- ▲ Avoiding higher-risk routes
- ▲ Keeping up to date with the security situation at both ends of a flight route, and along its path

Humanitarian organisations should decide which companies to avoid, and which routes to avoid, and stick to this decision.

If an air crash does happen, involving a member of staff, local authorities are likely to organise search and rescue efforts. The relevant manager should ensure that the staff member's Next of Kin are immediately informed, and kept up to date with the situation. See Annex 22 for a suggested procedure for informing Next of Kin.

(d) Ambush

The best defence against ambushes is to avoid them. Good security assessments, combined with mature and careful decision-making, will lead to decisions not to travel in areas where ambushes are likely.

While one can reduce the chances of meeting an ambush, one cannot eliminate the possibility without stopping all travel. In some circumstances, stopping all travel, at least for a time, may be the best decision. In other circumstances humanitarian managers may decide that, if for example the risk of ambush is very low and travel is essential in order to save many lives, travel is justified. This is a matter for case-by-case decision by experienced and competent managers.

Armoured vehicles can be a further protection against ambush, appropriate in some circumstances. They require drivers who are familiar with the different handling qualities of these vehicles. They are expensive to buy and maintain. They do not protect against all types of weapon. They can also give an unfortunate impression to local people that you wish to fortify your organisation.

If staff are ambushed, there are methods of reacting which can increase the chances of survival. While there have been many unfortunate cases of people being killed and injured in ambushes, there have also been cases of people surviving unhurt.

The best action to take will depend on many factors, including the nature of the road, the terrain, whether staff are on foot or in a vehicle, the type of vehicle, the number of people travelling, the level of training of those travelling, the goals of the ambushers, the number of ambushers and their level of training, the kind of weapons used, etc. If the staff travelling are knowledgeable about as many of these factors as possible, their ability to make good decisions will be increased.

There follow some possible procedures for reacting to some types of ambush. They may be advisable in some circumstances but may not be appropriate, or may even be dangerous, in others.

Good judgement and training are required, to enable a good decision to be made at the critical moment. These procedures are provided to staff to help them think through their possible responses in advance. It is vital that procedures suggested here are selected and adapted as appropriate to the local situation.

Scenario one: ambush using a roadblock

You round a corner and see a roadblock (or even simply a checkpoint) ahead. Your knowledge of the area tells you that this is not a normal checkpoint, but could be an ambush.

- ▲ You will have to assess very fast whether it is simply a checkpoint, with no hostile intent, or whether it may have hostile intent against you
- ▲ If you assess that it may be violent, stop immediately if you can. Then reverse back round the corner. Once round the corner, if the road is wide enough, turn round and drive away. If it is not wide enough, continue reversing. Send an immediate incident report.
- ▲ If the roadblock is so close that stopping and

SECURITY INCIDENTS: PREVENTION AND REACTION

A28

reversing is likely to result in being attacked, an instant decision is necessary, as follows:

- If you assess that the intention of the road block may be to kill or injure you or your passengers:
 - ▲ Drive fairly fast through the roadblock if it physically possible. This may include ramming an obstacle in order to knock it out of the way. Do not drive so fast that you may lose control. Do not zigzag, since you are likely to roll the vehicle. Once through the roadblock, keep driving at a safe speed, even if you are being shot at, and send an immediate incident report as soon as you can. Your passengers should lie down throughout, or keep as low a profile as possible.
 - ▲ If it is not possible to drive through the roadblock (perhaps because the obstacle is too big), consider reversing back round the corner even if it will attract shooting. Then send an immediate incident report.
- If it is neither possible to reverse round the corner, nor to drive through the roadblock, you have at least two further options:
 - ▲ Slow to a halt, 5 metres or so in front of the roadblock, just as if you were at a normal checkpoint. Comply calmly with any demands made of you. It may be that the attackers do not wish to kill you: they may only want your vehicle and possessions, for example. If appropriate, negotiate with them and persuade them not to harm anyone. Send an immediate incident report as soon as possible, but do not do this within the sight or hearing of the attackers.
 - ▲ Or, particularly if you are certain that you will be killed if caught, you may decide to drive off the road and escape across country. If it is not possible to drive off the road, stop abruptly and tell all passengers to run. This is obviously very risky, but it may save some or all of your lives, in which case it is

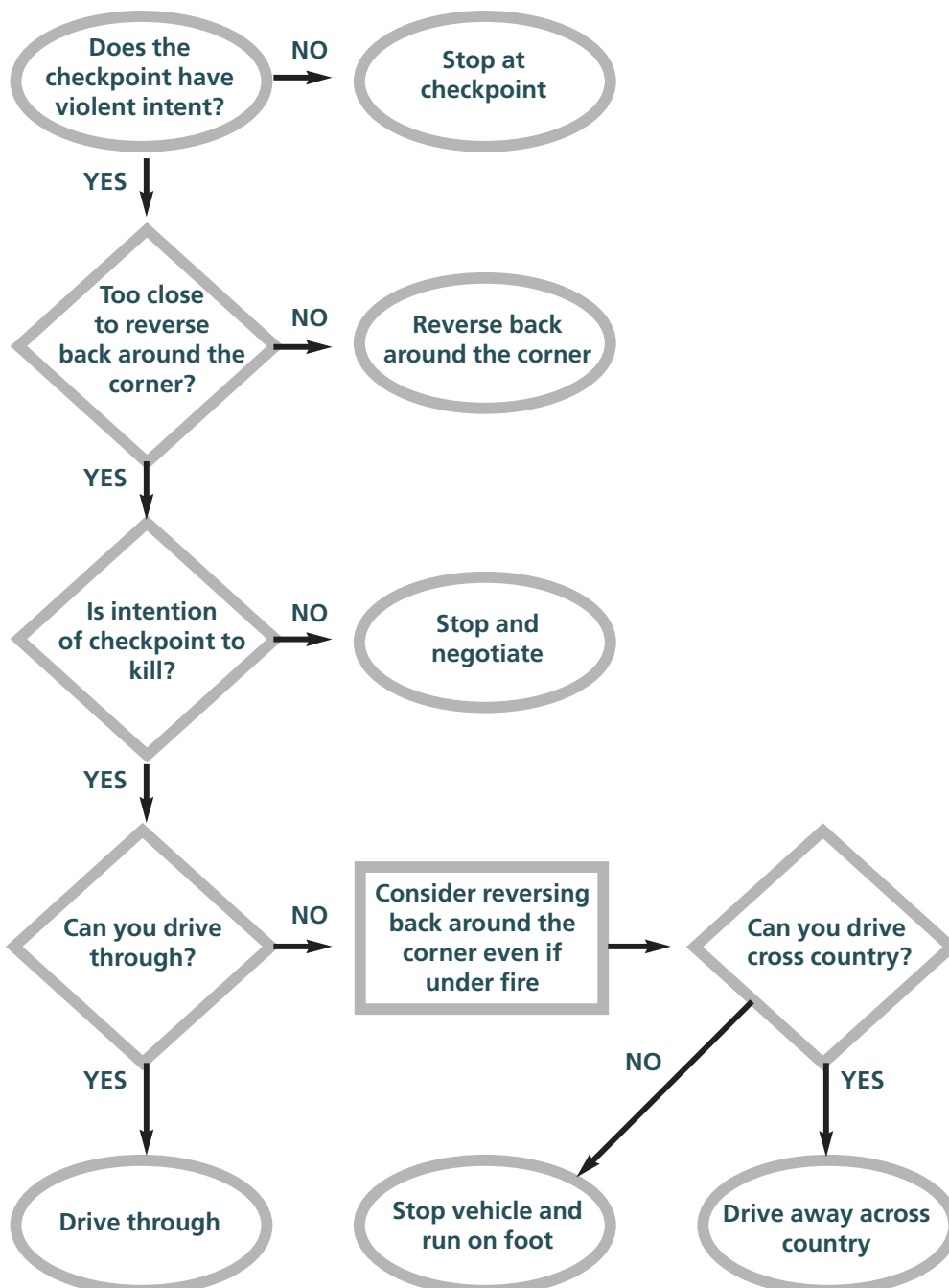
better than everyone being killed. It may be wiser for each person to run in a different direction, so that if some are caught, others may escape. Send an immediate incident report as soon as possible – so it is helpful if you can keep a radio with you as you flee.

- If you are confident that the intention of the roadblock is not to kill or injure:
 - ▲ Slow to a halt, 5 metres or so in front of the roadblock, as if you were at a normal checkpoint. Comply calmly with any demands made of you. Remember that losing a vehicle or other possessions is not important, compared to saving a life. Hand over anything demanded, swiftly and calmly. If the attackers then leave, make no sudden movements until they are out of sight. Then send an immediate incident report, if possible, and move all staff to a safe location.

SECURITY INCIDENTS: PREVENTION AND REACTION

A28

The following flowchart is a simplified illustration which summarises some of the possible procedures described above.



SECURITY INCIDENTS: PREVENTION AND REACTION

A28

Scenario two: ambush not using a roadblock

Driving along a road, you hear gunfire close by. It may hit the vehicle. Or you may not be sure if it is aimed at you, and it may not be clear where it is coming from.

- ▲ Accelerate, if it is safe to do so, and drive on past the ambush. (Assume that it is an ambush: do not take time to check.) Do not drive so fast that you may lose control. Do not zigzag, since you are likely to roll the vehicle. Keep driving at a safe speed, even if you are being shot at. Your passengers should lie down throughout, or keep as low a profile as possible. Send an immediate incident report as soon as you can.

It is difficult to make good decisions in the middle of an ambush. But it is a little easier if staff are competent, well trained, well briefed and experienced. It is better by far to avoid ambushes altogether, through good security assessments and wise decision-making.

In the heat of the moment, staff who have just survived an ambush can forget to send an immediate incident report. It is vital that they remember to report, both for their own safety and to warn other road users not to fall into the same ambush.

(e) Arrest or detention

Humanitarian staff are sometimes arrested or detained. The risk of this happening can be significantly reduced by:

- ▲ Good relations with local authorities and groups
- ▲ Appropriate behaviour, on and off duty
- ▲ Obeying local laws and customs
- ▲ Ensuring that all legal documentation is correct, and carried by all staff and vehicles as required
- ▲ Training and briefing staff before they begin their assignments

If a staff member is arrested or detained, their manager should take swift action. The best action to take will depend on the circumstances, but may include:

- ▲ Visit the staff member as soon as possible, to reassure them and to establish the facts
- ▲ Meet a senior official of the organisation which has detained your colleague. Depending on the circumstances, you may decide to request their release, or to protest at their detention and demand their release.
- ▲ Obtain the assistance of a lawyer, if necessary
- ▲ Inform other humanitarian organisations. If they consider the detention unjustified, they may wish to take coordinated action to persuade the authorities to release the person concerned.
- ▲ Inform the ICRC and ask their advice, if appropriate
- ▲ Inform consular authorities, if the staff member is from another country
- ▲ Inform the Next of Kin if the person is not released very quickly

In many cases, the knowledge that other international organisations are aware of the detention may be enough to persuade the authorities to release the detainee.

In other cases, the detention may be justified, if the detainee has in fact committed an offence or is reasonably suspected of having done so. If so, it is important to respect the duty of the authorities to ensure that correct legal procedures are followed. Your lawyer should advise on the best course of action.

The detention may in reality be a hostage seizure. This may not be apparent at first, but may become clear when demands are made for ransom, or other conditions for release. In this case see the section on kidnap in this Annex for further information.

(f) Assault

An assault may accompany a robbery or other crime. An assault may also occur with the simple aim of killing or injuring. Every situation is different, and you should use your judgement to decide the best response if you are assaulted. Options to consider include:

- ▲ Run away

SECURITY INCIDENTS: PREVENTION AND REACTION

A28

- ▲ Call for help, using radio, telephone or your voice
- ▲ Attract attention: scream, shout, use an alarm, sound your vehicle horn, etc
- ▲ Defend yourself
- ▲ Submit (this is only an option if you assess that your attacker will not try to kill you)

Self-defence techniques require training and practice, but can give self-confidence. Self-defence using an improvised weapon also requires skill, and the weapon could be taken from you and used against you. It is normally forbidden for staff of a humanitarian organisation to carry weapons.

(g) Bomb

Bombs can take a variety of forms, including:

- ▲ Car bombs
- ▲ Letter bombs
- ▲ Booby trap bombs
- ▲ Suicide bomb attacks
- ▲ Bombs dropped by aircraft

The first four of these are sometimes known as improvised explosive devices (IEDs).

Prevention

As with all other threats, it is important to assess the threat posed by bombs, if any. If you assess that there is a threat of bombs, you are likely to need specialist advice on what security measures to take.

A car bomb threat may require the prevention of vehicles from coming within a certain distance of any location regularly used by staff, and may oblige staff to check vehicles for bombs before using them.

A letter bomb threat may require specialist screening of letters and staff training. If a suspicious letter or package is discovered, it should be put down gently. Do not put anything on top of it, and do not put it in water. Evacuate the building and the area around until the package is examined by an expert. Suspicious characteristics to look for include:

- ▲ An unusual or unknown place of origin
- ▲ No return address

- ▲ An excessive amount of postage
- ▲ Abnormal or unusual size
- ▲ Oily stains on the package
- ▲ Wires, strings or metal foil protruding from or attached to an item
- ▲ Incorrect spelling, poor handwriting or typing on the package label
- ▲ Differing return address and postmark, or incorrect address
- ▲ Unfamiliar handwriting
- ▲ Peculiar smell. (Many explosives used by terrorists smell of shoe polish, machine oil or almonds.)
- ▲ Unusual heaviness or lightness
- ▲ The packaging may be soft but the contents will feel hard
- ▲ The package may be wrapped more than normal
- ▲ Uneven balance or shape
- ▲ Springiness in the top, bottom or sides
- ▲ The package may have been delivered by hand by someone you don't know

Never cut tape, strings, or other wrappings on a suspect package or immerse a suspected letter or package in water. Either action could cause an explosive device to detonate. Never touch or move a suspicious package or letter.

Most casualties from urban terrorist attacks are from flying glass. Any bomb threat, or threat of other explosions (shells, grenades, rockets etc), will require windows to be fitted with blast film, and possibly special net curtains and other measures, to reduce casualties from flying glass. Blast film should be polyester film 175 microns thick (including adhesive layers of multi-ply) or film with equivalent properties: thicker grades may be needed for large windows.

You should consider how your programme would continue if an explosion destroyed a key building, important documents or assets.

For further information, see "Bombs – protecting people and property", a guide published by the British Government Home Office²⁴.

Reaction

If a bomb is suspected or discovered, the best action

²⁴ Available in two parts at www.homeoffice.gov.uk/docs/bombs.pdf and www.homeoffice.gov.uk/docs/bombs2.pdf.

SECURITY INCIDENTS: PREVENTION AND REACTION

A28

to take will depend on the circumstances. As a general rule, the following procedure can often offer a framework for action:

- ▲ **CONFIRM** whether there is reasonable suspicion that it may be a bomb. Do not touch it or move it.
- ▲ **CLEAR** the area of people quickly, to a distance of at least 100 metres, but 400 metres if the suspected bomb is larger than a suitcase or is a vehicle. Leave doors and windows open, but do not stop to open them if this will delay your departure from the building. Do not use lifts/elevators. If possible, cut off electricity and gas supplies to the site, to reduce the fire hazard.
- ▲ **CORDON** off the area, at a radius of 100 metres (400 metres if the suspected item is larger than a suitcase or is a vehicle) from the suspected bomb, and allow no people to enter within the cordon.
- ▲ **CONTROL** the situation. Summon the police or other relevant authority. Follow their instructions when they arrive.

If a competent police officer or other suitable official is present when the suspected bomb is discovered, he or she will supervise the above procedures. If no such official is present, the senior manager present should supervise until the police or equivalent arrive.

Once the above steps have been carried out, the security forces will make the bomb safe or detonate it. No-one should re-enter the area until the security forces have given permission.

If a bomb explodes, be aware that another bomb may be in the area. Provide first aid to those who need it, while clearing the area of other people and calling the police or other relevant authority.

(h) Bomb threat by telephone

A bomb threat may be received by telephone. In this case the following procedure may be appropriate, depending on the circumstances:

- ▲ Keep calm, don't hang up
- ▲ Record the exact wording of the threat

- ▲ Questions to ask:
 - Where is the bomb right now?
 - When is it going to explode?
 - What does it look like?
 - What kind of bomb is it?
 - What will make the bomb explode?
 - Did you place the bomb?
 - Why are you doing this?
 - What is your name?
 - What is your address?
 - What is your telephone number?
- ▲ If possible, make a note of:
 - Background noises (street noises, house noises, music etc)
 - Does it sound like a local, long distance or international call?
 - The accent of the caller
 - The voice of the caller (loud, soft, clear, muffled, calm, emotional etc)
 - The caller's sex, estimated age
 - The time, date, duration and number called
- ▲ Report the call immediately to your manager and to the police or other appropriate security force

Evacuate the location immediately, following the procedure given under 'Reaction' above. Inform the police or other relevant authority.

Many bomb threats are hoaxes. But treat all bomb threats as real and urgent until the area has been searched, and the police have pronounced it to be clear. There have been cases where slow reactions to bombing warnings have led to additional deaths and injuries.

For further information, see "Bombs – protecting people and property", a guide published by the British Government Home Office²⁵. This also contains a form for completion by the person who receives a bomb threat phone call.

(i) Chemical, biological or radiological attack

It is beyond the scope of this Guide to give advice on the complex topic of chemical, biological or radiological attack. If a threat of this kind is identified, consider whether your staff should continue to work in the area. If you do continue to work, expensive

²⁵ Available in two parts at www.homeoffice.gov.uk/docs/bombs.pdf and www.homeoffice.gov.uk/docs/bombs2.pdf.

SECURITY INCIDENTS: PREVENTION AND REACTION

A28

training and equipment are likely to be necessary.

(j) Crowds

Crowds can be entirely peaceful. However, they can pose risks including theft and violence. A peaceful crowd can sometimes turn into a violent mob or a riot. It is important to be aware of when crowds are likely to form (such as during festivals or political demonstrations) and what their purpose is. If you assess that they may turn violent, keep away.

If you find that you are in a crowd which you think may become violent, try to keep a low profile and blend in as far as possible, while moving away from the crowd as soon as you can.

Never encourage a crowd to form (for example when planning a distribution) unless you are certain that you can meet all their expectations in a timely way.

(k) Earthquake

If you are working in an earthquake-prone area, you should take appropriate precautions. Consult earthquake expertise, which may be available locally. Issues to consider may include, but not be limited to:

- ▲ Assessing the risks of working in an earthquake-prone area
- ▲ Finding an earthquake-resistant building to live/work in (this may be difficult or impossible in some circumstances)
- ▲ Being prepared for an earthquake, for example as follows:
 - Secure equipment so it does not fall on people, fixing filing cabinets and bookcases to walls
 - Anchor and brace gas and fuel tanks
 - Restrain desktop computers and other appliances (for example with hook-and-loop ('Velcro') adhesive pads)
 - Install latches on cabinet doors and drawers
 - Stock emergency food and water, etc
- ▲ Recognising the signs of a tremor or quake
- ▲ Immediate action
- ▲ Post-earthquake action
- ▲ Other risks, e.g. broken gas or fuel pipes

(l) Fighting

Humanitarian staff should aim to avoid being in locations where there is armed conflict, unless there is a vital reason for them to be there and the likely benefits of their work outweigh the risks. Even so, any staff working in situations of fighting should understand the risks and should remain in the area only if they are freely willing to do so. In some cases the fighting may present little threat to humanitarian staff or programmes, in which case it may be assessed that the benefit of staying outweighs the relatively low risk.

By being well informed of the local situation, managers and staff should be aware of when tensions rise and fighting becomes more likely. They should adjust their plans accordingly, in order to avoid being exposed to fighting if and when it breaks out. In some cases this may mean being prepared to evacuate from the area. In other cases it may mean sheltering while the fighting goes on. The organisation may have a mandate to assist people during fighting – for example with medical treatment. If so, depending on the circumstances, the work may continue provided that staff are not directly threatened.

There is no substitute for training staff in reacting to the outbreak of fighting. Reading a manual cannot give anything like the same level of preparation. By teaching them the practical skills, then practising them in those skills until they can do them themselves, it becomes more likely that in a real event they will react appropriately.

Nevertheless, some written explanation in this Guide may be helpful. If you are caught in the open when shooting or explosions (such as mortar or artillery fire) take place, the correct action will depend on many factors including the type of fighting and your location. The following procedures may be appropriate, depending on the circumstances:

Shooting, when you are on foot in the open

- ▲ Drop to the ground and lie flat, unless you believe that you are the target and that you would still be visible to your attacker. If you believe you are the target, dash to a place

SECURITY INCIDENTS: PREVENTION AND REACTION

A28

which is out of sight of your attacker. Move rapidly away from the source of the shooting, remaining out of sight, towards a place of safety. If you assess that the shooting was not aimed at you, lie flat and remain still if it is safe to do so. If it is possible to roll or crawl into a ditch or other location that will shelter you from stray bullets, do so – but if there is a danger of landmines, remain out of ditches and other places which may be mined.

Shooting, when you are in a vehicle

- ▲ Assess rapidly what is happening and use your judgement to take the appropriate action.
 - Are the shots coming from ahead of you? If so, it may be best to stop, get out of the car and lie flat on the ground away from the vehicle – in a ditch if possible and if the area is not mined. If you assess that those shooting may wish to target you, it may be best to turn round and drive away.
 - If you cannot tell where the shots are, or if they are around you or behind you, it may be best to assume it is an ambush, accelerate as much as is safe, and drive on. The other alternative is to stop, get out of the car and lie flat on the ground away from the vehicle – in a ditch if possible, well away from the car (provided that it is not an area at risk of mines) since the car may attract shooting. You will have to judge which of these two options is best.

Shooting, when you are in a building

- ▲ Drop instantly to the floor. If it is possible to crawl without raising your profile to the designated shelter, or to an inner room or corridor that is better protected than other rooms from stray bullets, do so. Stay away from windows: shattering glass is a major cause of death and injury.

Explosions, when you are on foot in the open

- ▲ Drop instantly to the ground. Lie completely flat. If it is possible to roll or crawl into a ditch, into a building or behind a wall without raising your profile, do so. This may give you some protection. Otherwise, remain still. One explosion

may well be followed by another, which may be nearer to you. Most blast and shrapnel fly upwards from the site of the explosion in a cone shape, so your best defence is to stay as low as possible. In this way it is often possible to survive explosions that are very close by.

- ▲ Take account of the local situation. In some circumstances, grenade attacks are often followed by large volumes of indiscriminate fire. In other cases, initial small bombs are used to attract a crowd, and then a large bomb is timed to go off 5 to 30 minutes after the first, to kill many of the crowd. In these cases it is likely to be best to leave the area quickly after an explosion.

Explosions, when you are in a vehicle

- ▲ Stop the vehicle, get out fast and lie flat on the ground away from the vehicle, or in a ditch if available and safe. If however you assess that you may be targeted and that the risks of stopping are greater than the risks of remaining in the vehicle, then it may be best to drive away as fast as is safe. As always, the decision depends on an assessment of the situation, and good judgement.

Explosions, when you are in a building

- ▲ If you are in a building, drop to the ground and move away from windows. Many injuries and deaths are caused by shattering glass. If it is safe to do so, move (without raising your profile) into the pre-designated shelter, or to an inner room or corridor that is better protected than other rooms from stray bullets. Stay away from windows.

After you have taken the appropriate immediate action

- ▲ Provided that you are not a target of the attack, do not move until you are confident that the attack has finished. Beware: it may appear to have finished when in fact a second attack may be about to start. If there is a security officer for the humanitarian organisations, he or she may be able to announce the "all clear" by radio – but often this is not possible. You may therefore have to wait a long time

SECURITY INCIDENTS: PREVENTION AND REACTION

A28

before you can be reasonably confident that no more attacks are coming.

- ▲ If you assess that you may be a target of the attack, use your judgement to determine the best course of action – in some circumstances it may be best to move to a safe location rather than to stay in the same place.
- ▲ As with all incidents, do not use the radio unless it is absolutely necessary. Do not call your colleagues to check if they are safe: if they need help, they will call you. Keep the radio channels clear so that those who have emergency needs can use them.
- ▲ Report the incident as appropriate, bearing in mind the need to keep radio channels clear while others may need them for emergency messages.

(m) Fire

All staff should be aware of the fire procedure. A simple framework, applicable in many circumstances but not all, is as follows:

- ▲ If you discover a fire, raise the alarm by shouting "Fire!" and operating the fire alarm, if there is one
- ▲ Use a fire extinguisher or blanket to put out the fire if it is safe to do so and will not put your life or others' lives at risk
- ▲ Leave the building as fast as possible. Walk rather than run, in order to avoid accidents. Go to the fire assembly point.
- ▲ Close doors behind you as you leave, to help prevent the spread of fire
- ▲ Remember that smoke can kill. If there is smoke, crawl to keep your mouth below the level of the smoke.
- ▲ A nominated person should check that the building is empty of people. If the building is large, a system of fire wardens should ensure that all parts of the building are empty of people. A roll call should be taken at the fire assembly point to ensure that all occupants are accounted for.
- ▲ Call the fire brigade, if there is one. If not, raise the alarm among neighbouring buildings and improvise fire extinguishing efforts.
- ▲ Do not re-enter the building until a properly

qualified person announces that it is safe to do so

For suggested fire safety precautions, see Annex 12.

(n) Flood

If there is a risk of flooding, this should be identified in a security assessment, and measures taken accordingly. If possible, buildings should not be used which are in flood-prone areas, and routes should not be used at times when they may be flooded.

If however there is a risk of flood, the following simple precautions may help:

- ▲ Construct barriers to divert water and protect buildings
- ▲ Store any critical items, which may be damaged by flooding, above the level which may be reached by the water
- ▲ Ensure that there is sufficient accommodation on an upper floor which cannot be reached by the water
- ▲ Keep a stock of food, water and a means of cooking, above flood level
- ▲ Keep a stock of relevant medicines
- ▲ Ensure that there are toilet facilities, even if only improvised ones, above flood level
- ▲ Keep communications equipment above flood level. Ensure that batteries are kept charged. If possible, store a small generator above flood level to provide power for battery charging and other needs.
- ▲ If necessary, store a boat for transport during floods. Make sure that it is only used when it is safe to do so, and that it is used by a qualified and competent person. Other safety equipment may be necessary, such as life jackets.

(o) Fraud

Fraud is defined as a deliberate, improper action which leads to financial loss to the organisation²⁶. This includes theft of goods or property; falsifying expenses claims; and falsification (or destruction) of records to conceal an improper action. Fraud does not include: accounting errors; actions condoned by established practice; and cases where no loss is incurred.

Other possible irregularities include unauthorised

²⁶ This definition and part of this section is adapted from the Mango (Management Accounting for Non-Governmental Organisations) Training Manual, available from www.mango.org.uk.

SECURITY INCIDENTS: PREVENTION AND REACTION

A28

activities for private gain: e.g. 'borrowing' from petty cash; use of vehicles; or abuse of telephones and other equipment.

Inevitably, fraud has a damaging effect on the organisation. Not only does it divert resources from beneficiaries, but it can damage effectiveness, morale, credibility, and ultimately the organisation's funding and even its survival.

Incidents of fraud and irregularities require sensitive handling to minimise the long-term impact. It is important to be prepared to deal with any occurrences of fraud or financial irregularity by having a written procedure which covers the steps that need to be taken.

It is of course better to prevent fraud than to have to react to it, by having good financial procedures in place – see Annex 11.

If, however, fraud does occur, or you think it may have occurred, the following steps may offer helpful suggestions, depending on the circumstances:

- ▲ Do not overlook the fraud or suspected fraud. Take action.
- ▲ If there are key documents or items of evidence, take steps to secure them before informing staff of any suspected fraud
- ▲ Announce an investigation. The investigation should be conducted by someone competent to do so, who is independent of anyone who could have been involved in the fraud. An alternative, perhaps appropriate where fraud is suspected but has not definitely occurred, is to announce a financial inspection, possibly one required by HQ. (This is easier to announce if it is known in advance that HQ is liable to announce financial inspections without notice.)
- ▲ The investigation should result in a written report to the Director of Finance, and should include:
 - Confirmation of whether a fraud has taken place

- The amount of loss involved
- The identity of the person(s) who appear to have committed the fraud, if known
- Identification of any failures on the part of procedures or staff which enabled the fraud to take place
- Identification of any staff who should face disciplinary action
- Recommended lessons to learn for the future, and any procedures which need to change to prevent further fraud

- ▲ The Director of Finance or another senior manager should then ensure that any necessary disciplinary and other action is taken swiftly

For further information on reaction to fraud and other aspects of good financial management, see www.mango.org.uk.

(p) Grenade

A hand grenade is a small, hand-thrown bomb. It explodes either immediately or after a few seconds, sending blast and shrapnel over a wide area.

If a grenade is thrown near you, the following procedure reduces the risk of harm in many circumstances. You should make a rapid judgement to decide the best course of action.

- ▲ Shout "Grenade!" and drop instantly to the ground, covering your head. If you can do so in such a way that there is a barrier between you and the grenade, do so. But the crucial action is to drop to the ground, since the blast and shrapnel from grenade typically rise in a cone shape. For this reason it is sometimes possible to escape injury by lying flat, even if you are near the grenade.
- ▲ If there is time, lie with your head furthest from the grenade, and your legs crossed, pointing towards the grenade
- ▲ Others should drop instantly to the ground in the same way as soon as they hear someone shout "Grenade!"
- ▲ After the explosion, check to see if there is another grenade, or other type of threat, before moving

SECURITY INCIDENTS: PREVENTION AND REACTION

A28

If there is no explosion within 30 seconds, crawl away on your stomach until you are in a safe area, with solid cover between you and the grenade. Ensure no-one approaches the grenade. Report the incident to the appropriate authorities.

- ▲ Take steps to ensure that there is no further danger
- ▲ When you are confident that there is no further immediate threat, give first aid to those who need it. Bear in mind that in some circumstances a grenade may be followed by other violence, in which case you should leave the area quickly.
- ▲ Call for medical help
- ▲ Report the incident

(q) Hijack – vehicles

Vehicle hijackings may be carried out for various reasons including the following:

- ▲ To steal the car or other belongings carried in it
- ▲ To use the occupants as hostages
- ▲ To use the car for another crime, perhaps using the car's identity as a cover
- ▲ To cause a political effect, such as demonstrating that the local security forces do not have full control of the area
- ▲ To injure or kill the occupants, perhaps in order to cause a political impact, or to ensure that the occupants do not reveal the identity of those who have stolen the vehicle

Because of the dangers involved, it is important to avoid hijack if at all possible. While one can reduce the chances of being hijacked, one cannot eliminate the possibility without stopping all travel. In some circumstances, stopping all travel, at least for a time, may be the best decision. In other circumstances, humanitarian managers may decide that, if for example the risk of hijack is very low and travel is essential in order to save many lives, travel is justified. This is a matter for case-by-case decision by experienced and competent managers.

Armoured vehicles can be a further protection against hijack, appropriate in some circumstances. They require drivers who are familiar with the differ-

ent handling qualities of these vehicles. They are expensive to buy and maintain.

A hijack may be attempted in many ways. Among the most common are:

- ▲ Setting up a roadblock or checkpoint to stop the vehicle
- ▲ Surrounding the vehicle when stopped at traffic lights or in a traffic jam
- ▲ Using another vehicle to cut in on or ram the target vehicle, to force it to stop
- ▲ Setting up a fake accident or breakdown, to induce you to stop and offer help. The attackers, posing as casualties or bystanders, then turn on you. If you assess that this ruse is a significant possibility in your area, all drivers should be instructed not to stop at accidents or breakdowns, but to drive on in case it is an attempted hijack.

To prevent hijacking if you are being followed, the following action may in some circumstances be appropriate²⁷:

- ▲ Try and stay calm and do not start driving fast. You will alert the people who are following you apart from increasing the risk of an accident.
- ▲ Change direction to see if they still follow you but NOT into a small side road or somewhere you don't know. Keep to busy parts of town.
- ▲ Do not drive to your home but go to a police station, petrol station, UN compound etc
- ▲ If the hijackers start closing up on you, try and keep to the centre of the road to make it harder for them to overtake and cut in front of you. But be aware of the risk of causing a collision with oncoming traffic.

If an attempted hijack does take place, a response similar to the response to an ambush may be appropriate (see the section on Ambush, in this Annex, for suggested anti-ambush procedures). If you assess that the hijackers are likely to kill or seriously injure occupants of the vehicle, driving away is likely to be the best response, if possible, even if this poses some risks.

²⁷ Adapted from UN Security Coordinator for Kenya security advice

SECURITY INCIDENTS: PREVENTION AND REACTION

A28

If a hijack succeeds and the hijackers demand the vehicle or other property, cooperate calmly and quickly, without making sudden movements which might be misinterpreted. Hand over anything that they request – remember that no property is worth risking life for.

Note that even innocent movements, such as reaching for the seatbelt release catch or for a document, can be interpreted as reaching for a weapon, so warn the hijacker before making such a movement.

If a hijack succeeds and staff are taken hostage, see the section on Kidnap, in this Annex, for suggested action.

(r) Hijack – aircraft

Aircraft hijacking is statistically rare, so it is unlikely that you will be the victim of a hijack. Aircraft may be hijacked for the following reasons, among others:

- ▲ To cause a political effect, such as obtaining publicity for a political cause
- ▲ To carry out a terrorist attack using the aircraft
- ▲ A mentally unbalanced person may attempt a hijack

The best protection against hijack is to use only airlines which have good security procedures. Passenger vigilance can also help, by reporting anything suspicious to airline or security staff. As always, there is no 100% secure method of preventing hijack.

The following precautions²⁸ may help you to cope, should a hijack occur:

- ▲ Discreetly get rid of anything that you cannot explain or which might make the hijackers angry or suspicious
- ▲ Remain calm and obey the hijackers
- ▲ Respond simply, if you are asked questions by the hijackers. Do not say or do anything which might cause the hijackers to take an interest in you.
- ▲ Use your native language, even if the hijackers' language is different and you are able to speak

it. This could provide you with information as to what the hijackers intend to do next.

- ▲ Try to appear uninterested as to what is going on around you. Sleep, read a book, etc.
- ▲ Try to maintain your composure. Fear is natural. Pause, breathe deliberately and slowly, and try to organise your thoughts.
- ▲ Since the hijackings on 11 September 2001, some think that passengers should consider rushing the hijackers as a group, if they assess that the hijackers intend to kill more people by crashing the plane into a target. The idea is that, if a large number of passengers rush the hijackers, possibly carrying pillows, cushions or other items to act as shields, then some may be injured or killed but the hijackers are likely to be overwhelmed. In this way the target will be spared, and the passengers will survive if the aircraft can be landed safely. This Guide can make no recommendation as to the right course of action to follow: it must be an individual decision based on the circumstances at the time.
- ▲ In the event of a rescue attempt, slide down in your seat as far as possible or get onto the floor, and cover your head with your hands or a pillow to avoid being injured
- ▲ After the incident, you may feel a strong need to tell your story in detail. This is normal. Consider requesting a debriefing from a trained counsellor. Some stress reactions can appear after a delay, sometimes months later. If so, recognise them and ask for counselling if necessary.

(s) Kidnap

Humanitarian staff are unfortunately sometimes at risk of kidnap. They may be kidnapped for several reasons including:

- ▲ To hold for ransom
- ▲ To cause a political effect or achieve publicity
- ▲ To be used as human shields

As always, prevention is better than cure, so security procedures should be designed to minimise the possibility of kidnap, where it is assessed as a significant threat.

If kidnap occurs, HQ should immediately set up a cri-

²⁸ Adapted from the UN booklet *Security in the Field*, UNSECOORD, 1998

SECURITY INCIDENTS: PREVENTION AND REACTION

A28

sis management team. It may be appropriate for a similar team to be set up at the field office responsible for the staff member who has been kidnapped. It should be made clear at once which manager has responsibility for managing the incident. That manager should then consider the following actions, depending on the circumstances and his or her assessment of the best course of action:

- ▲ Inform the local police and other appropriate authorities
- ▲ Inform all relevant parties of the name and contact details of the incident manager. Request that no action be taken in relation to the incident without prior agreement with him or her.
- ▲ The incident manager should delegate responsibilities to colleagues as appropriate: e.g.:
 - Contacting Next of Kin (see Annex 22 on informing Next of Kin). This should be a top and very urgent priority. Failure to do this quickly can damage the relationship of trust with the staff member's family, particularly if they first hear the news through the media. This could then make the management of the crisis much more difficult.
 - Answering enquiries from the press
 - Keeping contact with all relevant staff and other agencies
 - Providing 24-hour communications and logging all messages and events
 - Marking maps
 - Ensuring that the crisis management team has sufficient food, water and rest
- ▲ Make a plan. Will you negotiate directly with the kidnappers, if that is possible? Or will you appoint an intermediary? (A trusted intermediary is often thought preferable, to give time for decision-makers to consider their responses to any messages from the kidnappers.)
- ▲ Decide whether to call in specialist advice, either from the police or from a reputable company specialising in hostage negotiations. It may help if contact has been made with such a company before any kidnap occurs. If you are

not sure that you have the necessary expertise to handle a kidnapping, specialist advice from a reputable company is strongly recommended.

- ▲ Allocate the necessary resources – human, financial and other – to ensure that your plan has the best possible chance of success
- ▲ Carry out your plan
- ▲ While you will naturally desire to conclude the incident safely and as quickly as possible, kidnap negotiations can sometimes last months or even years. Prepare the crisis management team for this, while encouraging them to remain optimistic. Keep morale high: enough food and rest are helpful, but possibly the greatest aid to morale is to manage the incident well, keeping everyone fully informed, and taking the best available advice.
- ▲ Ensure strict confidentiality from the onset of the crisis. Information should be shared only on a need to know basis. This may require the usual management chain to be bypassed, e.g. if someone is part of the crisis management team, he or she should be exempted from reporting to his or her superior on the crisis.

The staff member who has been kidnapped can improve their own chances of survival and early release in a number of ways including²⁹:

- ▲ Your only job is to survive. It is the HQ's job – not yours – to achieve your freedom.
- ▲ At the time of your seizure, do not attempt to fight back. The time during and soon after the abduction is the most dangerous. Do not play the hero; do not talk back or act "tough".
- ▲ You may be blindfolded and drugged
- ▲ Be calm, quiet and cooperative. Make no sudden movements.
- ▲ Try not to give up clothes or identification
- ▲ Try not to allow your kidnappers to exchange clothes with you: if there is a rescue attempt you could be mistaken for a kidnapper, and attacked
- ▲ Be certain that you can explain everything you

²⁹ Adapted from UN Hostage Incident Card (undated)

SECURITY INCIDENTS: PREVENTION AND REACTION

A28

have on your person. Do not carry any items that may call into question your motives or status within the mission.

- ▲ Fear is a normal reaction. Try to relax, pause, take a deep breath and accept the situation. Focus your mind on pleasant scenes, memories or prayers.
- ▲ As the situation stabilises, continue to keep a low profile.
 - Be cooperative without appearing either servile or antagonistic. Follow the instructions of your captors.
 - Be cautious about making suggestions to your captors, as you may be held responsible if something you suggest goes wrong
 - Don't beg or plead, and try not to cry. It is normal to feel humiliated, but do all you can to maintain your dignity.
 - Do not make threats against your captors or indicate that you would testify against them
 - Avoid appearing to study your captors, although if you are able to notice unobtrusively their appearance, dress, and apparent rank structure, this may help the authorities after your release.
 - Be a good listener. Do not argue. Be polite.
- ▲ Try to gain your captors' respect and try to build rapport with them. An excellent topic of discussion is family and children.
- ▲ Emphasize that as a humanitarian, you are neutral and not involved in politics
- ▲ Encourage your captors to let the authorities know your condition and whereabouts
- ▲ Take care of yourself and build a daily routine: exercise, stay tidy and clean, sleep when possible
- ▲ Eat and drink even if you are not hungry
- ▲ Politely draw attention to anything you need or want, such as food, water, medicine, use of the toilet, books or writing materials
- ▲ Be patient and mentally prepared for a long captivity – perhaps months
- ▲ Stay mentally active: read, write, exercise your memory
- ▲ Do not believe everything you are told
- ▲ Do not despair. Your survival chances increase with time.
- ▲ Do not attempt to escape unless you are certain you will be successful

- ▲ If there is a rescue attempt by force, drop to the floor and keep your hands over your head.
- ▲ Once the situation stabilises, or when the rescuers ask you to, identify yourself.
- ▲ Do not negotiate your own release for a ransom, even if your parents or friends are rich. This would conflict with the negotiations being conducted by your organisation.
- ▲ If released peacefully, this can also be a dangerous time. Obey instructions promptly. Make no sudden movements. Stay alert. Be prepared for delays and disappointments.

Ransom should not be paid. All humanitarian organisations should have a clearly stated policy that ransom will not be paid in case of kidnap, since to do so encourages more kidnapping. The paradoxical truth is that, by paying ransom, organisations place their staff at greater risk than if they do not pay ransom. All staff should be informed of this policy before signing their contract, and the contract should clearly mention it as a condition of employment.

Once the kidnap victim has been released, he or she will need time and space to recover. There may be medical or psychological needs, so a full medical and psychological assessment should be arranged, with counselling if appropriate. The needs of the victim's family should also be catered for.

Throughout the crisis, significant events and decisions should be recorded, and lessons learned wherever possible. After the end of the crisis a report should be written identifying any lessons to learn.

By good leadership, good advice, efficient teamwork and a caring attitude, a kidnap incident may be well managed to achieve a successful result.

For more information on kidnapping, see chapter 13 of *Operational Security Management in Violent Environments*³⁰.

(t) Looting

Looting is a common problem in situations of disorder or conflict. It can affect any location including shops, warehouses and homes. If looters cannot be prevented,

³⁰ K. Van Brabant (2000) *Operational Security Management in Violent Environments* published by ODI Humanitarian Practice Network as Good Practice Review No. 8. Available as free download from www.odihpn.org.

SECURITY INCIDENTS: PREVENTION AND REACTION

A28

remember that life is more valuable than property: do not risk injury from looters in order to protect property. The risk from looting can be reduced by simple precautions including:

- ▲ Keeping reduced levels of stock in warehouses
- ▲ Making copies of key documents and records and keeping them elsewhere
- ▲ Bolting safes to walls or floors and minimising the quantity of cash in them
- ▲ Distributing goods between a number of sites
- ▲ Ensuring doors and windows are strong, and strongly locked
- ▲ Removing logos and any form of agency identification from vehicles so that the looters are not mistaken for agency drivers and staff
- ▲ Ensure you have records of serial numbers of vehicles and other high-value equipment, to help you trace and recover them in future
- ▲ Putting high value items in containers and welding them shut. Stack high value containers on top of others so that there is no access from ground level
- ▲ Blocking the doors of a warehouse with filled containers with welded doors
- ▲ Distributing valuable items among trusted staff (especially those who can keep them safe in rural areas) – provided that this will not put them at unacceptable risk
- ▲ Keeping valuable items such as vehicles out of sight. Consider immobilising vehicles, for example by removing the wheels (if you may need a vehicle for an evacuation or other urgent journey, do not immobilise it if it will take some time to make good again).

(u) Medical emergency

In a medical emergency, staff should follow standard first aid procedures. A doctor or nurse should be called if possible, and depending on medical advice the casualty should be removed to a medical facility as soon as possible.

A doctor should assess whether medical evacuation (Medevac) is necessary. See Annex 20 for further information on Medevac.

(v) Mines, booby traps and unexploded ordnance (UXO)

A common risk is from mines, booby traps or unexploded ordnance (UXO). Unexploded ordnance is unexploded ammunition such as bombs, grenades, rockets, shells or bullets. It is also sometimes referred to as “explosive remnants of war” (ERW).

Before entering any area where there may be a threat from mines, booby traps or UXO in your area, all staff should be properly trained in Mine Risk Education (MRE) by a qualified instructor.

In an area where mines, booby traps or UXO may exist, it is vital that all staff are fully aware of the threat; trained in how to avoid it and how deal with an emergency; and equipped as necessary. Make sure that all staff know what to do and whom to contact for help in case of a mine/UXO emergency.

Avoiding mines, booby traps and UXO

If you are working in an area where mines, booby traps or UXO have recently been a problem, you should make yourself familiar with what they look like. There are many different types. All of them can cause death and serious injury. You should also know the local methods for marking mines – they may be different from the internationally recognised signs.

Avoid going anywhere unless you are sure that it is clear of all mines. This means that you should have accurate information on the location of any areas that have not yet been cleared of mines. Sources of information (not all of them necessarily reliable) may include:

- ▲ Local police
- ▲ Local military force
- ▲ Local civilian authorities
- ▲ Hospitals and health posts
- ▲ International military force (if present)
- ▲ International police force (if present)
- ▲ UN security officer (if present)
- ▲ Mine clearance organisations (if present)
- ▲ Local people
- ▲ Other humanitarian organisations

SECURITY INCIDENTS: PREVENTION AND REACTION

A28

If in doubt, don't go to an area that you are unsure of.

All staff should avoid touching or approaching any object which may be a mine, booby trap or UXO. Proximity to mines and UXO is always dangerous and should be avoided. Even objects that appear to have exploded should not be approached. They can still be lethal for at least the following reasons:

- ▲ They may not have fully exploded
- ▲ They may contain poisonous substances
- ▲ They may be a decoy for a booby trap.

People are sometimes tempted to collect fragments of exploded ammunition, or even live ammunition, as souvenirs. This should always be avoided, both because of the dangers mentioned above and because of the suspicion that can arise if you are found in possession of such items.

Other good practice in areas which may have a threat of mines, booby traps or UXO includes:

- ▲ Tell your colleagues where you are going, always – including when off duty or at weekends
- ▲ Stay within radio contact
- ▲ Carry a first aid kit. Ensure all staff are trained in first aid.
- ▲ Travel with a local guide, if they are well informed
- ▲ Only use roads and tracks that have been well used, recently, by others
- ▲ Remember that mines may have been freshly laid, so that even a well-used track may have new mines in it. Allow sufficient time in the morning for local traffic to have travelled the roads before you.
- ▲ Do not move onto the verges of roads: stay on the tarmac (or if not tarmac, on the well-used road surface). This applies when in a vehicle and on foot.
- ▲ Do not approach suspicious objects. Mines and booby traps are sometimes disguised as attractive or interesting objects such as a toy, a cigarette lighter, etc.

If you discover mines

It can happen that, even if you think you have reliable information, you unexpectedly find yourself in

an area that has mines. Page 51 and the following pages of the Landmine and UXO Safety Handbook³¹ gives advice on what to do in this situation. Note that many Mine Risk Educators now advise against prodding for mines, but instead advise staff who find themselves in a minefield to wait for help.

As soon as you can safely do so, report the incident to your superior and to responsible local authorities. Remember that it is not safe to use a radio, mobile or satellite phone near mines, booby traps or UXO, as radio signals may detonate them.

There is a debate among professionals as to whether non-specialist staff who have found a mine, booby trap or UXO should be instructed to mark the location. While marking it may warn someone else and protect them from injury, a non-specialist might accidentally detonate the device by the very act of marking the location. Whatever policy the organisation decides to adopt, staff should be clearly instructed on this point.

For further advice on mine awareness and procedures, see the UN/CARE International Landmine and UXO Safety Handbook.

(w) Rape and sexual violence

Everyone, male and female, is a potential victim of sexual violence. It may take a variety of forms. It has such a serious impact on its victims that great care should be taken to minimise the risk of it happening. How to minimise the risks will depend on the local situation, but may include:

- ▲ Avoid walking or driving alone, particularly at night
- ▲ Avoid isolated, unsafe or poorly lit locations
- ▲ Avoid bars or clubs where crime is known to take place
- ▲ Trust your instincts – if they tell you to leave, leave immediately
- ▲ Avoid drugs and excessive use of alcohol
- ▲ Carry an alarm
- ▲ Carry a radio or mobile phone
- ▲ Ensure that drinks are not deliberately contaminated with drugs
- ▲ Dress unobtrusively and appropriately, bearing

³¹ CARE and UNSECOORD, Landmine and UXO Safety Handbook, 2000. Contact MineAction@un.org, website www.un.org/Depts/dpko/mine/.

SECURITY INCIDENTS: PREVENTION AND REACTION

A28

- ▲ in mind the local culture
- ▲ Wear comfortable shoes
- ▲ Socialise in groups rather than alone
- ▲ Share accommodation rather than living alone

Although the great majority of rape attacks are against women, some are against men. Victims of rape require sensitivity and confidentiality, and will usually require counselling and/or medical treatment.

If a rape takes place, a sympathetic person of the same sex as the victim should immediately be assigned to comfort her or him. A doctor, if possible of the same sex, should examine the victim as soon as possible in case urgent treatment is necessary. This may include treatment for sexually transmitted diseases including HIV; the prevention of pregnancy; or treatment of injuries.

The victim's confidentiality should be respected. The police should be informed, if the victim consents, so that they may investigate the crime. Specialist counselling may be necessary – seek medical advice and consult the victim about this.

It will probably be necessary for the victim to be given immediate leave, to recuperate. The victim may wish to leave the area permanently, or to end their contract altogether. A senior manager should ensure that full support is given, and that a suitable agreement is reached on the staff member's immediate future.

Sexual assault and its aftermath can be a terrifying experience. Victims often react with a combination of fear, anger and shame and find it difficult to discuss the attack or seek help.

If you are assaulted your options are likely to be:

- ▲ Passive resistance – do or say anything to ruin the attacker's desire to force sexual contact with you
- ▲ Active resistance – shout for help; use an alarm; run away if there is somewhere safe to run to; or fight back furiously, such as with a knee to a man's groin
- ▲ Submit – do this only if you sense your life is in danger. Survival becomes your objective.

If you are assaulted, you will have to decide whether or not to report the crime. If you do, the police are likely to question you in detail about the event. Sometimes the police behave very professionally, treating the victim with dignity and respect. In other instances, the police may be less sensitive. You will need to have a medical examination before washing, in order to preserve evidence. Insist on being examined by a doctor or nurse of the same sex. Medical treatment may be necessary.

You can ask a friend to go to the police with you – many people find it helps not to be alone.

Various reactions can happen. You may have nightmares or not be able to sleep. You may not want to eat. You may experience mood swings. You may feel guilty, have difficulty making decisions, or find that you cannot stand anyone touching you. Almost any reaction is normal, and it will take some time to recover.

Remember that you are not alone. It usually helps to talk about it with a sympathetic person of the same gender: try to do this if you can. A shocking experience can upset anyone in this way. There is nothing to be ashamed about. It is not your fault, and you don't have to cope with it on your own. Help is available, so ask for any help you need.

Witnesses of rape and sexual violence and colleagues of victims will also be affected and will need appropriate support.

Counselling may also be helpful. The sympathetic support of close friends and/or colleagues will be essential. The team leader should ensure that such support, and specialist help where necessary, is provided. It may take a long time for the victim to recover fully.

For more information on rape and sexual violence, see chapter 12 of *Operational Security Management in Violent Environments*³².

³² K. Van Brabant (2000) *Operational Security Management in Violent Environments* published by ODI Humanitarian Practice Network as Good Practice Review No. 8. Available as free download from www.odihpn.org.

SECURITY INCIDENTS: PREVENTION AND REACTION

A28

(x) Robbery

Robbery may or may not be accompanied by violence. It can be a very frightening experience. If carried out on a person away from their home or workplace, it is sometimes known as mugging.

Staff should take precautions to avoid robbery, for example by:

- ▲ Keeping to areas known to be low-risk
- ▲ Avoiding poorly lit or isolated places at night
- ▲ Avoiding going out alone
- ▲ Carrying an alarm
- ▲ Carrying a radio

If robbery is attempted, try to call for help by:

- ▲ Activating your alarm (if you have one)
- ▲ Calling for help on the radio – even a one-word call may be enough to alert colleagues if there is no time to say more
- ▲ Shouting or screaming

If you assess that it is safe to escape by running into a home, or by out-running your attackers, do so. If not, cooperate calmly with them by giving them what they ask for. Make no sudden movements. Do not risk injury in order to protect material possessions.

As soon as the attack is over, move rapidly to a safe place and report the incident. Try to remember the details of your attackers' appearance, to help the police to identify them.

It can be helpful to keep your money in several different places on your person, such as two pockets and a wallet or purse, plus a money-belt. In this way you may be able to give the muggers the contents of only one pocket and a wallet or purse, for example, if the muggers do not notice the other places. It is good to limit the amount of cash you carry.

Robbery can also take place at the home or workplace. In this case, if you can lock the door before the robber is able to enter, do this – provided that it is safe to do. Call for help and sound the alarm, if it is safe to do so.

If the robber succeeds in entering the building, it is usually best to cooperate calmly by giving them what they ask for. Make no sudden movements. When they have left, secure the building or move to a safe place, and report the incident as soon as possible.

(y) Sexual harassment

Sexual behaviour varies widely from culture to culture. (In one culture, for example, women who object to being harassed by strangers on the street may be punched and knocked down by them.) What is regarded as harassment in one society may be regarded as the norm in another. Humanitarian organisations should set a clear policy on what is considered to be harassment and let all staff know what this is, while encouraging their staff to be aware of the cultural context and to take appropriate precautions.

Sexual harassment can be very distressing. If left unchecked it can lead to sexual violence. But even if it does not lead to violence, it is a serious issue in its own right, often causing both psychological and physical problems. It can be caused by a male or female harasser, and take many forms including:

- ▲ Constant invitations for drinks, dinner, dates
- ▲ Suggestive remarks
- ▲ Close physical contact
- ▲ Suggestive looks
- ▲ Uninvited visits to your home or hotel room
- ▲ Sexual gestures
- ▲ Pressure to engage in sexual activity
- ▲ Threat of, or actual assault

If facing sexual harassment, take time to think about how you will respond. Options may include:

- ▲ Ignore the advance. In some cases, this may persuade the harasser to stop
- ▲ Confront the harasser. If you stop and politely ask, "Were you speaking to me?" this may embarrass the harasser into desisting.
- ▲ Tell the harasser directly that you do not like what he/she is doing, preferably in the presence of a witness.
- ▲ Get help, from a trusted friend, colleague or manager.

SECURITY INCIDENTS: PREVENTION AND REACTION

A28

It is entirely understandable if you do not wish to report the harassment, but it is helpful if it is reported immediately to a manager. If a manager is the harasser, a more senior manager should be informed instead. The manager should then take immediate steps to warn the harasser, and to protect the person being harassed. If the harasser is a member of staff, disciplinary action is likely to be appropriate. It may be appropriate to inform the police, if a crime has been or may have been committed. Counselling should be offered if necessary.

If you do not wish to inform a manager, many organisations retain an independent counsellor, whom you may wish to speak to confidentially. He or she should be able to offer advice, or to direct you to appropriate advice and help.

It is often helpful to keep a log of incidents, including dates, content of conversations, and witnesses. Do not leave this log at work, or anywhere where it may be found.

(z) Shooting

See under "Fighting" above.

(aa) Terrorism

The word "terrorism" can be used in many ways, to cover a wide variety of incidents. For this reason it is usually more helpful to describe an incident in terms of what has actually happened. Has a bomb exploded? Was there shooting? Has a person been kidnapped? Then react to the event accordingly.

It is, however, important to take account of the motive behind an incident, when deciding on how to react and how to protect staff against future incidents. In this sense, the terrorist nature of an incident may affect reactions and security measures.

A humanitarian organisation may be the victim of a terrorist act by accident, or because it is perceived as associated with a government or group hostile to the terrorists. Terrorist motives may include:

- ▲ To gain publicity
- ▲ To provoke a reaction, for example by government or by security forces

- ▲ To change the behaviour of an organisation

(bb) Weapon finds

If you discover a weapon, or you are offered the chance to handle one, do not touch it. All kinds of firearms, guns, mines, grenades etc can fire or explode if not correctly handled by a trained person. There is also a risk of being trapped into adverse publicity: if you are photographed holding a gun, even if you were only holding it for a few seconds out of curiosity, you and your organisation could suffer damaging exposure in the press.

Any weapons finds should be reported to the police or other appropriate authority.

SECURITY INCIDENTS AND 'NEAR MISSES': REPORT FORMAT

A29

An agreed incident report format helps to ensure a quick and effective response to a security incident. It provides the essential information in a logical order, allowing managers to make soundly-based decisions.

It is important that an incident report states the facts and that any analysis or opinion is either clearly identified or left for the next stage of incident inquiry and analysis. Do not confuse fact and opinion.

There are typically three types of incident report:

- ▲ **Immediate incident report**, sent the moment the incident begins or as soon as possible thereafter, often over the radio
- ▲ **Follow-up incident report**, giving more information as soon as this is possible
- ▲ **Full incident report**, sent after the incident is over. This is usually written.

A common format for an **immediate incident report** is as follows:

- ▲ **Who?** – who has the incident happened to?
- ▲ **When?** – when did the incident happen?
- ▲ **Where?** – where did the incident happen?
- ▲ **What has happened?**
- ▲ **What have you done about it?**
- ▲ **What help do you need?**

In some cases there is no time to send all the above information – for example if an ambush has just begun. In this case send whatever information you can – there may only be time to shout “Ambush!” into the radio before you take evasive action. Even this is useful, and may allow your colleagues to avoid running into the same ambush, while taking steps to bring help to you.

A follow-up incident report follows the same format as the immediate report, updating information as required, as soon as the situation allows.

A full incident report gives a complete account of the incident, and may follow a format of this kind:

- ▲ Full chronological account of the incident
- ▲ Who was involved

- ▲ Reasons for any decisions taken
- ▲ Lessons to learn from the incident
- ▲ Identification of any failure of procedures or staff, and recommendations for any remedial or disciplinary action
- ▲ Date, author, role of author (involved in the incident or not?) and signature. These are important: unfortunately the date and author's name are often omitted by report-writers, which causes problems if there are any queries concerning the incident.

A 'near miss' incident in some cases will not require an immediate or follow-up incident report, but should always result in a full incident report so that lessons can be learned.

SECURITY MANUALS

A30

The aim of a security manual is to provide staff with an easy-to-use reference document, covering all common security advice, procedures and rules.

A security manual is no substitute for training (teaching and practising staff in a skill until they can do it themselves); briefing (providing up-to-date information on a particular situation) or equipping. But it does form part of the essential equipment of well-managed humanitarian personnel.

Organisations wishing to produce their own security manuals may wish to use existing security manuals for inspiration. In addition to this Generic Security Guide, the following documents are available in the public domain:

Operational Security Management in Violent Environments by Koenraad Van Brabant published by the Overseas Development Institute (ODI) Humanitarian Practice Network as Good Practice Review No. 8. Available as free download from www.odihpn.org.

Safety First: a field security handbook for NGO staff by Shaun Bickley, revised version published 2003 by Save the Children UK. Available from www.plymbridge.com.

Staying Alive, safety and security guidelines for humanitarian volunteers in conflict areas, by David Lloyd Roberts, published 1999 by ICRC. Available from www.icrc.org.

Landmines and Unexploded Ordnance, a resource book, 1999, Rae McGrath, Pluto Press. Available from www.plutobooks.com.

SECURITY PLAN

A31

The aim of a security plan is to provide staff with a concise document which sets out the security rules and procedures applying to the location(s) where they are working. **It must be short** (many experienced field managers say it should be less than 10 pages), otherwise it is likely that some staff will not read it.

It is vital that your security plan is tailored to your particular circumstances, taking into account the local situation, the characteristics of your staff, and the results of your security assessment. There is no single format which will fit all situations. The security plan should be updated whenever necessary, for example when your assessment of the security situation changes.

That said, many security plans contain some common features. The following suggested format contains some of these, and is offered as a memory-prompt to assist with writing a security plan. It should be adapted and added to as required by the circumstances. It could be dangerous simply to copy this format without adaptation, since it may not meet all the needs of a particular situation.

Possible Format of a Security Plan

Name of organisation: [enter name]

Distribution: All staff

Introduction

Example of some text you might use:

“The aim of this security plan is to inform all staff of the location-specific security rules and procedures that apply to [name of the area]. It does not repeat generic security rules or procedures that are common to most operations in insecure locations. For those, please refer to [the organisation’s security manual or equivalent].

Every member of the team has a responsibility to promote security, and is required to follow all rules and procedures contained in this security plan. Failure to do so could endanger life, and is a disciplinary

offence. The security plan is designed to help keep you and your colleagues safe, and to enable our work to run smoothly.

The person overall in charge of security is [name]. Other staff with security-related responsibilities are [give their names].

The security plan will be updated as often as necessary. All staff are encouraged to contribute updates as the need arises through the person named above. This version was written/updated by [name] on [date]: all previous versions should be destroyed.

Please read this plan immediately and keep it with you at all times. If you have any questions about it, or suggestions for improving it, please inform your manager or the team leader as soon as possible.

You should have a copy of [the organisation’s generic security manual or equivalent]. You should also be familiar with the organisation’s security policy – ask your manager for a copy.”

In an emergency

Name the person or organisation to call in an emergency, together with their full contact details. Explain what to do if no communications are working or available.

The security situation

Short description of the local situation, identifying:

- ▲ The authorities, and other main groupings
- ▲ Significant historical and recent events
- ▲ The threats you assess to exist against humanitarian organisations and their staff. Ensure that you include any specific threats to national staff, or to women, or to other individuals or groups.

[Note: this should only be a summary – perhaps 3 or 4 paragraphs. Much fuller briefing on the local situation should be given to all staff before arrival, and on arrival, and updated regularly. But it would be a mistake to include a long analysis in the security plan, since the situation changes rapidly; the analysis could cause problems if read by local authorities;

SECURITY PLAN

A31

and it would make the security plan too long for many staff to read.]

Security rules

List here the security-related rules and procedures that apply to this area ("location-specific" rules and procedures). Do not include generic security rules and procedures that apply to almost all insecure areas, as these will make the security plan too long. Instead, make specific reference to the organisation's security manual, stating that it should be read, understood and followed by all staff.

Examples of location-specific rules and procedures may vary between international and national staff (if so, this should be made explicit). They might include:

- ▲ Behaviour: are there certain behaviours to adopt, or avoid, because of local culture?
- ▲ Law and custom: what local laws and customs should staff be aware of?
- ▲ Dress: are there some forms of dress that should be avoided, or adhered to, because of cultural or other issues? For example, are shorts unacceptable? Should any khaki or green items of clothing be avoided, to prevent them being mistaken for military uniform? Etc.
- ▲ Equipment: is there any equipment that staff should keep with them, or have available? E.g. torch/flashlight; first aid kit; passport or other papers; a quantity of money for emergencies, etc.
- ▲ Medical precautions: any location-specific medical precautions
- ▲ Locations: are there any places which are out of bounds, either at all times or at certain times (such as night-time, or religious festivals, etc)?
- ▲ Communications: Not a guide to radio use (which should be in the security manual) but procedures specific to this location – e.g. whether staff are expected to be reachable by radio or mobile phone at all times; times of radio checks; radio channels that must be monitored; which communication means to use in an emergency.
- ▲ Travel: what are the location-specific procedures to follow when travelling? For example, are staff required to get permission from their

manager, and/or from local authorities, before travelling? On the day of travel, whom should they inform, when, and how? Is any means of travel prohibited for security reasons? May staff travel alone? Locations of checkpoints, and how to handle them? How should they call for help if in trouble? What to do in the event of a vehicle accident? Etc.

- ▲ Night: any location-specific procedures for night-time
- ▲ Curfew: is a curfew in place? If so, what are the details?
- ▲ Shelter: all staff should be familiar with the shelter in each building, to be used in case of attack
- ▲ Reaction to threats: if some types of threat are assessed as particularly likely, give the correct reaction procedures for these. In this case it may be helpful to repeat, in brief summary, a section of the security manual, and/or to refer explicitly to the relevant section.

Medical facilities

List here the medical facilities available, with full contact details and directions of how to find them. Include any necessary warnings about the shortcomings of those facilities.

Medical evacuation (Medevac)

Give the procedure for a medical evacuation. For example, are all staff entitled to medical evacuation, or only some? Who authorises it and how? What are the contact details for calling in the medical evacuation company (if you have one)?

Evacuation for security reasons

Explain the procedure for evacuation, should it become necessary for security reasons. Keep the procedure clear and concise. It might include:

- ▲ Who authorises an evacuation
- ▲ Assembly points
- ▲ Equipment to carry when evacuating
- ▲ Limits on amount of baggage when evacuating
- ▲ Likely evacuation routes
- ▲ Procedures when moving during an evacuation
- ▲ Communications procedures during an evacuation

SECURITY PLAN

A31

- ▲ Arrangements for national staff
- ▲ Responsibilities of those remaining behind:
 - Interim team leader
 - Logistics and property
 - Administration and finance
 - All the above are likely to need written authorisations
- ▲ Other alternatives, e.g. reduction in staff or hibernation

If for good reason the evacuation plan is lengthy, consider attaching it to the security plan as an annex. (See Annex 10 for suggested evacuation procedure.)

Annexes to security plan

A. Contact list

Give here the full addresses, callsigns, frequencies and phone numbers of:

- ▲ All offices, accommodation and other buildings used by the organisation
- ▲ Police or other local security forces
- ▲ Relevant civil authorities
- ▲ Relevant military authorities, if appropriate

B. Attach a map, with relevant locations marked

(Note: The information in these attachments may be updated more often than the security plan – so is easier to attach them as annexes, and replace them when necessary, rather than to incorporate them into the main body of the security plan.)

SECURITY POLICY

A32

A security policy is the top-level document which describes the overall security policy of an organisation. It forms part of the hierarchy of key security documents, as follows:

- ▲ **Security policy** – giving overall policy for the organisation
- ▲ **Security manual** – giving generic procedures for the organisation
- ▲ **Security plan** – giving detailed procedures for a specific location

In the interests of clarity, there should be as little overlap as possible between these three types of document.

A security policy should be tailored to the needs of the organisation. A suggested list of topics to cover is as follows:

- ▲ Principles
- ▲ The primacy of life over assets
- ▲ Approach and framework for security management
- ▲ Attitude to security risk – how much is acceptable?
- ▲ Assessment of the threats against the organisation, at a global level
 - Who should assess this, how often?
 - How should this be communicated around the organisation?
- ▲ Roles and responsibilities of relevant managers for security matters. For example:
 - The Chief Executive is overall responsible for security, as for the whole organisation. He or she delegates day-to-day security management to line managers at every level.
 - The Security Advisor (if there is one) is not responsible for managing security but for providing security advice and support to line managers and staff, as requested. He or she also monitors the effectiveness of security management throughout the organisation and regularly reports this to the Board.
 - Line managers at every level are responsible for the security of themselves and their staff
- ▲ All staff have a responsibility to ensure their own security and promote the security of colleagues

- ▲ The organisation's security responsibilities to staff
 - International
 - Regional
 - National
 - ... making it clear that the organisation aims for the same standard of safety for all staff since they are of equal value
- ▲ Minimum requirements before deployment in a new geographical location (e.g. threat assessment, risk/benefits assessment, competence of the agency to fulfil operational demands and manage risk, assessment of material resource and staffing requirements for responsible security management, etc)
- ▲ The organisation's security responsibilities to others when in the field:
 - Supporters
 - Volunteers
 - Consultants
 - Partners
- ▲ Required standards of preparation and precaution before travel to the field. This should be attached as an Annex to the policy, since it may need regular modification.
- ▲ The importance of nurturing a culture of security awareness and discipline throughout the organisation
- ▲ Requirements for monitoring the effectiveness of security management
- ▲ The organisation's policy (giving overall principles only) on:
 - Security plans
 - Kidnap and ransom
 - Weapons
 - Evacuation
 - Medical emergencies
 - Incident reporting and analysis
 - Serious or high-profile incidents (who is responsible for leading the crisis management team, and who else takes part in it?)
 - Collaboration on security with other NGOs and UN agencies
 - Contact with military forces, regular and irregular
 - Armed guards
 - Private security companies
 - Evacuation

SECURITY POLICY

A32

- Security training, equipping and briefing of staff and managers
- (Some of these points are better placed in an Annex to the policy rather than in the main body)
- ▲ The organisation's approach to funding security measures, possibly including the role that it expects institutional donors to play
- ▲ Procedure for revising the security policy – how often, and by whom?

For further suggestions on the creation of a security policy, see People In Aid's "Policy Pot" on Safety and Security, May 2003 ³³.

³³ Downloadable via the www.peopleinaid.org home page.

SHELTERS

A33

The purpose of a shelter is to protect staff in the event of an attack on the building, or if there is fighting or disorder nearby.

Shelter design should depend on the local circumstances, and the nature of the possible threats. For example, if there is a significant possibility of stray mortar or artillery shells landing in the vicinity, the shelter should be protected against blast and shrapnel. If artillery and mortars are not a threat, then this kind of protection is unnecessary.

If there is no significant threat of direct attack, and if the threat of local fighting or disorder is low, the designated shelter may simply be an inner room or corridor. It should either have no windows or the windows should be blocked off by an effective protection against stray bullets, such as sandbags.

Points to bear in mind when designing a shelter may include:

- ▲ The impact of any obvious shelter construction on agency image, and the messages it may give to onlookers. For example, sandbags on the inside of a building have a lower profile than on the outside.
- ▲ No direct line of sight to windows
- ▲ Thick walls, able to stop a stray bullet (or blast and shrapnel, if they are assessed to be a significant threat). An alternative may be to have more than one wall between you and the outside – if the walls are thick enough. Take specialist advice on the necessary thickness, if you are unsure.
- ▲ Suitable roofing, taking into account the assessed threats. For example, a threat of shelling, blast and shrapnel will require a different standard of roofing from a threat of falling spent bullets
- ▲ Lockable doors, either to the shelter or to the outside doors of the building in which the shelter is located
- ▲ Two exits
- ▲ Stock of water and food (to last 15 days or whatever period is assessed as more appropriate)
- ▲ Toilet facilities (improvised toilet facilities if no toilet is within the shelter)

- ▲ Power supply
- ▲ Fuel stock
- ▲ Lighting, including torches/flashlights and spare batteries, candles and matches
- ▲ Warm clothing
- ▲ Sleeping mats/mattresses and sleeping bags
- ▲ Communications equipment, battery chargers and spare batteries
- ▲ Maps
- ▲ Notebooks and pens

For more detailed advice on constructing a shelter, see the ICRC booklet “Staying Alive”³⁴.

³⁴ Author: D. Lloyd Roberts, published 1999. Available from ICRC Publications Division via icrc.gva@icrc.org.

SITREP FORMAT

A34

It is helpful to staff and to managers if there is an agreed format for routine situation reports (sitreps). An agreed format frees staff from the responsibility of creating a new format. It also helps managers and HQ to find the information they need, easily and quickly.

Non-routine sitreps, such as an emergency sitrep on a new crisis, may adapt the format of the routine sitrep if appropriate – or use a different format.

The format for a routine sitrep will vary according to each organisation's needs. A framework commonly used contains the following sequence:

- ▲ **Local situation**, including any changes in the situation of:
 - Local population (divided into groups if necessary)
 - Politics
 - Local authorities
 - Security, including actions of armed groups
 - Local economy
 - Humanitarian needs
 - Action by humanitarian organisations

- ▲ **The organisation's own programme**, listing for each project:
 - Action taken in the reporting period*
 - How that action compares with the action that was planned
 - Successes
 - Problems

- ▲ **Administration**, including:
 - Personnel
 - Finance
 - Logistics

- ▲ **Action requested**
 - From local manager
 - From HQ
 - From other parties

* The "reporting period" is the period to which the sitrep relates. For example, a weekly sitrep may be dated 24 March, covering the period 16 to 23 March. The reporting period is therefore 16 to 23 March.

STRESS

A35

Stress is a risk to health, and to security. Managers and staff should aim to prevent stress, and should be alert for signs of it among their team. It affects different people, and people from different cultures, in widely varying ways. The points below are suggestions only, and should be selected and adapted according to the situation and culture.

Causes of stress

The causes of stress may include many things, such as:

- ▲ Personal loss
- ▲ Overwork, or high-pressure work environment
- ▲ Conflicting job demands
- ▲ Multiple supervisors
- ▲ Lack of clarity about responsibilities or expectations
- ▲ Job insecurity
- ▲ Trauma
- ▲ Mission failure
- ▲ Feeling overwhelmed by the scale of need around
- ▲ Human error
- ▲ Misunderstanding
- ▲ Illness
- ▲ Inter-personal difficulties
- ▲ Antagonism from authorities or local people

Prevention of stress

Stress can often be prevented by taking a few simple precautions, including:

- ▲ Realistic work plans and working hours
- ▲ Clear briefing
- ▲ Efficient, caring management
- ▲ Listening regularly to staff, particularly when they are under pressure
- ▲ Keeping staff fully informed
- ▲ Encouraging staff and praising them for good work
- ▲ Rapid resolution of any grievances or complaints
- ▲ Sufficient rest, including a weekly day off in all but the most acute emergencies, and enforced Rest and Recreation (R&R – see Annex 25) in periods of high pressure
- ▲ Enabling staff to see their families and/or phone home
- ▲ Efficient mail service, and private access to personal e-mail, where possible

- ▲ Privacy in living accommodation
- ▲ Little luxuries, such as books, magazines, videos, good quality soap
- ▲ Eating properly, with a variety of menus
- ▲ Building team spirit
- ▲ Friendships
- ▲ Exercise
- ▲ Recognition, praise and reward for good work
- ▲ Adequate pay
- ▲ Secure home environment

Signs of stress

Managers and staff should look out for signs of stress in themselves and among their colleagues. Common signs include:

- ▲ Uncharacteristic or erratic behaviour
- ▲ Talking much more or much less than normal
- ▲ Irritable moods or short-tempered outbursts
- ▲ Headaches
- ▲ Depression or anxiety
- ▲ Apathy
- ▲ Unexplained aches and pains
- ▲ Skin problems
- ▲ Overwork
- ▲ Disregard for security, risky behaviour
- ▲ Indecisiveness, inconsistency
- ▲ Reduced efficiency at work
- ▲ Inability to concentrate
- ▲ Frequent absence from work
- ▲ Recurrent minor illnesses
- ▲ Disillusionment with work
- ▲ Disrupted sleep or oversleeping
- ▲ Over- or under-eating
- ▲ Overuse of alcohol or use of drugs

Treating stress

A doctor or trained person will advise on treating stress. Debriefing should be done by a trained person if possible. In the absence of a trained person, the following tips are often found helpful, but the appropriate action may vary widely according to the individual and the culture:

- ▲ Take time to talk with the person suffering stress. Encourage them to express how they are feeling. Reassure and encourage them. Allay or deal with any worries they may have. Find

STRESS

A35

out if they would benefit from any changes to work practices. Do they need more help with their tasks? Are there other pressures on them, for example bad news from home?

- ▲ Enable the person suffering stress to take time out from high-pressure work, but not to stop work completely. Suggest useful tasks that they can do, which are not stressful. This can help them to feel useful and valued, and can be part of the treatment process.
- ▲ Ensure they have access to recreational or religious facilities, and counselling if desired.
- ▲ Encourage them to look after themselves: eating well, taking exercise, frequent rest, etc
- ▲ Keep talking with them regularly – or ensure that a sympathetic colleague does so.
- ▲ After a short while, depending on the circumstances, it is often possible for them to resume their normal work. Indeed returning to work, after a sensible pause and without overloading them, can help recovery.
- ▲ Continue to monitor them and to listen to how they are getting on.
- ▲ If they do not respond, or if they are not able to return to work, seek medical advice.

Traumatic stress

Any event which is very distressing and outside the realm of normal human experience can result in traumatic stress. Traumatic stress usually produces a very intense response, including fear and/or helplessness, which may overwhelm the individual's coping mechanisms. Such a response is a normal reaction to an abnormal situation. It does not necessarily indicate that the person has developed a psychiatric disorder. Nonetheless, such exposure can lead to the development of post-traumatic stress disorder.

Traumatic stress is brought on by exposure to emotionally powerful events or "critical incidents". The event may be sudden and unexpected or ongoing in nature.

Some staff may experience 'vicarious' or indirect trauma through witnessing trauma or violence, or being associated with a tragic event such as acute disaster recovery efforts. Others may experience 'compassion fatigue' as a result of exposure to

human suffering or tragic situations that are more chronic and long-term. In many cases, the symptoms of vicarious trauma or compassion fatigue resemble those of victims experiencing direct trauma. Individuals with a prior history of significant trauma, instability in current life circumstances, or other vulnerabilities may be at highest risk.

Regardless of the source, traumatic stress may be one of the more serious occupation hazards experienced by staff, both in the field and in HQ. Dealing with traumatic stress is a specialist area and requires professional attention.

Burnout

'Burnout' is often used to describe a person who has become exhausted. Some signs of burnout are similar to the signs of stress, though are likely to be more severe. Signs of burnout within a team may include high turnover of staff; lack of team unity; a culture of blame; an unwillingness to take the initiative; increased sick leave; and decreasing effectiveness. Managers should watch out for these signs, and take action accordingly. Best of all, they should put in place working practices which prevent stress and burnout from occurring.

For further information see *Managing the Stress of Humanitarian Emergencies*, a UNHCR guide, by Sheila Platt³⁹. Also see *Humanitarian Action and Armed Conflict: Coping with Stress*, by Barthold Bierens de Haan, published by the ICRC⁴⁰. The Finnish Red Cross has also published *Security, Health and Stress in the Field*, by Hamberg-Dardel and Quick⁴¹.

³⁹ Published 2001. Available at www.the-ecentre.net/resources/e_library/index.cfm or by using a search engine.

⁴⁰ Published 2001 (3rd edition). Available from www.icrc.org.

⁴¹ Available at www.odihpn.org.uk.

SYLLABUS FOR A BASIC SECURITY TRAINING COURSE

A36

Organisations should assess the specific security training needs of their staff, and ensure that the training syllabus is designed to meet those needs. The following syllabus lists a number of topics that are likely to be required in most basic security training courses. The list is not exhaustive.

Introductory topics

- ▲ Humanitarian principles
- ▲ Basic outline of the humanitarian system
- ▲ Red Cross/NGOs Code of Conduct
- ▲ Cultural and context awareness
- ▲ Dress and behaviour
- ▲ Personal equipment

The organisation

- ▲ Mission
- ▲ Mandate
- ▲ History
- ▲ Values

Security-specific topics

- ▲ Assessing risks
- ▲ Precautions at home and office
- ▲ Precautions when travelling
- ▲ Map reading
- ▲ Armed checkpoints
- ▲ Reacting to security incidents
- ▲ Evacuation
- ▲ Dealing with the military
- ▲ Dealing with rebel/irregular troops
- ▲ Basic tips on dealing with the media

Communications

- ▲ Radio handling
- ▲ Handling satellite phone, fax, e-mail
- ▲ Reporting

Vehicles

- ▲ Driving a 4-wheel drive vehicle
- ▲ Tips for safe driving
- ▲ Equipment that every vehicle should carry
- ▲ Basic vehicle checks and procedures

Medical

- ▲ Health and hygiene in the field
- ▲ Handling stress, including in a team context

▲ Medical evacuation

For advice on designing and delivering a security training course, you may wish to contact a recognised security training organisation. A number of these are listed in the **Security Training Directory** which accompanies this Guide.

SYLLABUS FOR A SECURITY COURSE FOR FIELD MANAGERS

A37

Organisations should assess the specific security training needs of their field managers, and ensure that the training syllabus is designed to meet those needs. The following syllabus lists a number of topics that are likely to be required. The list is not exhaustive.

- ▲ Approaches to security: acceptance, protection, deterrence
- ▲ Security-related responsibilities of a field manager
 - Team leadership
 - People-management
 - Security assessments, including understanding the local context, influential actors and threats, assessing the implications of political and security developments
 - Analysing the risks and likely benefits of a programme
 - Writing a security plan
 - Giving a security briefing
 - Writing sitreps and incident reports
 - Security coordination with other agencies
 - Common security problems and dilemmas
 - Deciding on and managing an evacuation
 - Organising security training/workshops for staff
- ▲ Winning acceptance among staff, local leaders and people
- ▲ Dealing with senior civil leaders, police and/or military commanders
- ▲ Handling the media
- ▲ Serious incidents: kidnapping, assault, rape, murder etc
 - Securing buildings
 - Managing communications
- ▲ Security aspects of administration:
 - Human resources aspects of security management: recruitment, contracts, briefing, discipline, termination of contracts etc
 - Financial security
 - Security of property, inventory management etc
- ▲ Stress: prevention and treatment
- ▲ The UN Security Management System

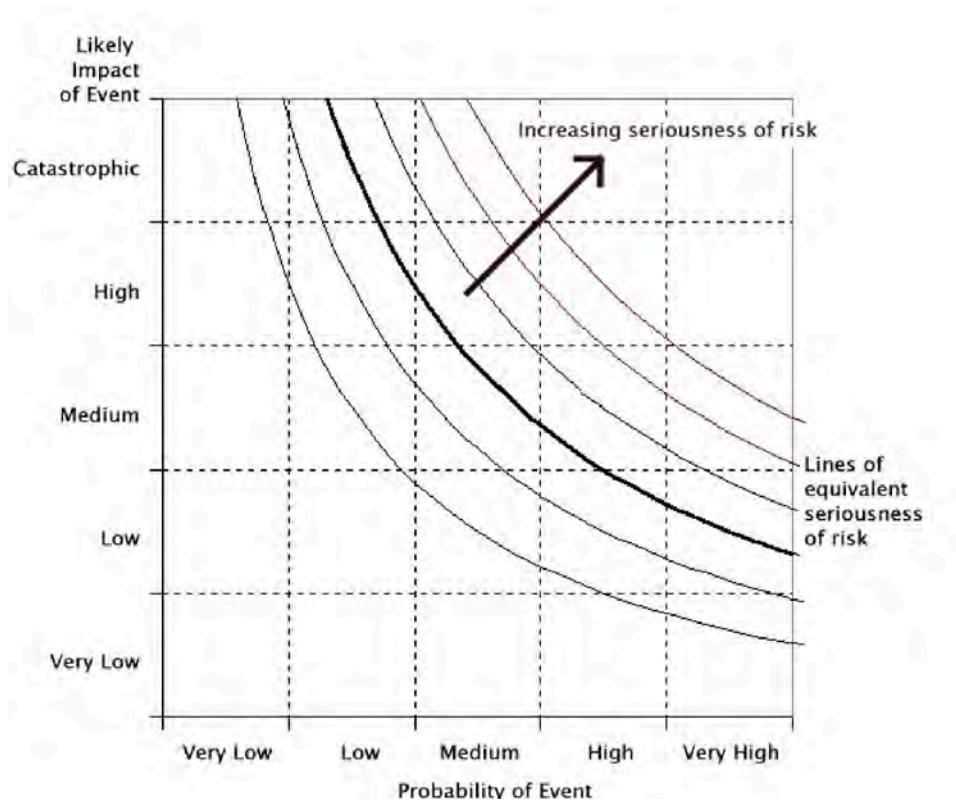
THREAT IMPACT CHART

A38

A helpful way of considering threats, their relative likelihood, and their impact if they occurred is to plot them on a chart⁴². List the threats you assess to be present, with the likelihood of each threat occurring, and the impact that it would have if it did occur, on a scale of 1 to 5. For example, murder would have very great impact, so should be rated as 5, though its likelihood may be rated as low – say, 1.

Threat Event	Probability (0-5)	Impact (0-5)

Now plot each threat as a point on the chart below. It gives you a picture of your assessed threats. Those nearer the top right corner should give most cause for concern.

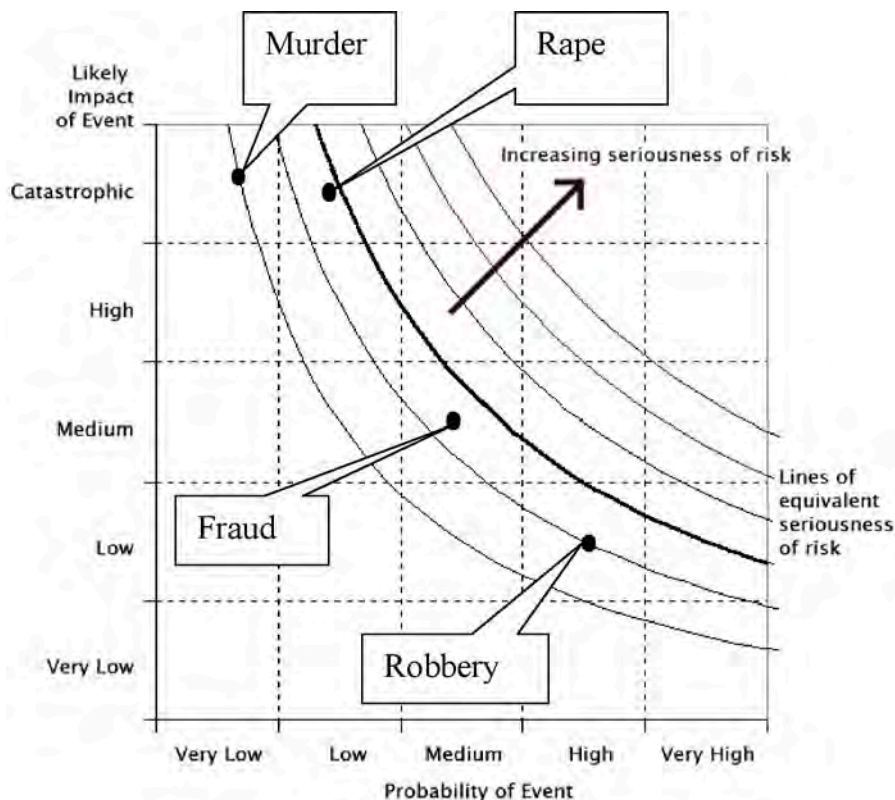


⁴² Adapted from RedR risk assessment training handout.

THREAT IMPACT CHART

A38

A few threats are marked on the following chart, to illustrate the method:



The curved lines represent thresholds of risk. The threshold of acceptable risk varies according to what you expect to achieve. To save life you would normally be prepared to take greater risks than if you were simply carrying out routine work. It is for you and the responsible manager to decide what level of risk is acceptable. If any threats lie beyond the threshold of acceptable risk, action is required either to remove the threat, or to remove staff from the threat.

TRAVEL AUTHORISATION FORMAT

A39

It can help efficiency and security to require staff to complete a simple travel authorisation form, before going on a journey. This helps to ensure that the trip is well planned, safely managed and that other relevant colleagues know any necessary details.

A travel authorisation form may need to be adapted to the local circumstances but often includes the following basic elements:

- ▲ Names of people planning to travel
- ▲ Purpose of the trip
- ▲ Destination
- ▲ Route
- ▲ Estimated time of departure
- ▲ Estimated time of arrival
- ▲ Any threats assessed to be relevant to the trip
- ▲ Communications arrangements including frequencies, callsigns, phone numbers and reporting times
- ▲ Signature of authorising manager

UN SECURITY PROCEDURES

A40

In many emergencies, UN agencies play a leading role in security management. Many NGOs cooperate with the UN on security matters, exchanging information and informing each other of security plans. It is therefore helpful for all humanitarian organisations to be aware of the UN security system.

Structure

The UN security system typically has the following components on the ground during an emergency:

- ▲ **Designated Official.** In each country the UN Secretary-General appoints a senior official, normally the UN Resident Coordinator, as the Designated Official for Security (DO). The DO is responsible for ensuring the safety and security of UN personnel within that country. He or she reports to the UN Secretary-General, through the UN Security Coordinator (UNSECOORD). The DO prepares a security plan for the country, and grants security clearance for UN staff and their dependants to enter the country if a UN security phase is in effect.
- ▲ **The Security Management Team (SMT)**, a committee chaired by the DO which usually includes the heads of the operational UN agencies, meets regularly to discuss security management, and advise the DO.
- ▲ **Area Coordinators.** In some larger countries, the DO and SMT may appoint Area Coordinators who coordinate security arrangements for a particular area which may be distant from the capital city. Such areas usually have their own Area SMT.
- ▲ **Security Officers.** There are likely to be:
 - One or more security officials, usually known as **Field Security Coordination Officers**, employed by UNSECOORD. They assist the DO, particularly by keeping staff and dependants informed on security matters, advising on security measures, and coordinating UN responses to crises.
 - One or more **Field Security Coordination Assistants**, locally recruited staff members who assist the Field Security Coordination Officers.
- UN agencies present on the ground may employ their own Field Security Officers, sometimes known as single-agency security officers. They advise and assist the country representative of their agency on security matters.
- ▲ **Communications networks.** In addition to its internal channels, a UN operational agency may make one or two radio channels available to all humanitarian organisations, to improve coordination and security.
- ▲ **Wardens**, who act as information conduits to UN staff on security matters, and ensure implementation of the UN security plan in their zone of responsibility
- ▲ **Minimum Operating Security Standards (MOSS).** These set out the minimum security measures which any UN agency must put in place in order to be allowed to work in a particular country. They include equipment, procedures and documentation. A country-specific MOSS is developed for each country, using the 'baseline MOSS' produced by UNSECOORD.

In the case of a UN peacekeeping or special mission, the Special Representative of the Secretary-General (SRSG), and/or the Force Commander or Chief of Staff, are responsible for the security of its military and civilian personnel.

At UN HQ in New York, UNSECOORD is responsible for all policy and procedural matters related to security, and ensuring that each UN field operation has adequate security measures in place. UNSECOORD, on behalf of the UN Secretary-General, decides whether relocation or evacuation is necessary in situations of insecurity, taking into account information and advice provided by UN staff in the field.

The HQ of each UN organisation appoints a security focal point at HQ, who manages security within that organisation and liaises with UNSECOORD and other agencies. On the ground, normally the head of each UN agency present is a member of the SMT.

UN SECURITY PROCEDURES

A40

UN security phases

The UN operates a system of five security phases, each denoting a different level of insecurity, and requiring different security measures:

Phase One: Precautionary

- ▲ Exercise caution
- ▲ All travel into the area requires advance clearance by the Designated Official (DO)

Phase Two: Restricted Movement

- ▲ Staff and families remain at home
- ▲ No travel into or within the country unless authorised by the DO

Phase Three: Relocation

- ▲ Internationally-recruited staff and their families are temporarily concentrated or relocated to specified sites/locations and/or
- ▲ Eligible dependants are relocated outside the country
- ▲ According to the local UN security plan and the decision of the DO/Country Director, locally recruited staff may:
 - Leave the duty station on special leave with pay, or
 - Be relocated to a safe area within the country with up to 20 days Daily Subsistence Allowance (DSA), and
 - Receive up to 3 months salary advance and, if needed, a grant to cover transport costs for themselves and eligible dependants

Phase Four: Programme suspension

- ▲ All internationally-recruited staff who are not directly concerned with emergency or humanitarian relief operations or security matters are relocated outside the country
- ▲ Locally-recruited staff: as for Phase Three

Phase Five: Evacuation

- ▲ This requires the approval of the UN Secretary-General
- ▲ All remaining internationally-recruited staff leave
- ▲ Locally-recruited staff: as for Phase Three

Security coordination with other organisations

Other humanitarian organisations often look to the UN Security System for security-related information and informal coordination. In many cases, the UN hosts a regular security coordination meeting to which other

humanitarian organisations are invited. Often, the UN makes available one or more radio channels to the wider humanitarian community, to allow all organisations to communicate easily on security matters or in case of urgent need.

A security briefing may also be given as part of the agenda of general humanitarian coordination meetings. This briefing is typically given either by a UN security official or by an officer of an international peacekeeping force, if present.

Annex 41 sets out a Menu of Options for security collaboration between the UN and NGOs, as agreed by the UN Inter Agency Standing Committee (IASC).

Inclusion of other organisations in UN security arrangements

In general, the UN is not responsible for the security of any other organisation. But in 1996 the UN published a directive⁴³ on the inclusion of international staff of intergovernmental organisations and NGOs (those who are implementing partners of the UN) in UN security arrangements. An implementing partner interested in the inclusion of its international staff in UN security arrangements at a particular duty station should submit its request to the UN Designated Official (DO) for security at that duty station.

If the DO agrees, he or she will prepare a draft Memorandum of Understanding between the UN and the implementing partner, using the model Memorandum of Understanding provided by UNSECOORD. The implementing partner must agree to share the cost of any security arrangements, including evacuation costs. It must also agree to:

- ▲ Consult with and assist the DO on all matters relating to security arrangements
- ▲ Fully follow the instructions of the DO regarding security matters
- ▲ Ensure that the DO is provided with updated lists of names and addresses of international staff
- ▲ Report all incidents with security implications to the DO
- ▲ Lend travel assistance to UN personnel, where possible
- ▲ And certain other requirements

⁴³ Security directive on inclusion of international staff of intergovernmental and nongovernmental organisations in United Nations security arrangements, UNSECOORD, 1996

UN-NGO SECURITY COLLABORATION: MENU OF OPTIONS⁴⁴

A41

At a UN Inter-Agency Standing Committee (IASC) taskforce on staff security in 2001, endorsed by the IASC Working Group in January 2002⁴⁵, the following was agreed. It is known as the “Menu of Options” for UN-NGO security collaboration.

Non-UN organizations are not bound by, nor participate formally in, Security Management Team (SMT) decisions on UN security policy. However, UN organizations and their IGO/NGO partners in specific humanitarian operations should agree on practical collaboration fitting the specific field situation. This would include choosing, according to the agency’s or organization’s mandate/mission and the scope of their operational involvement, the degree to which they would commit themselves to participate in the following:

Selecting IGO/NGO field security focal point(s): IGO/NGO partners to UN organizations select among themselves one or a limited number of field security focal points.

Convening broad-based fora for field security collaboration at regular intervals among all humanitarian actors at area, country and sub-office level in order to address practical security issues of common concern. These would normally include: the DO, Field Security Officer (FSO), Area Security Coordinator or other DO designee; members of the SMT as appropriate; NGO field security focal point(s); representatives of IGOs; representatives of the Red Cross Movement. The chairperson may be chosen on a rotating basis.

Including staff security concerns in Consolidated Appeals (CAPs): the CAP may include a project to cover the additional resources potentially required by enhanced collaboration on staff security by agencies and organizations represented in the taskforce such as telecommunication and training.

Meeting common, security-related needs: UN organizations and their IGO/NGO partners committed to security collaboration participate, to the extent feasible, in meeting the uncovered, security-related needs of the humanitarian community⁴⁶, including costs, according to the scope of their respective involvement.

Sharing resources: UN organizations and their

IGO/NGO partners cooperating in humanitarian field operations develop a local inventory for the sharing of their specialized, security-related human and material resources.

Facilitating inter-agency telecommunications among UN organizations and their IGO/NGO partners at field level by:

- ▲ The DO advocating with the relevant authorities for the use of telecommunication equipment within the framework of existing international agreements;
- ▲ The relevant UN body negotiating with the authorities a common frequency for security collaboration for UN organizations and their IGO/NGO partners operating in the same area;
- ▲ Humanitarian actors committed to security collaboration using standard communication procedures and, to the extent possible, providing staff with compatible communication systems.

Collaborating and consulting in security training: all UN organizations and their IGO/NGO partners (at HQ and at field level) carry out security training in collaboration and/or consultation with other agencies to the extent possible, and seek to increase their own capacity for security training at all levels.

Sharing information: security-related information is shared among UN organizations and their IGO/NGO partners while respecting the humanitarian character of the participants as well as the confidentiality required when dealing with sensitive information.

Identifying minimum security standards: UN organizations and their IGO/NGO partners jointly identify and agree how to apply minimum security standards adapted to local circumstances taking into consideration already existing standards including, for example, the UN MOSS that are binding for the members of the UN system.

Seeking adherence to common humanitarian ground-rules: the security collaboration of UN organizations and their IGO/NGO partners in specific field operations, to the extent possible, rest on respect for common, locally developed ground-rules for humanitarian action.

⁴⁴ This Annex was adapted from the WFP Emergency Field Operations Pocketbook, 2002, page 312.

⁴⁵ The task force included UNDP, UNHCR, UNICEF, UNSECOORD, WFP, OCHA, and IOM, as well as ICVA (International Council of Voluntary Agencies), InterAction (American Council for Voluntary International Action), SCHR (Steering Committee for Humanitarian Response) and, as invitees, the Red Cross Movement. Its summary report is entitled *UN/non-UN field security collaboration, Report of the consultant to the Inter-Agency Standing Committee Working Group Staff Security Task Force*, available on the internet at <http://www.humanitarianinfo.org/iasc/prodsec01.doc> or by using a search engine.

⁴⁶ “Humanitarian community” here refers to the totality of humanitarian actors in a given place addressing the same humanitarian concerns.

VEHICLE EQUIPMENT

A42

If properly maintained and equipped, vehicles are less likely to break down, and are more easy to recover if they do break down. It is good practice for a field operation to establish a standard equipment list for vehicles, appropriate to the local circumstances, and then to ensure that all vehicles have this equipment at all times.

This is a security issue, since a vehicle which breaks down in a dangerous area puts its occupants at risk.

The right equipment will vary, depending on the circumstances. Select from, add to or subtract from the following list:

- ▲ Two spare wheels (one is not sufficient in difficult or dangerous areas)
- ▲ Jerrycan of water (20 litres)
- ▲ Jerrycan of spare fuel (20 litres)
- ▲ Jack, wheel brace and any other tools for changing a wheel
- ▲ Tow-rope
- ▲ First aid kit (a large first aid kit (suitcase-size) may be necessary in some areas)
- ▲ Spare light bulbs
- ▲ Torch/flashlight and spare batteries
- ▲ Spare engine oil
- ▲ Snow chains
- ▲ Ice scraper
- ▲ Sand plates
- ▲ VHF radio
- ▲ HF radio
- ▲ Communications information: contact lists, frequencies etc
- ▲ Winch
- ▲ Front nudge bar
- ▲ Snorkel
- ▲ Fire extinguisher
- ▲ Locking wheel nuts
- ▲ Screwdriver
- ▲ Spare fuses
- ▲ Map
- ▲ Compass
- ▲ Warning triangle
- ▲ Identifying markings or flag
- ▲ Vehicle documents including:
 - Ownership documents
 - Authorisation documents

- Insurance certificate
- Vehicle logbook (for recording journeys made): to include columns for date, start location, time of departure, kilometre reading at departure, destination, time of arrival, kilometre reading at destination, purpose of trip, name of driver, signature

- ▲ Blankets
- ▲ Food (if travelling on long journeys, or if delays are possible)

Armoured vehicles are used by a few humanitarian organisations, in rare circumstances. Most humanitarian organisations take the view that if the security situation is such that armoured vehicles are necessary, then it is too dangerous to be working there at all. Note that armoured vehicles do not give protection against some weapons, including anti-tank mines, armour-piercing bullets, anti-tank grenades and missiles, and direct hits from shells. They are expensive, heavy and require special training to drive.

INDEX

To jump to the page number you want, use the 'Go To' function. Click on Document, then Go To, or hold down Ctrl and press N. (In later versions of Acrobat click on View, then Go To, or hold down Shift and Ctrl and press N).

In addition to the Index and the Table of Contents, you can search for words or phrases using the 'Find' feature in Acrobat. Click on Edit, then Find (in later versions, Search), or hold down Ctrl and press F.

A

Abbreviations	55
Acceptance approach to security	10
Accidents	35, 68, 96, 107
Accommodation	60
fire precautions	78
first aid kits	83
generators	99
guards	33
location and type	18
locking doors	29
R&R accommodation	100
Accounting	See Financial security
Advocacy for humanitarian space	49
Air attack	108
Air crash	108
Alarms	29, 60, 71, 72, 78, 80, 124, 126
Ambush	31, 62, 109, 116
Amnesty International	89
ANSO (Afghanistan NGO Security Office)	23, 26, 55
Archives	46, 49
Arrest	112
Assault	112
Assessment	See Security assessment
Audit	76

B

Bank	76
Behaviour of staff	28
Bioforce	53
Biological attack	114
Blast film	60, 113
Blood group	17, 19
Body armour	71
Bombs	60, 113, 114
Booby traps	123

Bribes	35, 65
Briefing	See Security Briefing
Buildings	18, 60

C

Cars	See Vehicles
Cash	17, 28, 74, 76, 98, 126
Casualties	49, 53, 107, 113, 119
Checkpoints	30, 62
Chemical attack	114
Civil-military relations	22, 23, 49, 64, 66, 82, 119
Clothing	See Dress
Code of Conduct	11, 13, 27, 29, 45, 50, 54, 139
Codes and Standards	50
Communications security	85, 97
Computer security	85
Contingency plans	26, 49
Contracts	15, 17
during evacuation	42, 73
ending contracts	45
standard contracts	15, 19
Convoys	64
Coordination on security	23, 26, 145
Copyright of this Guide	56
Corruption	35, 65
Crime	10, 28, 29, 35, 36, 107
Crisis management team	47, 49, 121, 133
Crowds	115
Cultural awareness	67

D

Death of staff member	40
Debriefing	
after an evacuation	43
after end of contract	96
after an incident	39, 120
after programme closure	46
Designated Official (DO) for Security (UN)	144
Detention	112
Deterrence approach to security	11
Directors of a humanitarian organisation	9
Discipline	29, 28, 30, 49
Donors	22, 25, 36, 37, 45, 54, 90
Dress	29, 30, 124, 131
Driving	68, 143
Drugs	29, 30, 124
Duress codes	99
Duty officer	32, 50

INDEX

E			
Earthquake	60, 115	vehicles	119
ECHO	2, 56	HIV/AIDS	83
Embassies	25, 42, 74	Hostages	See Kidnap
Emergency contact card	18, 34, 70	Hotels – security precautions	29, 78
Employment laws and disputes	15, 45	Human Resources management – security aspects	48
Equal opportunity	14	Human rights abuses	37, 89
Equipment		Human Rights Watch	89
general	16	Humanitarian Information Centres (HICs)	103
personal	71	Humanitarian space	13, 49
team	72	Hygiene	83
Evacuation	41, 73	I	
Evaluation	28, 45, 52	Identity badges	34
Explosions	116	Illiterate staff	17
F		Improvised Explosive Devices (IEDs)	113
Farewell events	46	Incidents	39, 107
Fatal incidents	40	high-profile incidents	48
Female staff	30, 67	incident analysis	39
Field-Headquarters relationship	26	incident reports	39
Fighting	115	near miss incidents	39, 128
Financial security	17, 33, 76, 117	serious incidents	40, 48
accounting records	17, 33, 49, 73, 117	Information	
need for accountant from outset	18, 33, 76	information gathering	20
Fire safety	33, 78	information security	33
First aid	28, 123	information sharing	21, 22, 26, 146
kits	19, 83	Insurance	17, 19, 32, 40, 48, 87
training	19	Integrated Regional Information Network (IRIN)	103
Flak jacket	See Body armour	InterAction Field Cooperation Protocol	51
Flood	117	Inter-Agency Standing Committee (IASC)	50, 146
Framework Partnership Agreement (ECHO)	36	International Committee of the Red Cross (ICRC)	37, 88
Fraud	117	International Crisis Group	103
G		International Humanitarian Law	49, 88
Generators	61, 72, 99, 117	International military forces	23
Get-you-in team	35	International police	24
Grenade	118	Inventory control	17, 90
Guards	33, 80	J	
Guns	See Weapons	Job descriptions	14
H		K	
Handbook	See Manual	Keys	34
Handover	46	Kidnap	49, 112, 120, 133
Headquarters aspects of security	47	L	
Health	See Medical	Legal aspects of employment	15, 45
Hibernation	41	Legal aspects of programme closure	45
Hijack		Legal protection of aid workers	37
aircraft	120	Legal risks	9, 48

INDEX

Local authorities	20, 26, 41, 44, 137	Next of Kin	
Local NGOs	25	informing Next of Kin	40, 94, 112
Local partners	25	Next of Kin records	17, 93
Local population	10, 14, 21, 42, 49, 65, 75	O	
Local security forces	22	Offices	18, 53, 60
Locks	34	P	
Looting	74, 122	Partners	25, 37
M		People In Aid Code	51, 96
Managers	8, 7, 47	Personnel records	17
senior managers	8, 16, 20, 46, 47, 48, 108	Phonetic alphabet	98
training	52, 140	Plan	See Security plan
Manual (financial manual)	77	Police	
Manual (security manual)	8, 9, 11, 12, 47, 129	international	24
Mass casualties	49, 53	local	22, 26, 39, 60, 64, 65, 82
Media	36, 91	Policy	See Security policy
after a security incident	39	Post-traumatic stress disorder	39
during programme closure	46	Preparation for the field	12
during suspension, evacuation, etc	43	Private security companies	26, 33, 80
Medical		Procurement	34, 65
emergency	40, 92	Programme design – security aspects	14, 27
evacuation (Medevac)	40, 70, 92, 123, 131	Property – disposing of	45
health and hygiene	19, 83	Protection approach to security	10
preparation	19	R	
Memorandum of Understanding (UN)	43, 145	Radio procedures	85, 97
Menu of Options for UN-NGO Security		Radiological attack	114
Collaboration	50, 145, 146	Ransom	49, 112, 120, 133
Military assets	24	Rape	10, 29, 124
Military forces		Recruitment	14, 17, 80, 102
international	23	RedR	53
local	22	Refoulement	88
Mine Risk Education (MRE)	123	ReliefWeb	103
Mines	88, 123	Relocation	41, 73
Minimum Operating Security Standards (UN)	144, 146	Reporting	27, 37, 39, 128, 136
Mugging	See Robbery	Rest and Recreation (R&R)	30, 100
N		Risk	7, 11
National staff	6, 75, 105	Robbery	80, 126
evacuation	42, 73, 74, 85	S	
information-gathering	20	Safe	60, 72, 76
insurance	87	Satellite phones	31, 85
recruitment	14, 102	Security – definition	10
security plan	130	Security advisor	8, 23, 26, 48, 133
stress	65	Security assessment	12, 20, 44, 101
threats to national staff	130	Security briefing	8, 16, 105
Near miss incidents	39, 128	Security coordination	26, 23, 144, 145
Negotiation	10, 13, 64, 121		

INDEX

- | | | | |
|--|---------------------------------|--|--|
| Security forces | | | |
| international | | 23 | |
| local | | 22 | |
| Security incidents | See Incidents | | |
| Security Management Team (UN) | | 144, 146 | |
| Security manual | | 8, 9, 11, 12, 47, 129 | |
| Security phases (UN) | | 145 | |
| Security plan | | 11, 12, 20, 47, 130 | |
| Security policy | | 11, 47, 133 | |
| Security Training Directory | | 6, 9, 16, 53, 139 | |
| Sensitive documents | | 17, 46, 62, 73 | |
| Sensitive information | | 32-4, 51, 85, 86, 99, 146 | |
| Sexual harassment | | 126 | |
| Sexual violence | | 124 | |
| Shelters | | 60, 108, 116, 131, 135 | |
| Shooting | | 115 | |
| Sitreps | | 27, 136 | |
| Software | | 19, 31, 56 | |
| Sphere project | | 51 | |
| Staff | | | |
| ending contracts | | 45 | |
| female staff | | 30, 67 | |
| illiterate staff | | 17 | |
| importance of quality staff | | 14, 48 | |
| national staff | See National staff | | |
| relocation or reduction | | 42 | |
| staff behaviour | | 28 | |
| training | See Training | | |
| use of experienced staff | | 53 | |
| Standard contracts | | 15, 19 | |
| Standard documents | | 19 | |
| Standard Operating Procedures (SOPs) | | 47 | |
| Standards and Codes | | 50 | |
| Stress | | 16, 30, 39, 100, 137, 139, 140 | |
| Suspension of a programme | | 41 | |
| Syllabus | | | |
| for field managers | | 140 | |
| for field staff | | 15, 139 | |
| T | | | |
| Teamwork | | 28 | |
| Telecommunications | | 17, 29, 31, 85, 97, 139, 140, 144, 146 | |
| Terrorism | | 101, 127 | |
| Theft | | 10, 11, 17, 29, 33, 40, 62, 76, 80, 90, 115, 117 | |
| Threat | | 7, 10, 37, 130, 133, 141 | |
| assessing threats | | 39, 101 | |
| bomb threats | | 114 | |
| bribes and threats | | 35 | |
| briefing on threats | | 105 | |
| resulting from evacuation | | 42 | |
| threats caused by rumours | | 91 | |
| threats from military forces | | 86 | |
| threats to female staff | | 30 | |
| threats to visitors | | 8 | |
| training | | 15, 52, 140 | |
| Threat impact chart | | 141 | |
| Training | | 7, 8, 15, 48, 52 | |
| administration of | | 18 | |
| directory | See Security Training Directory | | |
| fire safety | | 78 | |
| first aid | | 83 | |
| for field managers | | 140 | |
| for field staff | | 15, 139 | |
| for HQ managers | | 52 | |
| funding within the UN | | 146 | |
| guards | | 80 | |
| insurance requirements | | 87 | |
| sharing training | | 26 | |
| trainers | | 53 | |
| training policy | | 47 | |
| UN/IGO/NGO collaboration | | 146 | |
| Travel | | 35 | |
| authorisation format | | 143 | |
| decision to travel | | 79, 109, 119 | |
| procedures | | 131, 145 | |
| varying route and time | | 76 | |
| U | | | |
| Unexploded ordnance (UXO) | | 123 | |
| United Nations | | | |
| Consolidated Appeals (CAPs) | | 146 | |
| Designated Official (DO) for Security | | 144 | |
| Humanitarian Information Centres (HICs) | | 103 | |
| Integrated Regional Information Network (IRIN) | | 103 | |
| Inter-Agency Standing Committee (IASC) | | 50, 146 | |
| Memorandum of Understanding | | 43, 145 | |
| Menu of Options | | 50, 145, 146 | |
| Minimum Operating Security Standards | | 144, 146 | |
| role in evacuation | | 43 | |
| Security Coordinator (UNSECOORD) | | 50, 144, 145 | |
| Security Management Team | | 144, 146 | |
| security phases | | 145 | |
| security procedures | | 144 | |
| security system | | 23, 50, 144, 146 | |
| United Nations High Commissioner for Human Rights (UNHCHR) | | 89 | |

INDEX

V	
Vehicles	32
armoured vehicles	33, 109, 119, 147
vehicle equipment	147
vehicle hijack	119
Visibility	36
Visitors	
access	29, 34
emergency contact card	34, 70
instructions for guards	80
threats to	8
waiting area	61
Vulnerability	11
W	
War crimes	
records	37
reporting	37, 89
War risks insurance	87
Wardens	73, 117, 144
Warehouses	18, 60
Weapon finds	127
Weapons	11, 31, 32, 82, 88, 113, 133
Whistle-blowing	65
Women	See Female staff



EUROPEAN COMMISSION



Humanitarian Aid

<http://ec.europa.eu/echo>

Prepared by
THE EVALUATION PARTNERSHIP
www.evaluationpartnership.com



Design: Onefiveseven. 157@mistral.co.uk