



# **Risk & Security Guidelines for UK Links**

Written by Lucy Hodgson  
November 2008  
Copyright © 2009 THET

# Contents Page

*(Tables and Forms are listed in italics)*

<b>FOREWORD</b> .....	<b>4</b>
<b>I. INTRODUCTION</b> .....	<b>5</b>
AIM OF THESE GUIDELINES .....	5
<b>1. RISK</b> .....	<b>7</b>
WHAT IS RISK? .....	7
<b>2. RISK ASSESSMENT</b> .....	<b>8</b>
HOW TO ASSESS RISK .....	8
<i>RESPONSIBILITIES for risk assessment</i> .....	9
<i>Acceptable Threshold of Risk</i> .....	11
5 STEP RISK ASSESSMENT.....	11
<i>5 Steps to conducting a risk assessment, worked example</i> .....	12
VULNERABILITY ANALYSIS .....	12
<b>3. CONTEXTUAL ASSESSMENT</b> .....	<b>13</b>
<i>Relations with the local population</i> .....	14
<i>Relations with other organisations</i> .....	15
TRAVEL PREPARATIONS .....	15
BRIEFING.....	15
BASIC TRAVEL PREPARATION .....	15
<b>4. PROFESSIONAL, INSURANCE &amp; LEGAL ISSUES</b> .....	<b>16</b>
INSURANCE .....	16
TRAVEL INSURANCE .....	16
KIDNAP & HOSTAGE INSURANCE.....	17
PROFESSIONAL LIABILITY & INDEMNITY: .....	17
PENSIONS .....	18
<b>5. SECURITY PLANNING</b> .....	<b>19</b>
<b>6. INCIDENT REPORTING</b> .....	<b>19</b>
PREVENTION .....	19
REACTION .....	19
REPORTING INCIDENTS.....	19
'NEAR MISS' INCIDENTS .....	20
ANALYSIS OF INCIDENTS AND ADJUSTMENT OF PROCEDURES.....	21
<b>7. CULTURAL DIFFERENCES</b> .....	<b>21</b>
<i>Cultural Sensitivity</i> .....	21
<b>8. RELATIONS WITH PARTNERS/HOST ORGANISATIONS</b> .....	<b>22</b>
<i>Host Organisation rules &amp; regulations</i> .....	22
<b>9. PERSONAL CONDUCT</b> .....	<b>22</b>
<b>10. HEALTH AND HYGIENE</b> .....	<b>23</b>
<b>11. STRESS</b> .....	<b>24</b>
WHAT IS STRESS .....	24
<i>Types of stress</i> .....	24
TREATING STRESS .....	24

<b>12. SPECIFIC THREATS.....</b>	<b>25</b>
TRAVEL & TRANSPORT.....	25
CRIME (THEFT, ROBBERY, BURGLARY, ASSAULT, ETC).....	25
<i>Confronted with acts of crime</i> .....	26
HARASSMENT & SEXUAL VIOLENCE .....	26
SEXUAL VIOLENCE.....	27
<i>Mitigation Measures</i> .....	27
<i>In case of an Incident</i> .....	27
<i>Post Incident Measures</i> .....	28
HOSTILITY (CROWDS, MOB VIOLENCE, LOOTING, DEMOS).....	28
ARREST & DETENTION .....	29
<i>Detention</i> .....	29
<i>Arrest</i> .....	29
<i>How to avoid Arrest and Detention</i> .....	29
<i>If Arrested/Detained</i> .....	30
DANGER OF MINES, UNEXPLODED (IMPROVISED) ORDNANCE AND BOOBY-TRAPS.....	30
<b>13. RESOURCES.....</b>	<b>30</b>
<b>14. ANNEXES: TEMPLATES, FORMS AND CHECKLISTS.....</b>	<b>31</b>
RISK ASSESSMENT .....	31
<i>Risk Assessment Template</i> .....	32
RISK ASSESSMENT CHECKLIST.....	33
TRAVEL BRIEFING CHECKLIST .....	34
<i>Security briefing</i> .....	34
<i>Orientation</i> .....	34
<i>Documentation &amp; Equipment</i> .....	34
PRE DEPARTURE TRAVEL CHECKLIST .....	35
SUGGESTED CONTENTS OF A PROJECT/COUNTRY SPECIFIC SECURITY PLAN .....	36
EMERGENCY PROCEDURES POST SECURITY INCIDENT .....	38
POST INCIDENT REPORTING FORM .....	39
<i>Incident List</i> .....	41
CULTURAL ISSUES CHECKLIST .....	42
HEALTH PRECAUTIONS CHECKLIST.....	45
HYGIENE PRECAUTIONS .....	46
STRESS CHECKLIST .....	47
CHECKLIST TO MITIGATE RISKS OF OWN TRANSPORT.....	49

## Foreword

Most participants in International Health Links (Links) – long term partnerships between UK health organisations and counterparts in the developing world – will never experience a serious accident or security incident during their work. But every health worker knows that, when delivering health care, things occasionally go wrong. Travel always brings some risk of accidents. Some developing countries and regions have more security problems than others. So it is sensible to take reasonable precautions, and to identify and mitigate risks rather than ignore them.

The consequences of failing to clarify who is responsible for what, and what to do to minimise risk and respond if accidents occur, could be potentially much more serious – for the individual Link and for the Links movement – than the costs in time and effort of being prepared.

There is no need to reinvent the wheel. These Guidelines – aimed principally at UK Links participants, but we hope useful to developing country colleagues also - summarise the collective experience of many others and provide the tools and templates that will be most useful in dealing with risk and security issues. This is a living document, and we encourage Links to tell us how the Guidelines can be improved as they are tested in practice.

THET is very pleased to publish these Guidelines as a contribution to the Links movement alongside its main Links Manual and other resource materials, to be found on our website [www.thet.org.uk](http://www.thet.org.uk). We are most grateful to our consultant and author, Lucy Hodgson, to the Department for International Development for funding support, and to all those Links representatives and other experts who helped with their experience and comments.

Andrew Purkis,  
Chief Executive,  
THET,  
March 2009.

# I. Introduction

## Aim of these guidelines

I.i These Risk & Security Guidelines have been produced by THET to provide UK Link partners with information, commonly-used terms and tools to assist in the development of their own risk management procedures for undertaking initiatives or managing trips overseas. These are generic guidelines and will need to be adapted to individual circumstances. A condensed version, covering the key principles only is also included as a chapter on Risk within the main Links Manual. This longer version is intended for use by those involved in setting up or maintaining a Links programme, who require further detail and guidance to assist them in developing their own risk management procedures.

I.ii The main audience we have had in mind has been NHS Links, although we have also consulted some university-led Links and tried to ensure that the guidance is relevant to them, too. We welcome comments from university Links about any additional material they would like to see in a revised version of these guidelines. This document is not set in stone, and we intend to revise it in the light of feedback as we go along.

I.iii It is important that discussion takes place in advance between the Link committee and the management of the NHS Trust/University as to levels of responsibility in terms of risk management. It is advisable to establish a clear policy stating what the Trust is prepared to be responsible for, what the Links Committee is responsible for, and what is the responsibility of the individual.

I.v This document is produced for guidance only, and should be used together with contextually specific information and professional advice to create the necessary tools required to provide security and risk management procedures for your own programme. THET has made these guidelines available to assist Links in the creation of their own risk management and security procedures, for which Links themselves must take responsibility. **THET and the consultant accept no liability for incidents occurring as a result of use or non-use of these materials and contents.**

I.vi Links vary widely in the kinds of work they do and places where they go. Although, therefore, you can read these guidelines from cover to cover to gain an overview, there is a clear contents page so that you can also use it as a resource document, and pick out issues of concern in your particular circumstances. The Annexes include practical checklists and templates.

I.vii The purpose of thinking about risks and being prepared is not to unduly alarm people but to make it safer to work with developing country partners – ensuring that possible risks have been identified and mitigated, and that the right contingency plans are in place just in case something goes wrong. The greater long term danger to your Link would arise if something were to go wrong when the risks had been ignored, responsibilities were unclear and no plans were in place.

I.viii **Key Principles of Risk Management** - On the following page is a pictorial overview, indicating where in this guide you will find more information on each area.

**Factors Affecting Vulnerability**

- Culture – chapter 7
- Relationships with partner and others – chapter 8
- Conduct – chapter 9
- Health & Hygiene – chapter 10
- Stress – chapter 11

**Organisational Analysis**

Board and Management Responsibilities  
 Organisational Buy in to Link  
 Scope of Link  
 Partner Capacity  
 Chapters 1/2/4

**Contextual Analysis**

Contextual knowledge  
 Situational analysis  
 Chapter 3

**RISK ASSESSMENT**

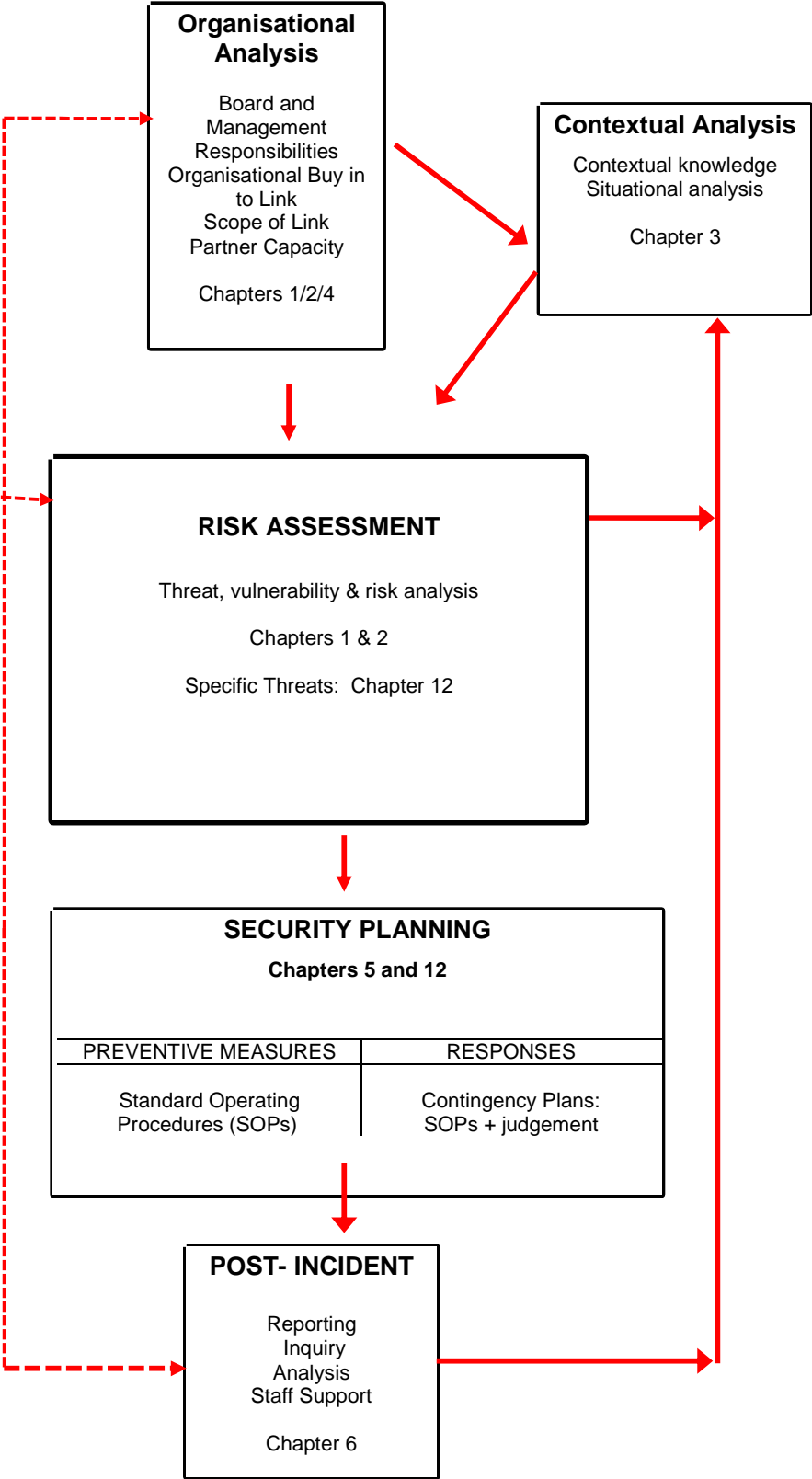
Threat, vulnerability & risk analysis  
 Chapters 1 & 2  
 Specific Threats: Chapter 12

**SECURITY PLANNING**  
 Chapters 5 and 12

PREVENTIVE MEASURES	RESPONSES
Standard Operating Procedures (SOPs)	Contingency Plans: SOPs + judgement

**POST- INCIDENT**

Reporting  
 Inquiry  
 Analysis  
 Staff Support  
 Chapter 6



# 1. Risk

1.1 In the set-up and maintenance of a Link it is important to evaluate the potential benefits of the project against the level of risk involved in implementing the project. The level of risk involved in a particular course of action may also influence the scope of a Link project. As Links are long term, organisationally owned partnerships it is important that each organisation is aware of, and accepts any risks posed by the project. Links should be beneficial to both partners and this benefit should outweigh any anticipated risks.

1.2 Risk analysis and assessment should form part of the process of establishing a Link, and has a bearing on all 4 stages of the Link establishment process (see THET's Links Manual, 2009, for further details). When going through this process, it is usually possible to identify ways of mitigating risks and bringing them down to acceptable levels, but occasionally the risk analysis at an organisational level may indicate that the risks are too high to make it worthwhile to continue to explore the Link partnership. In that case it is better to assess the issues at an early stage, rather than raise expectations and then dash them. Risk assessment is also a sensible regular process for an existing Link, so that long-standing and newer Link participants are informed and aware.

## What is Risk?

1.3 To understand Risk, we first need to understand the two components that make up risk.

1.4 A **threat** is a potential act or accident that may result in harm or injury to staff, or loss of, or damage to, an organisation or programme. Threats may be related to security, health & safety or legal issues.

1.5 **Vulnerability** is the extent to which the staff and assets of an organisations, or its programmes, are exposed to (susceptible to) a threat. It varies according to a number of factors.

1.6 Risk can be defined in many ways. It can be considered to be a function of the threats in the operating environment and our organisational/individual vulnerability to them.

1.7 Risk is the extent to which we are vulnerable to threats

Risk = Threat x Vulnerability

Risk ↓ = Threat (External) x Vulnerability (Internal) ↓

1.8 As we reduce either the threat itself or our vulnerability to it, we also begin to reduce the risk. Often we cannot affect the threats, but we can easily manage our vulnerability (exposure or the likelihood of encountering the threat) through our risk and security policies and practices, that is, how our activities are managed and implemented, how we conduct ourselves and the procedures we have in place.

## **2. Risk Assessment**

2.1 Assessing risk is essential, if we are to be able to reduce the likelihood of unwelcome events or incidents affecting us adversely. In order to assess risk accurately we need to understand where we are going to be living and working, as well as understanding ourselves. This is why having a good grasp of the overseas context (as outlined in the next chapter) is a pre-requisite to being able to carry out an accurate risk assessment relevant to an overseas trip or project.

### **How to assess risk**

2.2 Risk assessment and analysis helps you identify the most likely threats you will face, which helps you identify those measures most likely to keep you safe — it will also help you avoid unnecessary actions. Threats are things that have the potential to cause harm to your organisation or to individuals. These can include threats to do with liability and litigation as well as threats related to security and safety. A form for risk assessment is included in these guidelines. Your organisation may also have its own risk assessment procedures which can be used for this purpose. Many insurance providers also provide guides and frameworks for conducting risk assessment, so it is worth contacting your provider to see if they have these available.

## RESPONSIBILITIES for risk assessment

**This may change from organisation to organisation, however the following example is typical**

**Board** – The Board have overall responsibility for risk management which is delegated to the Chief Executive for operational purposes, and have statutory accountability for risk.

**Chief Executive** - The Chief Executive has overall responsibility for all risk management issues and to ensure that the Trust has in place an effective risk management system for meeting its statutory obligations, adhering to guidance issued by the Department of Health thereby ensuring robust governance arrangements are in place. In order for this responsibility to be effectively discharged, other senior colleagues will have specific delegated responsibility to support the Chief Executive in this process.

**Director of Finance and Information Governance** - The Director of Finance and Information Governance has delegated responsibility for managing the strategic development and implementation of financial risk management.

**Medical Director and Director of Modernisation and Nursing** - The Medical Director and Director of Modernisation and Nursing have joint delegated responsibility for managing the strategic development and implementation of clinical risk management and clinical governance.

**Director of Corporate Services** - The Director of Corporate Services has delegated responsibility for managing the strategic development and implementation of corporate risk management and assurance, and is responsible for the development and maintenance of the Risk Register.

**All Directors** - All Directors must ensure that where there is a potential risk to the health, safety or wellbeing of employees, service users, carers or the public, a suitable and sufficient risk assessment must be undertaken.

**Managers** - All Managers below the level of Director will be responsible for undertaking risk assessments. Where appropriate, the results of the assessments must be communicated to employees, service users, carers or the public before they are exposed to these identified risks. Directors will also be responsible for systematically identifying, assessing and analysing any strategic risks that may affect the organisation ensuring that such risks are included on the Trust's Risk Register.

**The Governance Committee** - The Governance Committee is in turn responsible to the Trust Board for;

- ensuring all risk management arrangements are in place
- overseeing clinical and corporate risk management practice
- ensuring that significant risks are brought to their attention
- monitoring and reviewing performance with regard to the management of risk
- developing key indicators capable of showing improvements in the management of risk and/or providing early warning of risk.
- reviewing the Risk Register on a regular basis to ensure effective management of risks
- receiving and taking appropriate action on incident reports, details of complaints and claims, from reports generated by the Risk Management System
- monitoring and ensuring compliance with legislation, standards, policies, procedures, protocols and guidelines etc
- ensuring robust risk management training arrangements are in place.

2.3 Risk Management starts at the organisational level. Senior managers may be on the Links committee but your Board should also be involved in establishing risk management policy and procedures, or extending existing policy and procedures to cover overseas activities. It is important that policies and procedures are put into place to manage all risks identified in your risk assessment, and that the resources are available to support and implement your chosen mitigation measures. It is recommended that a Links risk report is submitted to the Board at least annually. More important still is that individual staff have an awareness of risk and what they are expected to do on a daily basis to reduce their own personal risk.

2.4 Good risk management policies & procedures include:

1. Key organisational principles and responsibilities for risk & security
2. Method for assessing the potential risks you face, including provision for regular review of risk assessments
3. Actions to be taken at an organizational level to minimize risk - this may include training, written procedures, checklists and key areas of responsibility of individuals on the management committee
4. Actions to be taken by each individual to minimize risk
5. Arrangements with regard to liability insurance, including measures to take with regard to professional indemnity insurance and professional registration
6. Provision of appropriate travel & medical insurance
7. Security & conduct of staff and other stakeholders when involved in travelling overseas
8. Security & conduct of programme visitors from the overseas partner to the UK
9. Specific measures with regard to key threats identified as high or medium in the risk assessment, which will need to be enforced at a policy level.
10. Procedures for briefing staff on risk and risk management.

### Acceptable Threshold of Risk

Acceptable threshold of risk is the level of risk an organisation or individual is prepared to deal with to accomplish a goal or activity. It will vary depending on the cost/benefit analysis of each programme, and will also vary for each individual staff member. Another way to look at this is as an organisation or individual's sensitivity to risk, or willingness to take risk. It is important that this remains in proportion to the expected gains. If both the likelihood of a threat occurring and the impact of a threat occurring remain high or medium high despite mitigation measures then serious reflection is required as to whether this risk is so high as to make the programme activities non-viable.

Risk is a function of both threat and vulnerability so is specific to the organisation and individuals involved. Different organisations will have different acceptable thresholds of risk.

A particular NHS trust Link project was closed down after a risk assessment indicated that the potential risk of staff contracting diseases prevalent in the developing country could have an adverse effect on the operation of the Trust – both due to the potential of reduced staff capacity, and to the potential of spreading disease within the Trust itself. Senior management felt that the benefits of the Link project did not outweigh the potential impact of the risk. The project was then passed to the university, who put into place mitigation measures including briefing around the health risks and precautionary measures to reduce the risk of staff contracting disease as a result of their Link activities, and thus the Link project itself was able to continue.

## 5 Step Risk Assessment

1. *List existing threats:* both in terms of threats to the organisation and those that could affect staff whilst overseas. Knowledge of the threat in the overseas environment can be gained from previous visits, from overseas partners, through the experience of others, through research or context assessment.
2. *Further assess existing threats:* look at previous patterns, where these incidents are occurring, whether things are changing over time, certain incidents occurring more frequently, certain areas becoming too dangerous?
3. *Assess vulnerability:* identify the priority threats; namely those that pose real risks to your staff, assets and operations. The Key Question to ask is: "Where is our particular exposure, and why? What are the factors that leave us 'at risk'?"
4. *Adopt appropriate risk management strategies, policies and procedures:* Having identified the factors that make you vulnerable you are then in a position to reduce your exposure.
5. *Assess whether the remaining level of risk is acceptable:* Risk is something we face all the time in our daily life, but it is important that this risk is proportional to the expected gains.

### 5 Steps to conducting a risk assessment, worked example

A threat that is identified is: vehicle accident.

Are certain routes, types of vehicles (e.g. local taxis/buses) more prone to be involved in accidents?

Where will your staff be travelling by vehicle, will they be using roads with high accident rate?  
Who could be affected?

Make it less likely that such an event will befall your staff. Ways to do this might include:

- driving more slowly
- avoiding unnecessary travel especially through “accident black spots”
- using road worthy vehicles
- using skilled drivers

You also need to look at reducing the potential impact of a threat. Ways to do this might include:

- wear seatbelts
- take first aid training and kits
- take out travel & medical insurance
- have a mobile phone (charged and with airtime) with emergency contact numbers to alert assistance quickly

If these measures to reduce likelihood and impact are taken at the organizational and individual level, has the risk been reduced to a level which the organization and individuals are willing to accept?

If No: Are there other measures to take that will further reduce the level of risk to an acceptable one?

If still No - could this particular risk mean that you need to rethink the programme?

### Vulnerability Analysis

2.5 Vulnerability is the likelihood of encountering threatening incidents and as a result, harm occurring to staff, resources, organisational reputation or programme activities. Different organisations and indeed individuals will have differing vulnerabilities. A range of factors affect our vulnerability, some of which are easier to alter than others. Factors affecting vulnerability can include:

- Location: of staff and property;
- Exposure: where you are, and where you travel to, can increase or decrease exposure;
- Value of property;
- Type of activity: what work you are involved in and how this is perceived;
- Relationships: who are you perceived as being connected to in the context, and how are these other players seen?
- Gender/Age/Nationality/Race: demographic indicators can make us more vulnerable to some threats and less vulnerable to others;
- Adoption of appropriate security measures and compliance of staff with security measures;

- Staff interpersonal skills;
- Awareness of the local cultural norms, and how these can impact on vulnerability.

More detailed templates and checklists for risk assessment are in the Annexes.

### 3. Contextual Assessment

3.1 If we are to be properly prepared for visiting or living and working in a new environment, we need to research and understand it. This research includes things we do before leaving for/sending colleagues into a new environment, as well as gaining information on arrival from our surroundings and contacts.

3.2 This process is called **context assessment**. **Assessing the context** means gathering information to give an historical understanding of the political, social, economic and cultural background of a particular environment. This may include:

- Current situation (political, social, economic, humanitarian, military and cultural conditions)
- Roots and dynamics of any current or past conflict that still has a bearing on the current situation
- Infrastructure and climate
- Relations with other countries
- Cultural and societal norms and attitudes

3.3 A good context assessment will help both in getting to know more about where you are living and working, as well as providing information to assist with the **risk assessment**. Information from the **context assessment** should be written down and can be used to inform your Link handbook or project information sheets, and for briefing of staff. Whilst detail from other sources, and useful web based references can be included and used for the detail, it is important to create a concise and clear context assessment specific to the needs of your organisation.

3.4 Where an initial **context assessment** has already been carried out, this can be updated prior to any field visit with a short **situational assessment**, dealing with recent developments.

3.5 The **situational assessment** builds upon the **context assessment**, and enables the tracking of new and emerging trends and developments. It also enables you to analyse how your project activities and partners may be perceived.

3.6 Typical areas to cover in a situational assessment include:

- *Relationship Analysis*: How different groups relate to each other, and perceive each others agendas and actions
- *Political Analysis*: Relationships within and towards national and local authorities, and other seats of power in country. What are the relations between those in power and the general population? Are these static or changing?
- *Profile of Crime*: The nature of criminal activity, its social context and its acceptability and the targets
- *Conflict and Violence Mapping*: Both a geographical visualisation of any continuing conflict and as a means to understand the structure of the conflict, and its evolution.

3.7 Sources of information for contextual assessment are widespread. The following are suggested as good starting points for information pre-departure.

- Partners in country
- Other Links working in the same country
- THET (depending on the country)
- DfID/FCO: [www.dfid.gov.uk](http://www.dfid.gov.uk)
- Relief and Development agencies that are working in the same region.
- Relief web: [www.reliefweb.net](http://www.reliefweb.net)
- Alertnet: [www.alertnet.org](http://www.alertnet.org)

3.8 Being well informed is one of the keys to managing risk. This applies at every level: all staff should be aware of what is going on around them.

### **Relations with the local population**

Relations with the local population are probably the most important of all sources of contextual information. Good relations are vital for successful programming, and for security. Relationships with leaders of all significant groups, and with ordinary people of all types, greatly increase your ability to work well and get the most out of your overseas experience and to do so in a way that is safe for others, whether these are local people or other international staff.

When overseas it can greatly assist both your work and the experience if you are able to spend a proportion of 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 staff and directors of partner organisations
- Regular meetings with local leaders of significant groups
- Visiting people living away from major towns, and away from major roads if possible. Encourage your partners to assist you in doing this as there is a tendency for busy staff to visit people near easily accessible towns and routes far more than those in areas off the beaten track
- Attendance at social occasions, when invited
- Encourage your partners to assist you in discussing and sharing information with other organisations
- Reading local press and listening to local radio and TV

## **Relations with other organisations**

Work with your local partner to access other organisations. Good relations with other organisations in the area can help to enhance security, for 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 with other organisations
- 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

In some cases NGOs and similar organisations 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 and need to be skilfully chaired to ensure that discussions are efficient.

In many countries 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 other relief & development actors.

## **Travel Preparations**

3.9 Appropriate pre-visit planning, will make your trip go smoothly. It is also a key way of reducing risk. Good planning will help those travelling overseas, along with those supporting them.

### **Briefing**

3.10 A good briefing helps prepare staff and visitors for the area they are going to, and is vital to reduce risk. Try to identify a number of experienced staff who would be willing to brief new participants. This briefing should be as thorough as possible and if possible be accompanied by basic written information, to remind staff of points that they may not have taken in during face-to-face briefing.

3.11 Checklists for briefing and pre-departure on overseas trips are included in the Annexes.

### **Basic Travel Preparation**

3.12 The checklists in chapter 14 describe this in more detail, however at a minimum each Links participant should have ready access to a functioning mobile phone that works in the developing country, and essential numbers needed in the event of any sort of security or safety incident. These numbers should include:

- Contacts for partner agency in country
- Contacts for Links committee back home
- Insurance details
- Medical evacuation provider details

- British Embassy in country
- A 24 hour emergency contact number – someone who can provide emergency support and back up, and who has copies of essential documentation including next of kin details.

3.13 Essential documentation should also be given and carried by each participant. This should include:

- In date passport, with valid visas and at least 2 blank pages.
- Travel Plan, including all flight details and details of in-country contacts and accommodation addresses
- Medical information, including blood group and list of any pre-existing conditions
- Insurance documentation, including copy of policy and key contact details taken; (plus summary of procedures e.g. getting police report, first contact in an emergency etc)
- Communications plan with project coordinator, including plans for emergency contact;
- Vaccination Booklet with immunisations taken as appropriate for the country;
- Authorisation letter from partner/other key contact in country sourced – this is a simple letter saying who you are and where you are going, and can help in case of simple problems at border controls etc;
- Medications and copies of repeat prescriptions, including glasses/contact lens prescriptions.

3.14 It is advisable to agree a communication plan pre-departure. This should cover frequency of communications and who these will be with. A contact should be arranged on arrival to ensure that the traveller has arrived safely.

3.15 When travelling in-country it is advisable to ensure that this procedure is also followed, so that someone is aware of where the Links participant is at all times and their planned movements, so that they will be noticed if they fail to ring in/turn up and so that a designated person knows he or she is responsible for immediate follow up and raising the alarm if necessary.

## **4. Professional, Insurance & Legal Issues**

### **Insurance**

4.1 Appropriate insurance provision is a key measure in reducing the impact of a whole host of threats. In advance of activity and visits overseas, each Link should look at what insurance provision is appropriate. Check what kind of cover is already offered by the Trust or University's insurance provider. The Links committee should discuss with the Board or Deanery where additional cover is required and decide who will cover this additional cost. Advice on insurance provision can be obtained from British Insurance Brokers Association (BIBA) [www.biba.org.uk](http://www.biba.org.uk) who can provide details of specialist insurance brokers.

### **Travel Insurance**

4.2 Whilst many individuals will have their own "worldwide" travel insurance, and indeed many banks and credit card companies now promote certain products as automatically Linked to "worldwide travel insurance", these are designed for travel and tourism and are unlikely to cover staff on project visits. Links co-ordinators are advised to establish in advance with management who will be responsible for identifying and paying for additional

insurance. It is possible to take out specific insurance cover for individual trips, or if your Link is planning several trips each year, it may be cheaper and more effective to take out a Group Travel Policy which covers all travellers. This has the added advantage of simplifying procedures as in the event of an emergency, all personnel will know exactly who to contact regardless of the individual(s) affected, and in the case of an incident affecting more than one staff member, cuts down on the administration/number of calls to make.

4.3 Areas to ensure are covered by your travel insurance, whether group or individual, include: personal accident, medical expenses, war cover and political evacuation. It is also advisable to select an insurance policy which is Linked to a medical evacuation service such as CEGA (<http://www.cegagroup.com/>), who provide dedicated air ambulance service, medical assistance and repatriation services.

4.4 Some countries are NOT covered by standard Group Travel Insurance Policies – these are usually linked to FCO advice. Check with your insurance broker for exclusion areas. An FCO advisory against travel does not preclude activity in this area, however it may mean that special insurance provision, that may be more costly, needs to be taken out.

THET's Broker has kindly offered to provide initial advice free of charge to Link Members. If this is of interest, please contact them on 07525 038803 and mention that you are responding to the information provided on the THET web-site. Further advice from Towergate is available in fact-sheet form on THET's website.

## **Kidnap & Hostage Insurance**

4.5 Standard Group Travel Cover may include an inconvenience benefit (payable per day of abduction). There are a small number of overseas workers kidnapped or abducted annually. This risk is slight, and much more prevalent in some areas than others. Even in some areas of high risk, such as Columbia, where the motivations are largely economic it is often wealthy nationals who are most vulnerable rather than overseas workers. An overview of reported instances involving NGO workers is available from Interaction at [http://www.interaction.org/files.cgi/6595\\_YB\\_KRE\\_NGO\\_Stats\\_011409\\_chart\\_nonames.pdf](http://www.interaction.org/files.cgi/6595_YB_KRE_NGO_Stats_011409_chart_nonames.pdf) If your risk assessment indicates this to be a risk in areas where you are sending personnel, it is also worth considering taking out a special insurance policy to cover this area, which can be extremely complex and costly. Specialist Kidnap and Hostage insurance packages usually include provision of skilled advisors to assist in managing incidents of this nature.

## **Professional Liability & Indemnity:**

### **Vicarious liability**

4.6 This is a legal concept that exists in the UK and means that the employer is vicariously liable for the acts or omissions of an employee for work undertaken during the course of that employment. This concept does not apply worldwide. Staff should not, therefore, rely on the fact that their overseas employer or partner might have vicarious liability and should check up on the indemnity arrangements before they leave the UK, to determine if they need to make their own arrangements for indemnity.

4.7 Staff are normally covered for work undertaken in their own Trust(s) by the NHS Trust(s) with which they have a contract of employment. This arrangement may have very little bearing on the indemnity arrangements for work undertaken overseas.

## **Professional Indemnity cover**

4.8 It is advised that each employee contact their usual provider of professional indemnity cover prior to departure to ensure that they have adequate cover. RCN members automatically have worldwide indemnity insurance (excluding USA and Canada) - if in full category RCN membership. If in doubt, please check with the RCN. Other professional staff (particularly doctors) are advised strongly to check with their relevant professional insurance/indemnity companies (MDU, MPS etc).

## **Registration**

4.9 When selecting/deciding who will be best to take part in a project, bear in mind that most professional regulatory authorities recommend that it is in an individual's best interest to have 6 to 12 months UK experience to consolidate their pre-registration education and to adapt to their role as professionally accountable practitioners.

4.10 Most professionals will be bound by the code of professional conduct for the profession they are registered with, even whilst overseas. It is important that professionals practise in accordance with the laws of the host country and codes of practice that apply there. Professionals are responsible for ensuring that they continue to meet the requirements for maintaining their registration whilst abroad, e.g. continuing professional development.

4.11 Depending on the activities they will be carrying out, practitioners may be required to register with the regulatory body for the country in which they intend to work. Just as in the UK, it may be unlawful to practise without the appropriate authority and/or registration. The GMC can provide UK doctors with contact details of most overseas regulators (details on their website <http://www.gmc-uk.org/>). Similarly, the GMC provides information packs for doctors from overseas who are intending to come to work in the UK. The NMC Registration department can provide UK nurses and midwives with contact details for most overseas regulators. Where there is no system of nurse or midwifery registration, NMC registration is valid. As nurses working for the armed forces and voluntary organizations can be exempt from these requirements, we advise Links to contact the NMC to ascertain if registration is required for their specific programme circumstances. For those professions registered with the HPC, contact <http://www.hpc-uk.org/> for further information.

4.12 For the UK, if a visiting doctor is to be practising (including prescription or invasive procedures) they must have limited registration with the GMC.

## **Pensions**

4.13 For those working in the NHS who retain their NHS contract whilst working/visiting overseas, as long as the employer continues to pay pension contributions then there is no change to pension provision. There is no problem posed by the typical pattern of short teaching and training visits undertaken by most Links. If there is a break in service, then the effect on pensions depends on the length of the break. Less than 12 months is usually not a problem and there is no reduction in pension accrual. If the period is greater than 12 months, then there will potentially be a reduction. It is sometimes possible to get an exception with the direction of the Secretary of State if the break is to work overseas for a charity. This may involve the worker having to pay the employer's contribution themselves. For further details, contact the NHS pensions agency:  
<http://www.nhspa.gov.uk>

4.14 The UK Government has created a £13m fund to contribute towards the pensions of public servants while they volunteer with VSO or another British Volunteer Agencies' Liaison Group (BVALG) member organisation (currently, International Service (UNAIS), Student

Partnership Worldwide, Skillshare International, Progressio and VSO). The fund will buy added pension benefits (or equivalent) for any current public servant, including those working in the NHS, who returns to a pensionable UK public service job after an overseas volunteer assignment starting between April 2008 and March 2011 and lasting between seven and 24 months. Further information on the new pension offer is available in the FAQs section of VSO's website:

<http://www.vso.org.uk/volunteering/faq/pensions.asp>

## **5. Security planning**

5.1 Where there will be a permanent overseas presence, or a number of staff on long-term assignments on the part of a Link, or where there are visits to countries where there is evidence of insecurity, it can be worth developing a country security plan, giving context-specific security rules and procedures. These rules and procedures should be decided in the light of the risk assessment and should be reviewed at least annually.

5.2 In low-risk locations, both the risk assessment and the security plan can be very short. In high-risk locations, both documents are likely to be somewhat more detailed. In all cases they should be as concise as possible, since busy staff may be tempted to ignore long documents. What is important is that they must be appropriate to the circumstances of the particular location that they refer to. Suggested contents for a security plan are included in the Annexes. THET will be glad to assist with information and advice for countries with which it is familiar, or to give contacts of other Links that have addressed similar issues.

## **6. Incident Reporting**

### **Prevention**

6.1 Prevention is better than cure. Training and experience are the most important factors in preventing security and safety incidents from occurring, and in limiting the damage should they happen despite careful planning. Everyone can help prevent security incidents and many kinds of accident by:

- Being alert and aware of our surroundings
- Being well informed, through regular briefings and any other appropriate channels
- Observance of security rules and procedures
- Only taking risks that are necessary, and justified by the benefit gained
- Applying common sense

### **Reaction**

6.2 If an incident or accident occurs, its impact can often be greatly reduced by applying sound procedures.

### **Reporting incidents**

6.3 This section refers to both security and safety incidents and accidents. It is useful not only for the management of incidents, but also to enable appropriate measures relating to insurance and organisational duty of care, that the responsible project manager/coordinator or Links committee member is informed of any incident as soon as possible.

6.4 A standard 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.

6.5 There are three types of incident report:

- **Immediate incident report**, sent the moment the incident begins or as soon as possible thereafter, often by phone or radio. It alerts colleagues to the incident and enables them to respond;
- **Follow-up incident report**, giving more information as soon as this is possible. Written is preferable, but it may be by radio or phone if necessary;
- **Post incident report**, compiled after the incident is over. This must be written.

6.6 The standard format for an **immediate or follow-up 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?**

6.7 If there is no time to send all of the above send whatever message is possible to your key contact – e.g. “Ambush!” or “car crash!” – which gives some idea of what is happening. Your contact may be able to work out how to respond, and how to avoid the same danger, from even the briefest of information, and this could save lives.

6.8 A **follow-up incident report** follows essentially the same format as the immediate report, updating information and giving more detail, as soon as the situation allows.

6.9 A **post incident report** gives a complete written account of the incident and if completed by ALL those involved in the incident, can ensure that a possible forgetfulness due to stress or shock is not overlooked by a 2<sup>nd</sup> or 3<sup>rd</sup> person, and should follow this format:

- 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, and signature.

### **‘Near miss’ incidents**

6.10 ‘Near miss’ incidents should always be reported. A ‘near miss’ is where it appears that a security or safety incident came close to occurring. It may reveal a weakness in security/safety procedures, or new information about threats.

6.11 A ‘near miss’ incident in some cases will not require an immediate or follow-up incident report, but should always result in a post-incident report so that lessons can be learned.

## Analysis of incidents and adjustment of procedures

6.12 After an incident, the relevant managers and staff 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 or other bodies? Should follow-up action be taken (possibly including disciplinary action) in relation to any member of staff/volunteer?

6.13 Records of all security/safety 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?

6.14 Templates for incident reporting, analysis and tracking are included in the Annexes.

## 7. Cultural differences

7.1 It is difficult, if not impossible, to learn all the potential cultural differences or sensitive areas between your culture and the various cultures where you may work or visit. The following list of typical “cultural pressure points” has been prepared as “food for thought” when visiting a country, or when preparing context- specific cultural guidelines.

### Cultural Sensitivity

- **Communicate respect** for the other culture(s). Learn a few words of greeting and politeness at the beginning. Learn basic historical, political and social facts about the country. Find out the essential courtesies, customs and non-verbal behaviour.
- **Be non-judgemental** - Assume that there are differences until you are sure of the similarities.
- **Tolerate ambiguity** - learn not to be upset by strange situations, or to feel uncomfortable if you are unsure of your status or peoples' reactions to you. Don't assume the worst, look for other explanations first if a person's behaviour appears to you to be offensive.
- **Be tolerant** of other people's customs – avoid unreflective indignation about “issues of conscience” such as attitudes to gender, nepotism and corruption.
- **Be flexible and patient** - becoming angry or “uptight” will never help a situation. Be prepared and willing to learn and to adapt to your situations.
- Know where you stand - **understand your own culture** and how you feel about it.

## 8. Relations with Partners/Host Organisations

8.1 Links are usually characterised by close working relationships with local and international partner organisations. Most work is carried out via partners. For this reason staff presence is usually restricted to short term field visits, where staff are based within the partner organisation or other affiliated body. Given this, the relationship between the staff member and the host organisation, whether for a short term field visit, or for a longer period, is of prime importance.

8.2 It can therefore be helpful to develop a general Memorandum of Understanding (MoU). Information on how to develop an MoU is available in THET's Links Manual. A well developed MoU will also act as a tool to reduce risk to your organization, by spelling out the roles, duties and responsibilities of the parties. THET has a more detailed template for MoU's available on request.

8.3 To maintain the reputation of the Links partnership, Link participants' conduct should be consistent with the intent of the MoU. Statements and behaviour made even outside normal working hours should give a positive impression of the partnership. Take care not to make statements or behave in a way that may damage this reputation, and respect local and national law and customs at all times. Staff of the host organisation should of course be treated courteously, equitably and without discrimination. This is important in its own right but also enhances confidence, security and safety.

8.4 Premises and property of the host organisation should likewise be treated with respect. An advance arrangement should be made in terms of use of resources and reimbursement. Use of materials/resources outside this agreement would only be possible with the express permission of the host organisation.

### Host Organisation rules & regulations

The actions of visiting staff may have an impact on the security of partners, and *vice versa*. It is therefore important that there is close liaison between partners on security and safety matters. Staff, when travelling to/based with partner or other organisations overseas, should ensure they are familiar with and comply with any security procedures or guidelines that the host organisation may have in place. Where these procedures and guidelines are LESS stringent than those contained in your organisation's risk and security policy and other guidelines, it is advisable to follow those of your own organisation. Where the host organisation's security rules are more stringent, these should be adhered to. Not only may the host organisation have a more accurate picture of the risk environment, but this will help promote equity and foster strong relationships between the staff members and staff of the host organisation.

## 9. Personal Conduct

9.1 The following guidelines can be used to develop your own conduct guidelines for inclusion in briefings or in a handbook. As well as reducing risk, they help in getting the best experience out of your visit overseas.

9.2 Your conduct will not be only ascribed to you personally. You are, in whatever situation, an official representative of both your home and host organisation and will be considered as

such. Unacceptable behaviour, either on or off duty, could harm not only your own reputation, but that of the organisation and of partners.

- Your personal behaviour contributes substantially to risk.
- Try to remain just and act tactfully. Never use unnecessary violence or force.
- Do not become involved in personal or sexual relationships which may threaten your independence.
- Make no explicit or implicit promises that you cannot or will not keep.

9.3 Whilst all this sounds like common sense, it can be helpful for staff to produce a statement related to expected conduct, which can be supported with tips and hints on cross cultural communication. Some of the guidance in chapter 8 may be helpful in developing these guidelines.

## 10. Health and Hygiene

10.1 Common illnesses affecting those visiting or working in developing countries include potentially fatal infections such as malaria. People involved in the Link should be advised to take good care of their health, and be rigorous about hygiene and other preventive measures.

10.2 You may wish to establish a policy that all staff have a medical examination before going overseas. This ensures that any medical problems can be dealt with, and helps to protect the organisation from false claims concerning medical problems resulting from the overseas visit. It can also result in lower insurance premiums

10.3 All Links participants should take qualified medical advice on health and hygiene precautions in any areas with which they are not already familiar as trained professionals.

10.4 A checklist on health precautions is included in the Annexes.

Further information is available from:

- World Health Organisation: see the section on International Travel and Health at [www.who.int/ith](http://www.who.int/ith)
- Helpful travel health information website from the UK National Health Service, at [www.fitfortravel.nhs.uk](http://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 Dawood
- ***The Traveller's Good Health Guide***, a book by Dr Ted Lankester. 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.

## 11. Stress

### What is Stress

11.1 Stress can be defined as any demand or change that the human system (mind, body and spirit) is required to meet or respond to. There are normal stressors such as those consistent with life: breathing, blood circulation, walking, eating, talking and even playing.

11.2 While some stress can be good for you, prolonged or extreme stress can mean staff manage safety and security risks less well.

#### Types of stress

- Basic stress: Can occur on arrival in the field, be brought from home or be a result of a mixture of different factors.
- Cumulative stress: Builds up slowly as a result of a variety of internal or external factors. It can lead to burn out, over working, alcohol or drug abuse, health problems and risky behaviour.
- Acute or traumatic stress: Acute or traumatic stress is caused by an unexpected and violent event, which harms or suddenly threatens an individual or someone close to him or her either physically or psychologically, calls up images of death, and provokes fear and a feeling of helplessness.

11.3 Different 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.

11.4 A checklist on causes of stress and potential prevention measures is included in the Annexes.

### Treating stress

11.5 A doctor or trained person will advise on treating stress. Debriefing should be done by a trained person if possible (as it will be in many Links). 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 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

## **12. Specific Threats**

12.1 This section of the guidelines deals with some specific threats, which can be a risk in developing or conflict countries. There may be additional threats identified for your particular location from the risk assessment. This section gives an idea of some common mitigation and contingency measures to deal with each threat. It is vital to adapt these for your particular context, as not all measures are valid for every circumstance and location. Certain more serious threats such as kidnap & hostage taking and conflict environment based threats are not included here, as most Links are unlikely to be operating in these high risk environments. THET has its own guidelines on these issues which can be shared with Links on request.

### **Travel & Transport**

12.2 Vehicle accidents are one of the most common causes of injury and death to overseas workers. Safe driving practices and vehicle management reduces the risk of accidents and gives a responsible approach to vehicle use. Not only are accidents a serious safety risk, but staff may expose themselves to security risks in the aftermath of a road accident. Whilst in many countries public transport can be overcrowded and unsafe, often engaging a local driver is far safer than driving an unfamiliar car in an unfamiliar environment. Ensure that staff select the safest means of transport possible for the environment. This will include checking that vehicles are roadworthy and equipped with basic safety devices such as seatbelts, and that drivers are known to staff or to partners and have appropriate skills. A fuller checklist on travel and transport is included in annex in chapter14.

### **Crime (theft, robbery, burglary, assault, etc).**

12.3 Crime is a key threat in many environments. The exact nature of crime and the key points of vulnerability should be identified in your risk assessment.

**Confronted with acts of crime, general points to be considered:**

- Maintain a low profile, particularly after working hours;
- Seek advice from trusted locals;
- Reinforce usual security set-up, in particular information gathering;
- Avoid driving or walking alone (lone people are the easiest targets);
- Do not give away information (no name on luggage/when answering phone, etc.);

**Particularly when under threat of theft, (armed) robbery, burglary, attack, assault (mugging, hold-ups) it is advised to:**

- Not carry large amounts of money, but to have always some small cash;
- Not display wealth (watch, jewellery, etc.);
- Carry discreetly mobile phones and lap-tops, if any;
- Visually check the surroundings when entering/leaving a building;
- If possible, use alternate route to and from the office/home;
- Apply irregular time schedules;
- Move in vehicle only, and if possible always, together with a local driver;
- Do not leave equipment/material unattended in the vehicle;
- Keep some freedom of movement (distances from other traffic) in order to escape, if necessary;
- Define off-limit zones and impose internal curfew if appropriate;
- Stay only with partners, other organisations or in mid-level hotels with good security that have been recommended

**In case of threat of (armed) burglary:**

- Check that your residence and buildings are secure and ensure that any existing security measures are being followed.
- Keep doors and windows locked;
- Have outside light on;
- Have emergency numbers always available, check if telecommunication means are working;
- Get to know neighbours personally;

## **Harassment & Sexual Violence**

12.4 Harassment is defined as any violation of personal integrity or personal space, which is unwanted by the recipient. Harassment may be persistent or an isolated incident and may be directed towards one or more individuals.

12.5 Harassment is not only unwanted physical conduct, assault or propositions. It includes suggestive remarks or gestures, pin-ups, graffiti, offensive comments, jokes and banter. The definition of harassment can be both cultural and personal and may vary depending on the perspective of the recipient.

## Sexual Violence

12.6 Sexual violence is a non-consensual sexual act forced upon a person. It is violence of an explicitly sexual nature. The consequences of sexual violence are severe and the risk needs to be recognised and managed. The motive for sexual violence is not usually sex but power and humiliation and as a weapon of war. The key message as a potential victim or witness is to **protect and preserve life**, and this can be helped by being prepared. Sexual violence can affect both men and women. For a victim, rape is considered the second most violent crime after murder. Sexual violence will also have consequences for witnesses, families, and colleagues who can be affected as a result.

12.7 Sexual violence constitutes an extremely serious threat, one which, due to under reporting, can be difficult to accurately assess during a risk assessment. It is a significant risk in some conflict and post conflict environments.

### Mitigation Measures

- Adopt a conservative personal appearance and manner in keeping with local societal and cultural norms.
- Where possible avoid being alone in high risk areas, travel with others, and take accommodation with other organisations/partners.
- Consider investing in devices such as whistles which can be used to attract attention.
- Take care when selecting accommodation – hotels, parts of town, quality of room and staff, identification. Choose a room that is not on the ground floor.

### In case of an Incident

- Ensure the physical security of the survivor (and witnesses)
- Prevent any further suffering
- Ensure privacy to the furthest extent – the attack should not be broadcast and it should be the victim who decides who should be told and what they should be told, except where reporting protocols require otherwise.
- Be guided by the best interests of the survivor.
- Respect the survivor's wishes in all instances.

### Surviving Sexual Violence

No general rule on how to survive, beyond seeking help at the first possible opportunity.

### Post Incident Measures

- Seek immediate medical attention
- Counselling for survivor(s), witness(es) and colleagues.
- Criminal investigation/prosecution and legal implications - prosecution the survivor's choice
- Incident analysis – revision of security guidelines?
- Sharing of information about the security incident - but main issue here is **survivor confidentiality**.

### Hostility (crowds, mob violence, looting, demos)

12.8 Even in relatively stable environments tensions can rise periodically, increasing the security risk to those caught up in the situation. It is therefore important to provide staff with guidelines on how to avoid getting caught up in hostile situations, as well as with advice on how to react when confronted with rising tension - crowds, mob violence, riots, protests, demonstrations, looting, etc. The appropriate behaviour will vary depending on the context, and local partners and contacts can usually provide good advice.

12.9 The following generic guidance may also help you when developing your context specific procedures:

- Remain alert to changing situations
- Exercise much greater caution than usual
- Enhance information gathering
- Seek advice from local contacts/partners
- Avoid large crowds and other situations in which sentiments may be expressed
- Never attend public meetings where grievances are the theme
- Reduce movements/visibility (no private movements) and coordinate vehicle movements.
- Communicate with partners and other organisations and establish close Links to authorities
- If in a vehicle when confronted, do not get out, lock doors, close windows and drive carefully away
- Maintain poise and dignity if confronted by a hostile situation
- Do not become angry, or at least, do not show the anger
- Impose internal curfew

## Arrest & Detention

12.10 Arrest and Detention are two related threats that staff may be vulnerable to, depending on the country of work, the nature of partner activities and how these are perceived by authorities. The risk of both can be reduced by ensuring acceptance from the community for the work that the Link and partners are engaged in, and by good contextual knowledge as well as through good operational practice, transparency, integrity and respectful attitudes.

### Detention

Staff are kept under the control of an individual or group. There is no serious threat to life, but also no clear conditions for release. The detention can be any length of time, from a few minutes to several months. Detention can be a high risk in conflict and post conflict environments.

### Arrest

Staff are detained, usually with charge, by state bodies, or the “presumptive authorities”. This can be done legally and openly, or secretly out-with usual judicial mechanisms.

### How to avoid Arrest and Detention

- Avoid being in high risk areas
- Have good relations with local authorities
- Ensure that all legal documentation is correct, and carried by all staff and vehicles as required
- Be aware when activities may cause potential friction
- Avoid photographing sensitive objects
- Sensitivity when reporting human rights incidents, especially if perpetrated by the military, police or groups they support
- Culturally appropriate behaviour
- Respect local laws and norms
- Appropriate conduct at checkpoints

### **If Arrested/Detained**

#### Individual:

- If possible retain communications device
- Behave with respect and courtesy
- Request essentials that you need

#### Manager:

- Ensure that someone external is aware of the situation
- Report to embassy/commission
- Elicit information as to reason for the arrest/detention
- Obtain the assistance of a lawyer, if necessary
- Inform the ICRC and ask their advice, if appropriate
- Inform the UN where appropriate
- Inform the Next of Kin if the person is not released very quickly

### **Danger of mines, unexploded (improvised) ordnance and booby-traps**

12.11 Even in relatively stable environments, there can be remaining threat of unexploded ordnance or mines that remain long after the end of a conflict. If this is identified during the risk assessment, it is important to ensure that mitigation measures are followed by staff. Never take any risks in connection with mines, unexploded (improvised) ordnance and booby-traps. These deadly devices are insidious and powerful; and they never miss.

12.12 In areas likely to contain mines, unexploded (improvised) ordnance and booby-traps, never touch or even go near any object that seems unusual or out of place, whether it looks like a mine or not. Beware in particular of trip-wires and pieces of metal sticking out of the ground. Never go near any ruins or wreckage, and remember that abandoned bodies may be bobby-trapped. If you find yourself in a mine field by mistake, firstly try to contact professional assistance, and remain where you are. As a last resort, if there is no help available and there are other associated risks of remaining in situ, try to retrace your footsteps or wheel-tracks.

## **13. Resources**

13.1 The following resources are useful for further insight on risk management and security, and can assist in creating your own procedures and documentation:

[Operational Security Management in Violent Environments](#), Koenraad Van Brabant. A manual designed for the security management of non-governmental organisations. (The book is also known as GPR 8, for number 8 in the series of Good Practice Reviews published by the [Humanitarian Practice Network](#).)

[Mainstreaming the Organisational Management of Safety and Security](#), Koenraad Van Brabant. In 2001, Van Brabant's follow-up to GPR 8 was published. Where GPR 8 is primarily field-oriented, "Mainstreaming" focuses on security management practices and philosophies.

UN: [Landmine and UXO Safety Handbook](#)

## **14. Annexes: Templates, Forms and Checklists**

14.1 These Annexes can be adapted and used to enhance Risk and Security Management of Links.

### **Risk Assessment**

Explanation of Form overleaf:

In the "Hazard/Threat" column, list all threats identified in the threat assessment. Beside each threat, give a rating for the impact on your Link if this threat were to occur, along with an assessment of the probability or likelihood of this threat occurring. The combination of these 2 ratings will give a rating for the level of risk. For all hazards with a significant risk of 5 + (impact \* probability) the mitigation measures which are to be taken should be listed. After listing these measures, reassess the risk and assign a new rating to it.

## Risk Assessment Template

To be completed for all journeys outside of the UK

Event and Date: \_\_\_\_\_ Completed by: \_\_\_\_\_

### Risk Mitigation Factors

For all hazards with a significant risk of 5 + (impact \* probability) the mitigation measures which are to be taken should be listed – if needed as an addendum to table. The risk with these measures should be then be inserted.

Hazard (Threat) with notes	Impact I (1-5)	Probability P (1-5)	Risk = P x I	Mitigation Measures	Mitigated risk

Probability & Impact	
Low	1
Medium	3
High	5

*NB: This form should be updated in case of new information established after arrival, for any changes in the security environment, and in the case of a change in original travel arrangements requiring additional travel to other towns/regions.*

## **Risk Assessment Checklist**

This checklist can be used to assess risk for a project or visit, as well as a guide in the set up of appropriate risk management plans for a location where Link staff are/will be based.

### **Threats**

- What are the major threats in the region?
- Rank the threats in order of lethality
- Rank the threats in order of probability

### **Vulnerabilities**

- What are the vulnerabilities of the project/staff?
- How can these vulnerabilities be minimised?

### **Risk**

- What is the acceptable level of risk for the project?
- What is unacceptable risk?
- Are risk management procedures in place and adequate?

### **Programme**

- What impact will the project have on the local partner
- How can the Link strengthen relationships with the community and improve the reputation of the partners?
- Are there weaknesses in the Link that leave the partners susceptible to violent incidents or damaged reputation?
- Will staff be undertaking field visits to the location to support partners?
- Will visiting/placed staff be based in this location?
- Will staff be lodging/working with the support of another organisation?

### **Policies**

- What are the policies for risk management? Are they adequate?
- Do other policies (HR, Finance, etc) support the security of the project? Are they adequate?
- What changes or additions to policies would enhance the security of the staff when working/visiting this location?
- What resources are required to implement these policies? Are the resources available? How can they be obtained?

### **Preparation and Planning**

- Will there be frequent travel to/staff based in this location – if so is there a security plan? Is it adequate?
- Will staff be capable of supervising/executing the security plan?
- Are preparations made in accordance with the security plan?
- Is the project prepared to meet the identified threats given its vulnerabilities?

### **Communications**

- What are the methods of communication? Are they adequate?
- Are there redundant means of communications?
- Are there emergency communications procedures? What are these, and are there any restrictions/limits on how/where these will work.
- Is communications equipment used/stored/maintained properly?

## Travel Briefing Checklist

### Security briefing

A briefing on context & risk should be given to all staff and visitors, including:

- A summary of the prevailing situation;
- A short history of any conflict, if applicable;
- Identification of the main actors and their assumed interests and relationship;
- How partners are perceived by the population and the main actors;
- Summary of the most likely types of threats;
- Security procedures and measures that are in place (rules);
- Personal security matters and behaviours;
- Likely future trends and development.

### Orientation

In addition it is advised to brief about:

- Culture and local laws;
- History of project involvement in the country;
- Summary of projects and programmes;
- Presentation of partners and other organisations;
- Use of telecommunication equipment including local phones, satellite phone, mobile phone and radio (whichever is applicable);
- Vehicle use
- Medical evacuation procedures;
- Locations like, embassies, hotels, health facilities, police, etc. (provide a map and contact details).

### Documentation & Equipment

The following documentation should be given/completed:

- Constant Companion card (a card with key contact details on it which can be laminated and carried easily);
- Travel Plan (incl. communication details);
- Risk Assessment;
- Information about partners and other organisations;
- List with all relevant addressees, phone numbers;
- Mobile Phone, charger and airtime

## Pre departure travel checklist

Prior to travel the following checklist can help as a reminder:

- ❑ Travel authorisation form, including FCO advisory listing completed
- ❑ Travel Plan to be completed, including travel mode in country
- ❑ Insurance cover validated, and copy of policy and key contact details taken; (plus summary of procedures e.g. getting police report, first contact if an emergency etc)
- ❑ Ensure that personal data held by responsible co-ordinator/manager – this should include next of kin, and medical details
- ❑ Communications plan with project coordinator, including plans for emergency contact
- ❑ Vaccinations taken as appropriate for the country (See <http://www.who.int/ith/countries/en/index.html>)
- ❑ Anti-malarial precautions must be taken (See <http://www.who.int/ith/countries/en/index.html>)
- ❑ Flights and transport booked
- ❑ Visas procured
- ❑ Authorisation letter from partner/other key contact in country sourced – this is a simple letter saying who you are and where you are going, and can help in case of simple problems at border controls etc
- ❑ Emergency money taken
- ❑ Provider of professional indemnity insurance informed
- ❑ Professional registration procedures/needs verified
- ❑ Medications and copies of repeat prescriptions, spare glasses etc taken
- ❑ Contact details of partner and contacts in country taken

## **Suggested contents of a project/country specific security plan**

### ***Introduction***

For all documents, it is suggested that there should be an **Introduction** which includes:

- *Date and author* – so that it is known when and by whom it was produced;
- *Purpose of the document* – to be clear about its breadth of application. Strategic Priorities of the Agency cf. Security – People, Equipment, Project. Purpose is to mitigate risks and make them acceptable....otherwise 'don't be there';
- *Intended users* – so that the readership is clarified;
- *Use of the document* – how it is to be used, its role within on-going security management NOT a static bureaucratic document, but a part of every day life when on site.

### ***Background documents***

- *Purpose* – overall purpose of the project
- *Context assessment* – which may also be a programme document

### ***Threat/vulnerability/risk assessment***

*Threat/vulnerability/risk assessment* – updated to reflect changes in the environment

*Analysis summary* – a summary of the type, level and trends in the operating environment.

***Standard Operating Procedures*** (preventive routines, best practice given the context, mission and mandate)

These may include areas such as:

- Phases of security alert
- Staff conduct
- Incident reporting and analysis
- Vehicle movement
- Landmines
- Checkpoints
- Communications
- .....

***Contingency Plans*** (*reactive measures – WHEN THE WORST HAPPENS*)

- Medevac
- Staff death
- Staff assault
- Staff disappearance
- Abduction/kidnapping/hostage situation
- Natural disaster
- Bomb threat
- Evacuation/Relocation/Hibernation
- .....

**Support Documents** (*resources to make it happen*)

- Personnel roster, addresses, telephone numbers and passport numbers
- List of cooperating organisations, contact people, telephone numbers, radio frequencies
- List of support resources (fire, medical, security, transportation, utilities, immigration, finance) and appropriate contact people
- Maps indicating assembly points, roads, airfields, checkpoints, border crossings
- Emergency supply inventory (food, clothing, medical, documents, currency, etc.)
- Standard forms *e.g. incident report forms*
- Warden system, communications tree
- Insurance details

## Emergency Procedures Post Security Incident

This checklist may not be complete and need not necessarily be followed in this order, but will give guide-lines for actions.

- Give First Aid
- Secure area, apply life-saving measures;
- Gather information;
- What? Where? When? Who? by Whom? How? (Incident Report);
- Source of information?
- Reactions from officials, other agencies and local people?
- Inform Senior/Supervisor/HQ (oral information followed by written report);
- What happened;
- Actions and decisions taken;
- Any immediate follow up action to be taken;

## Post Incident Reporting Form

Completing a form such as this will assist in understanding and analysing incidents. It is also useful when reporting to the insurance provider.

Report :

### **POST INCIDENT REPORT (PIR)**

(All persons involved in the incident should complete one PIR each)

**Type of incident IE: Traffic Accident/Ambush/Robbery etc:**

.....  
.....  
.....

**Exact Geographical Location of the incident & description of physical location.**

.....  
.....  
.....  
.....

**Identification of ALL people involved (including witnesses)**

.....  
.....  
.....  
.....

**Comprehensive description of the Incident including Injuries and damage**

.....  
.....  
.....  
.....  
.....  
.....  
.....  
.....  
.....  
.....

Continue on separate sheet if required. You may find it useful in some cases to additionally draw a diagrammatic representation.

**Actions taken, Decisions made and by Whom.**

.....  
.....  
.....  
.....  
.....  
.....  
.....  
.....  
.....

**Responses by others (Other agencies, HQ etc)**

.....  
.....  
.....  
.....  
.....





## **Cultural Issues checklist**

### ***Time***

Different concepts of time can create misunderstandings, particularly in the work context.

- How important is “time” and what is the primary “time focus” (i.e. past, present, future)?

### ***Space***

Attitudes to physical space and distance often cause misunderstandings, discomfort or offence.

- What is the “comfortable” distance between people - is it important?
- What space is “private” or “public”? (e.g. is the office private; are meetings held in public; what does a closed door mean?).

### ***Physical contact***

- Physical contact acceptable? What, how, where, when and how much? (for example, kissing, shaking hands, holding hands; in public or private).
- Are there any taboos for certain parts of the body?
- Does physical contact have implications for medical practice?

### ***Communication***

Apart from the obvious barrier of language, attitudes towards communication and transferring information can often cause difficulty or frustration.

- Is the importance of open and frequent communication valued?
- How is communication carried out? (e.g. is it acceptable to ask direct questions? Is secrecy welcomed?).

### ***Body language***

It is very easy to send (or receive) the wrong message, or to cause offence.

- What are the normal gestures? Are they similar in meaning to your own? (e.g. does nodding your head mean ‘yes’ or ‘no’?).
- What is the attitude to eye contact?
- How does one show respect non-verbally?
- How does one greet another? Who does one greet?

### ***Dress***

- What is the attitude to wearing clothing in different situations (e.g. do you need to wear a hat/veil in public? Do you remove shoes when inside a room?).
- Are there any parts of the body which should be covered?
- How will your clothing affect the people you meet?

## ***Gender***

Attitudes to men and women, particularly in the work place, can vary significantly.

- Who normally does what type of work?
- How will your gender affect the people that you are working with, and your work? (e.g. if you are a woman, you may have to be treated as an “honorary male”).
- Are there any significant taboos relating to gender? (e.g. attitudes to eating).

## ***Age***

Attitudes towards age and seniority vary. This is not something that you can do much about, but it can explain why you have more or less respect in different cultures.

- Is age seen as important for status and seniority?
- Are there different ways of behaving with different ages?

## ***Emotions***

- What emotions can be shown and when?
- How do people react to emotive situations?
- What feelings can be discussed openly?

## ***Relationships***

- What does “friendship?” mean?
- How important are good relationships at work?
- Are there any rules for socialising after work?
- What are the attitudes towards sexual relationships?

## ***Respect & politeness***

- Who should be shown respect and how?
- What are the basic rules of politeness and decency?

## ***Religion***

- Is religion important during day-to-day life? What religions?
- How does religion affect working practices?
- How will religion impact on your work and standing?

## ***Authority and status***

Attitudes to authority and status will affect who you work with and the way that you work with them.

- How is authority and status derived?
- How is the “boss” viewed in the culture? (e.g. unapproachable and distant).
- How are “foreigners” viewed in the culture? (e.g. as experts; as interference).
- Are the systems clearly defined in the work place? (e.g. rigid; adherence to protocol).

### ***Decision making***

This will relate to attitudes towards authority and hierarchy.

- How are decisions taken? (by consensus or decree?).
- What importance is given to consultation before decisions are taken?
- How is responsibility viewed?

### ***Loyalty and trust***

Cultures differ in the importance they give to loyalty and unity. Attitudes towards the nature of people will vary, and this will affect the level of trust.

### ***Attitude to nature and work***

- What is the relationship between man, nature and the world? Is man or nature dominant? (e.g. "It can't be helped."; "If God is willing."; "Can do.>").
- What respect is accorded to natural resources or places?
- What importance is placed on work? Why? What is the relation between work and play?
- Can humans influence their life, take risks or chances?

### ***Law***

- What is "law" and what importance is attached to it?

## Health precautions checklist

- 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 an insecticide-impregnated 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
- Vaccinations against serious diseases. Some countries do not admit foreigners without a certificate of vaccination for certain diseases.
- 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. Your local partner or 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
- **In case of risk of exposure to HIV**
  - **DON'T PANIC.** The risk of transmission to healthcare workers is low.
  - Wearing gloves removes 60% of blood on a needle in a 'needle-stick' incident.
  - Wash the area of injection thoroughly using soap and water. If the eye or mucosa was splashed then rinse with copious amounts of water. Consider whether the patient is known to be HIV positive. This will rarely be known. If it is not then it is unlikely to be possible to persuade them to agree to counselling and a HIV test to verify their status.
- **Post Exposure Prophylaxis (PEP)**
  - **You may want to consider making these available for staff, or liaising with a local medical provider that can supply these.**

## 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

## **Stress Checklist**

### **Causes of stress**

The causes of stress may include many things, such as:

- Personal loss
- Overwork, or high-pressure work environment
- Lack of clarity about responsibilities or expectations
- Job insecurity
- Trauma
- 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
- Rapid resolution of any grievances or complaints
- Sufficient rest, including a weekly day off, and enforced Rest and Recreation in periods of high pressure. 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.
- Access to personal e-mail, where possible
- Privacy in living accommodation
- Ensuring staff have access to little luxuries, such as books, magazines, videos, good quality soap
- Eating properly, with a variety of nutritious food.
- Building team spirit & friendships
- Exercise
- Recognition, praise and reward for good work
- Adequate pay
- Secure home environment

### **Signs of stress**

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.

Common signs of stress 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
- Extended fatigue
- Disrupted sleep or oversleeping
- Over- or under-eating
- Overuse of alcohol or use of drugs

## Checklist to mitigate risks of own transport

- ❑ Seatbelts to be worn at all times
- ❑ All vehicles equipped with appropriate safety equipment
- ❑ Vehicles checked daily
- ❑ Vehicle logbooks maintained for each vehicle and contain a copy of the checklist and maintenance schedule and all vehicle documentation
- ❑ All drivers carry appropriate documentation including drivers licence.
- ❑ Drivers observe local driving laws and regulations and drive at appropriate speeds for the conditions.
- ❑ Vehicle fuel tanks are maintained above ½ full where possible
- ❑ Spare vehicle keys are kept in a safe location.
- ❑ Notification is made of travel time and destination. Procedures in place if arrival is not as scheduled
- ❑ No unauthorised passengers are carried
- ❑ Vehicle doors are kept locked when driving
- ❑ All drivers capable of performing basic maintenance such as changing tyre, vehicle checks etc.
- ❑ Vehicle accident and incident procedures and reporting policies in place and communicated
- ❑ Updated country and regional roadmaps available
- ❑ Primary and alternative travel routes are selected to avoid hot-spots and provide the safest journey possible
- ❑ Where travel is to a new or high risk area contact is made with relevant parties (UN/other organisations/authorities/partner agencies/etc), prior to departure to ensure updated information on context, risk safety and security.
- ❑ Vehicles have extra water and fuel prior to long trips
- ❑ A first aid kit is maintained in each vehicle
- ❑ For long trips, emergency stocks of food, blankets, torches etc should be carried.
- ❑ Mobile phones are fully charged prior to travel. Alternate mean of communication is carried whenever possible.