

Stay safe

The International Federation's
guide for security managers



International Federation
of Red Cross and Red Crescent Societies



Strategy 2020 voices the collective determination of the IFRC to move forward in tackling the major challenges that confront humanity in the next decade. Informed by the needs and vulnerabilities of the diverse communities with whom we work, as well as the basic rights and freedoms to which all are entitled, this strategy seeks to benefit all who look to Red Cross Red Crescent to help to build a more humane, dignified, and peaceful world.

Over the next ten years, the collective focus of the IFRC will be on achieving the following strategic aims:

1. Save lives, protect livelihoods, and strengthen recovery from disasters and crises
2. Enable healthy and safe living
3. Promote social inclusion and a culture of non-violence and peace

2011 – Third edition

International Federation of Red Cross and Red Crescent Societies

P.O. Box 372
CH-1211 Geneva 19
Switzerland

Tel.: +41 22 730 4222
Fax: +41 22 733 0395
E-mail: secretariat@ifrc.org

www.ifrc.org

© International Federation of Red Cross and Red Crescent Societies

Any part of this handbook may be cited, copied, translated into other languages or adapted to meet local needs without prior permission from the International Federation of Red Cross and Red Crescent Societies, provided that the source is clearly stated.

The International Federation of Red Cross and Red Crescent Societies would like to express its gratitude to the following for committing to and supporting this publication:



Finnish Red Cross



MINISTRY FOR FOREIGN
AFFAIRS OF FINLAND



Norwegian Red Cross



Icelandic Red Cross



Canadian Red Cross



Foreign Affairs and
International Trade Canada



NEW ZEALAND RED CROSS



SwedishRedCross
by government funding

All cartoons by Pierre Wazem, 2007

Contents

Acknowledgements	4
Foreword	5
Introduction	6
Chapter 1 Security management	7
Roles and responsibilities	7
Roles and responsibilities of the security unit at the Federation secretariat	8
Roles and responsibilities of field managers	9
Roles and responsibilities of security delegates	10
International Federation and Participating National Society interaction	11
The International Federation's security management process	11
Situational influences	12
Assessment	12
Planning: security strategies and plans	13
Implementation and security management	13
Review/evaluation	15
Information management	15
Briefing and debriefing	15
Chapter 2 Situation assessment	19
Determining risk	20
Situation analysis	20

Threat analysis	23
Vulnerability analysis	23
Risk assessment	25
Chapter 3 Security planning	29
Exit plan	31
Security strategies	31
Security regulations	32
Contingency planning	33
The contingency planning process	34
Relocation plans	35
Operational security phases	41
Security guidelines and advice	48
Welcome pack	48
Security briefings and debriefings	48
General security debriefing	49
Incident debriefing	49
Chapter 4 Incident management	51
Incident reporting	51
Defining a security incident	52
Examples of security incidents	53
Using the security incident report form	54
Incident analysis	54
Identifying trends	55
Critical incident management	56
Defining a critical incident	56
Critical incident management team	57

Stage 1. Establishing what happened	59
Stage 2. Analysing the situation	60
Stage 3. Option analysis	61
Stage 4. Implementation	63
Stage 5. Review/follow-up	63
Conclusion	65
Incident Log Template	66
Chapter 5 Working with the military	67
Using military assets	68
Guiding principles	70
Always consider	71
Absolute limits	71
Using armed escorts	72
Chapter 6 Using guards	75
Considerations prior to employing guards	76
Red Cross and Red Crescent image	76
Background information	76
Contractual issues	77
Maintenance services	78
Guard selection criteria	78
Minimum training standards	79
Equipment	80
Other considerations	80
Raising the alarm	80
Managing guards	81
Guard procedures	81
Access control procedures for visitors	81
Logbook maintenance	82

Area of control and patrol instructions _____	82
Guards' reporting lines and supervision of guards _____	82
Guards' responsibility in case of emergency _____	82
Armed guards _____	83
Policy issues _____	84
Services _____	84
Training _____	84
Contractual issues _____	84
Annexes _____	87
1 – Minimum security requirements (MSR) _____	87
2 – Security incident report _____	97
3 – Critical incident planning consideration _____	99

Acknowledgements

We would like to acknowledge the contribution made by our field managers, security delegates and various Federation colleagues both in terms of content contribution and advice, and also for their time in reviewing the draft text. In particular, we would like to acknowledge the contribution made to security within the International Federation by Tor Planting, whose efforts and drive led to the establishment of the security unit.

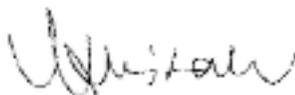
This security guide was prepared and written by Lars Tangen, John Dyer and Karl Julisson from the security unit of the International Federation of Red Cross and Red Crescent Societies. We would like to extend our appreciation to the publication team of the International Federation secretariat for their efforts on the layout as well as for organise all the additional work to make this book happen.

Foreword

The International Federation finds itself working increasingly in natural disasters and in areas with complex political and social circumstances that change rapidly and can have an impact on its humanitarian operations. As security risks are generally higher for those based in the field, promoting basic security awareness is important to ensure the safety and well-being of all Red Cross and Red Crescent personnel, whether they are Federation-employed delegates, staff-on-loan, local staff during working hours, volunteers working with the International Federation, visitors, consultants or family members accompanying delegates.

Although the degree of risk varies from country to country, it is important to understand that security incidents can occur in *all* operational areas. Worryingly, a rising number and range of threats are being faced every day by humanitarian workers throughout the world, increasing their personal vulnerability. In order to fulfil their humanitarian mission, Red Cross and Red Crescent personnel must *always* follow basic security rules and act appropriately in any given situation.

Understanding the different types of security situation you may face in the field and how to behave in order to minimize risks to your safety and that of your fellow colleagues is vital to staying safe in the field. Aimed at Red Cross and Red Crescent personnel, *Stay safe: The International Federation's guide to a safer mission*, together with the accompanying publication, *Stay safe: The International Federation's guide for security managers*, provide the necessary tools to implement and maintain a well-functioning security framework, adapted to the specific context, in each of the International Federation's operational areas around the world.



Markku Niskala
Secretary General

Introduction

The International Federation, through its senior field managers, has an obligation to ensure its operations are conducted within an effective security framework. This requires managers to understand the environment they are operating in, conduct a robust risk assessment and develop sound security plans that mitigate those risks. It is not sufficient however to simply develop plans; managers must then implement and oversee operations in accordance with this plan. This requires all personnel to understand not only the security programme itself but also the rationale behind it and therefore the requirement to operate within its parameters.

It must also be recognized that the environment can change and with this the threat picture. Plans must therefore be reviewed and adjusted to address these changes. Security will be most effective when field managers establish a security culture within their operations, where security becomes an integral element of the entire operation and not an 'add on'.

The security unit has written this manual with the aim of providing maximum usefulness and easy reference to assist managers to establish an effective operational security framework. As such, the manual – complete with annexes and supporting documents available from FedNet and the security unit's security management course – should provide you with a useful and effective toolkit enabling you to operate safely in the field.

Keep it within easy reach – and stay safe.

If you have any questions, comments or issues, do not hesitate to contact us in the security unit at security.unit@ifrc.org.

The security unit can be reached 24 hours a day, seven days a week, on the following numbers:

- Lars Tangen (Manager) – Mobile: +41 79 217 3371
- John Dyer (Security Coordinator) – Mobile: +41 79 251 8015
- Karl Julisson (Security Coordinator) – Mobile: +41 79 308 9842



The International Federation's approach to security is one of prevention. This can only be achieved through effective security management. Primarily, security management is about determining the risks facing the operation, developing effective security plans that will mitigate these risks and then implementing the plans in the best possible way.

In order to ensure that the organization fulfils its responsibility to create an operational environment that is as safe as possible, while at the same time enabling its humanitarian mandate to be achieved, a set of minimum security requirements (MSRs) has been established. These MSRs outline the key requirements that must be included in security plans, while reinforcing the implementation of the layered security framework that has been adopted.

The minimum security requirements are applicable to all operations of the International Federation and are provided in full in Annex A. This chapter outlines individual roles related to security management, the processes involved and the importance of information management and briefings.

Roles and responsibilities

The following diagram illustrates the current security management structure at the International Federation.

Security management structure



Roles and responsibilities
of the security unit at the Federation secretariat

...towards field-based staff

- monitoring security situations worldwide and disseminating relevant information to Federation staff (e.g., through the weekly HotSpots report and security updates)
- providing advice on all security-related matters and making guidance materials available on FedNet¹
- conducting security training and workshops
- briefing and debriefing delegates passing through Geneva
- supporting field managers in creating and updating security rules and regulations, including all related procedures
- conducting security assessments and undertaking troubleshooting missions when required
- assisting the handling of critical incidents, security incidents (during and after), relocation and medical evacuation of staff in the field
- being available 24 hours a day, seven days a week

¹ FedNet is the International Federation's extranet site, a private web site for sharing information between National Societies, Geneva-based staff and country and regional representatives in the field. It can be accessed via the internet by all Red Cross and Red Crescent personnel. The security unit maintains a section on FedNet, accessed through the Security tab on the home page or at <https://fednet.ifrc.org/sw99042.asp>.

...towards staff at the Federation secretariat

- supporting managers and National Societies on all security-related issues
- managing crises and critical incidents
- serving as the focal point for all security-related issues
- providing briefings and debriefings to delegates and new staff
- conducting workshops and training on security matters
- maintaining external relations and cooperation with other agencies and organizations at headquarters level
- giving support to member Red Cross and Red Crescent National Societies on all security-related issues
- being available 24 hours a day, seven days a week

The security unit's role is to advise and assist Federation managers, both in Geneva and in the field, to ensure that security management is appropriate and functioning at all times.

Roles and responsibilities of field managers

- explicit responsibility for ensuring that effective security management is implemented in the delegation by ensuring that minimum security requirements are in place and respected
- creation of a security plan based on a threat, vulnerability and risk assessment that includes – but is not limited to – security regulations, security guidelines, contingency plans and emergency procedures, as well as ensuring this plan is up to date for the given situation
- ensuring copies of all security rules and contingency plans are provided to the Federation secretariat
- ensuring that all new staff, dependants and visitors are briefed on the security plan and provided with a copy of security regulations immediately upon their arrival
- maintaining a high awareness of security issues within the operation by including security on the agendas of all internal meetings and sharing security-related information with all delegates
- ensuring the integrity of the International Federation by promoting correct institutional and personal conduct and behaviour as outlined in the Code of Conduct
- ensuring that additional training on driving, mine awareness, first aid, fire safety, radio communication procedures, etc., is available at the delegation

- immediately reporting any security incidents to the security unit in Geneva
- being aware of and mapping security/safety incidents that occur in the area of operation, even if the Red Cross or Red Crescent is not involved
- establishing a rest and relaxation (R&R) system if needed, and ensuring that staff are aware of the psychological support options available to them if required

Roles and responsibilities of security delegates

- constantly monitoring the security situation in the area
- advising the head of delegation or senior manager in the field of the need to update the operation's security plan whenever the situation changes
- reporting to the head of delegation or senior manager in the field if the MSRs are not being respected
- maintaining a security information network
- giving security briefings and debriefings to delegates and visitors
- providing reports on security to the field managers and the security unit in Geneva
- reporting and following up on any security incidents
- providing support to the head of delegation or senior manager in the field, the operation's personnel and Participating National Societies (PNSs) working bilaterally
- being available 24 hours a day, seven days a week

International Federation and Participating National Society interaction

As mentioned in Chapter 1 of the accompanying publication, *Stay safe: The International Federation's guide to a safer mission*, entitled Security framework, there are basically two options for the security management of PNSs and their delegates:

1. To have totally independent security management (i.e., they are entirely responsible for their own security).
2. To be fully integrated into the security management of the International Federation's delegation. In other words, the PNS agrees to subordinate security management to the International Federation.

Managing PNS security

If a PNS elects to be fully integrated into the International Federation's security management and signs an agreement to this effect, then the senior field manager (usually the head of delegation) must include the PNS's operations and personnel within his or her security planning, just as with any other element of the International Federation's operation. This means that:

- PNS personnel must be provided with and briefed on security regulations and plans
- appropriate security measures must be taken to safeguard PNS personnel and assets
- contingency planning must include provisions for the PNS
- the PNS has access to technical security advice and support

In return, PNSs are to:

- ensure that operations are structured in accordance with the MSRs, and that their personnel abide by all security regulations and procedures
- provide updated records of personnel and their location
- provide regular updates of their operational status and advise of any changes they may make

The International Federation's security management process

The security management process is the means by which managers establish and implement an effective security management framework that mitigates the risks facing the International Federation. The following diagram illustrates the various stages of the process.



Situational influences

Security management is influenced by the situation within which the International Red Cross and Red Crescent Movement operates. These influences can be both internal and external, and can impact on all aspects of the management process. Managers must understand these influences and determine what impact they may have on decision-making and the management process.

Assessment

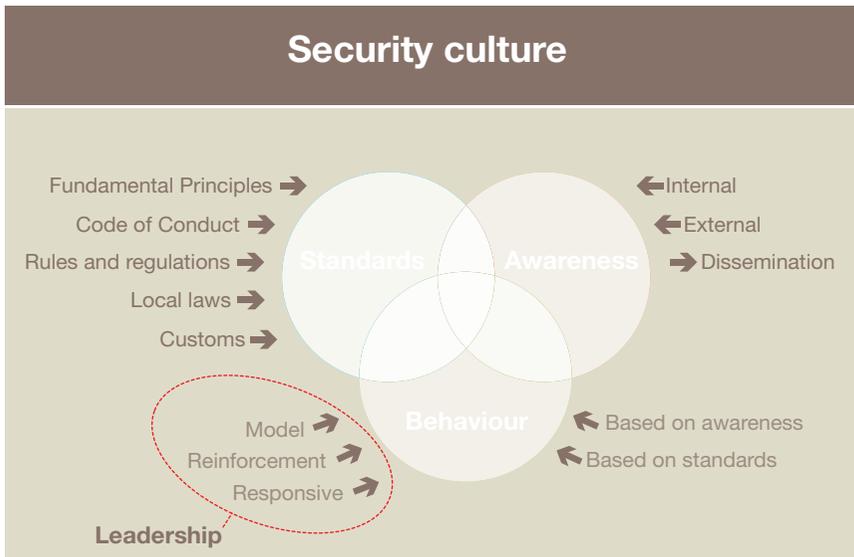
Assessment involves a logical analysis of the situation to identify the potential threats and the International Federation's vulnerability to those threats. Once a threat and vulnerability analysis has been completed, the impact of the threat and the probability of it affecting the organization are plotted on a risk matrix. The risk matrix enables risks to be prioritized, while actions are identified to mitigate them. These actions are used to form key components of the security plan. Determining risk is covered in more detail in Chapter 2 of this manual.

Planning: security strategies and plans

A security plan is an essential tool for developing and maintaining adequate security procedures and responses. The first phase of security planning is to identify and determine how the three security strategies (acceptance, protection and deterrence) can be utilized and implemented. The plan must relate to the specific operational situation and will comprise a number of components including: security regulations and guidelines; briefing and debriefing procedures; contingency planning; critical incident management. Formulation of the security plan should be conducted using input from all personnel within the team. Security planning is covered further in Chapter 3.

Implementation and security management

Implementation of the security plan and management of security is, perhaps, the most difficult part of the process. A key part of this process includes personnel being aware of all aspects of the plan as well as their roles and responsibilities within it. Routine management involves ensuring personnel operate within the framework of the plan. However, managers must also be able to deal with incidents and areas that can occur outside the routine. These aspects of the process are made easier thanks to contingency planning and established incident management procedures.



Security management is made easier when security is seen as an integral part of the operation – and not as an additional element. This means that the organization or an operation has a developed security culture, where security is automatically considered part of the overall planning and management process. This simply means that people behave in a manner consistent with established operational standards. This can be represented as follows:

Many of the elements in this model involve procedural aspects of management. However, to be truly effective, a senior manager in the field must also lead. The model contains three key components of effective security leadership:

1. Model

You must be seen as the model that your staff aspire to. This means:

- being seen to be setting standards
- not being compromised
- being approachable so that staff feel they can come to you with issues of concern; otherwise, you will not be informed of potential security incidents that are just waiting to happen

2. Reinforcement

- positive rather than negative reinforcement; it is always easier to correct mistakes (negative reinforcement), but stronger lessons are learnt by acknowledging correct behaviour
- making security part of your everyday management
- demonstrating flexibility and not being perceived as draconian in your approach, but rather as being prepared and able to consider all aspects of a situation

3. Responsive

- Be decisive and remember that you are the manager and should, therefore, act within your level of accountability without simply delegating upwards in order to avoid making an unpopular decision.
- Security management must be a dynamic process and if there are clear lessons learnt from operations, then you should be prepared to modify the way things are done.

Review/evaluation

Security plans must be monitored and continually evaluated to ensure their relevancy. This should occur as a matter of routine at least every six months, but also whenever there is a change in the situation on which the plan was based, or if the analysis of security incidents highlights any gaps in the plan. To enable this process to occur, it is vital that managers ensure constant monitoring of the situation and are aware of any changes to their environment.

Information management

Good information management is vital in any operation, whether or not the area concerned is at high risk. During times of heightened security, the efficient gathering, processing and distribution of information will be critical to ensure the well-being and safety of field-based staff.

Basic activities that will contribute to beneficial information management with regard to security include:

- regular external liaison with ICRC, the UN, non-governmental organizations, embassies and other institutions working in the country/region
- attending security meetings that are being held in the area of operation, and, if possible, obtaining regular security situation reports or operational updates
- regular information-sharing meetings with the host National Society and Participating National Societies
- obtaining information and news via other means (e.g., the internet, local news, etc.)
- using the weekly HotSpots report provided by the security unit to update yourself on the security situation in your area and the wider region

Briefing and debriefing

In general, all Red Cross and Red Crescent staff should have received some sort of introduction to the topic of security prior to their mission assignment (e.g., while attending their



basic training or induction course). Individualized briefing will also be provided by the secretariat-based security unit if the delegate travels through Geneva for briefing prior to starting a new mission. Senior managers in the field must also ensure that new staff are briefed on arrival in the country of assignment.

The objectives of a briefing session are to:

- provide a background on the history of the country, including the National Society, and the International Federation's involvement there
- provide an update on the current security situation, including previous security incidents (these aspects can be provided in a welcome pack which may also include key MSR elements, security regulations, etc., for visitors who may not need the complete set of documents)
- introduce the International Federation's security management structure, highlight the MSRs, security rules for the delegation, relevant guidelines and other security issues
- stress the requirement for compliance with the Code of Conduct and security regulations
- identify the roles, responsibilities and expectations of field managers, security personnel and individuals in relation to security
- highlight the importance of personal security awareness.

The objectives of an end-of-mission debriefing session are to:

- identify any issues or areas within the security set-up that can be improved
- provide a reality check on how security management is perceived by staff
- discuss any specific security-related incidents that occurred



Remember! Debriefing should also be conducted directly following any serious security incidents involving Red Cross or Red Crescent personnel, or any incidents that might have impacted negatively on staff or operations.

Case study

In a large-scale Red Cross and Red Crescent operation in a country recently affected by natural disaster, delegates reside and work in close proximity to many of the beneficiaries. The same area is also a known holiday destination for Western tourists. The operation has experienced some difficulties and delays, which resulted in complaints by sections of the local population and beneficiaries about the perceived lack of progress in delivering assistance to the area.

After a hard day's work, delegates often go to some of the five-star hotels, restaurants and bars in the area to unwind. They use their Federation vehicles for transport and leave them parked outside these premises.

One delegate is usually appointed as the designated driver and only has a glass of wine or beer throughout the evening, and then drives the other delegates back home.

One night, when a group of delegates come out of a bar, a gang of boys aged between 12 and 13 grab a handbag from one of the delegates and run off into the backstreets.

What are the security concerns, if any, in this case study?

Security considerations to keep in mind

Acceptance issues – The image of the organization is potentially damaged by clearly identifiable vehicles being parked outside a five-star hotel when local beneficiaries are suffering and complaining about a lack of progress.

Low profile – By parking outside the bar, the delegates are presenting themselves as potential targets (i.e., they can afford to go to expensive places, therefore they must have things worth taking).

Zero tolerance – Zero tolerance means just that. The delegate chosen to drive should not drink at all. He or she is breaking security regulations and the Code of Conduct. Does the senior field manager accept this sort of behaviour? If the answer is yes, then a culture of security has not been established.

Don't risk your life – While it may be tempting to chase after the robbers, it is not known what is around the corner and, by giving chase, delegates would be taking a significant risk. This should be reinforced in security briefings and training.

1

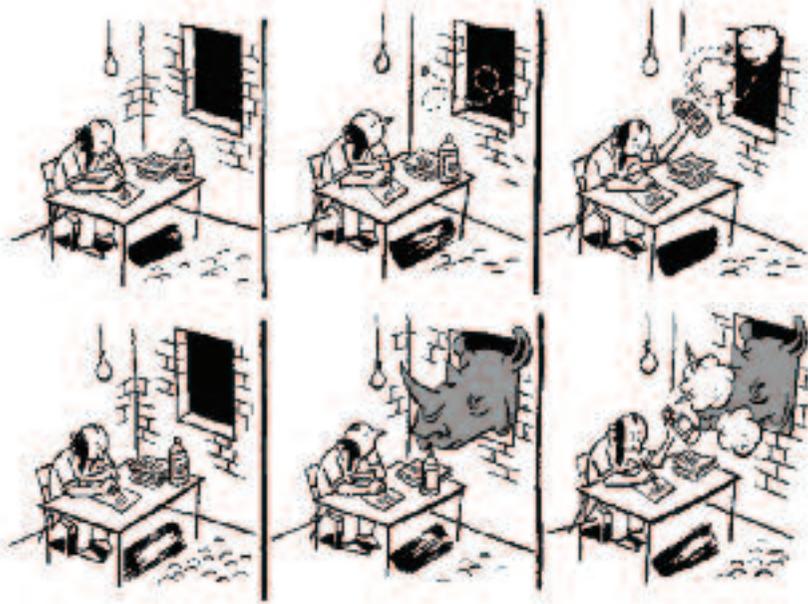
2

3

4

5

6



In the following chapter, we will discuss how you go about formulating security plans. However, before you can do this, you must complete a thorough analysis of the situation and environment you are working in. This involves identifying potential threats, your vulnerabilities, and then the consequent risks facing the operation. Some basic definitions are given here to clarify what is meant by the different terms used in the chapter.

A security threat is a potential act or danger in the operational environment that may cause injury or harm to staff and assets.

Vulnerability is the extent to which staff or assets are exposed to a threat.

Risk is the likelihood that a threat will happen to you.

threat + vulnerability = risk

In order to demonstrate these ideas in practice and to give you a concrete example of how a situation assessment can be conducted, a case study has been included on page 21 and will be referred to throughout the chapter.

Determining risk

Effective security management relies on determining the risks facing the operation, developing effective security plans that will mitigate these risks and then effectively implementing the plans. The various stages of the analysis process will be described, while a useful matrix is included to help you plan for potential risks in your operational area.

Situation analysis

Security management is influenced by the situation within which the Red Cross and Red Crescent must operate. There are both internal and external factors that



can influence all aspects of the management process. Managers must understand these influences and determine what impact they could have on decision-making and the management process. Situation analysis is, therefore, the first part of the

process of determining risk. The aim is to understand the risk environment by gaining awareness of the in-country context, the drivers, the potential implications and the indicators that we should be monitoring.

This involves an assessment of key factors that primarily affect the general security situation. The first to be considered are the external factors, which include:

- history and current dynamics of the country (include any regional influences)
- politics within the country or region and include any regional influences
- economy/resource base and infrastructure
- crime profile
- the likelihood and/or frequency that the country will be hit by a natural disaster
- military developments
- nature and structure of conflict or violence

Once you have considered all of the possible external factors, you should start to identify potential threats. Bear in mind that given the lasting effect that changes to any of these factors can have, they must be continually monitored.

A number of sources can be used to gather information on external factors and assist in analysing them. Typical sources could include:

- ✦ security incident reports
- ✦ National Society and Movement partners
- ✦ humanitarian agencies and government sources
- ✦ academics and local communities
- ✦ press, media or internet
- ✦ private security companies

In order to provide you with a practical example, the following case study will work through the process of conducting a threat, vulnerability and risk assessment.

Case study

Wainui is a nation of approximately 6 million people and is ranked low on the United Nations Development Programme's Human Development Index. The country lies in the tropics, north of the equator, and measures approximately 400 kilometres from east to west and 600 kilometres from north to south. Wainui's geography includes high mountainous areas that are difficult to access, valleys with great potential for agriculture, and tropical areas mainly covered by rainforest. The country has a coastline of approximately 300 kilometres with a deep-sea port in the capital, Baytown.

The roads are in a bad state and highly susceptible to the impact of natural disasters. The only international airport is in the capital. There are frequent flights between the capital and regional centres using ageing commuter aircraft. The national airline just avoided being included on the European Union's blacklist of unsafe airlines.

Political power has been in the hands of the National Social Party for the last 15 years. The party represents the interests of the upper and medium social classes, leaving the vast majority of indigenous people in the opposition. The most radical grouping is the Wainui Nationalist Movement (WNM), which, in the last 12 months, has started resorting to violence in a move to change the government. A number of attacks have been made on local police stations, while military convoys have been targeted in hit-and-run attacks, mainly at night. The underpaid police force is lazy, corrupt and cannot be relied on to follow up on general crime.

Regional health services are very poor and there has been a dramatic increase in the number of HIV-positive cases. Poverty has forced many to take extreme and drastic measures for their survival. Wainui has a very high crime rate. Prostitution, including child prostitution, is common in most parts of the country, particularly in the larger towns.

The disaster

An earthquake measuring 6.5 on the Richter scale recently struck the western part of the country.

The area affected has a population of approximately 30,000 and is located in the mountains some 1,500 metres above sea level and 200 kilometres from Baytown. According to officials, the earthquake left 300 dead and 500 injured, while 70 per cent of the buildings have collapsed. Food and safe drinking-water are urgent concerns. The lack of effective hygiene coupled with mass sanitation needs are the main health risks foreseen. There is one regional airport in the area capable of taking helicopters and general cargo aircraft with a maximum capacity of 6,500 kilograms.

After identifying the external factors, it is important to then identify any internal factors that will influence the situation. These may include:

- profile of staff in the operation (e.g., experience levels, gender composition, areas of expertise, etc.)
- activities that the operation is undertaking
- locations that staff are deployed to or need to deploy to
- current profile of the operation and the Red Cross and Red Crescent Movement in the country
- premises being used by the operation

Once these internal factors have been identified, you should also start to identify potential vulnerabilities.

The final aspect of situation analysis is to determine the other actors in the area and, in particular, their relationship to you and your operation. Principal among these will be other Red Cross or Red Crescent partners, ICRC, the host National Society and any Participating National Societies operating in the country. You need to determine whether the in-country image of the Movement is positive or negative, and what implications this may have – not just immediately, but also how you can develop it positively. Other areas for consideration will be:

- all actors relating to the delegation
- those with direct relationships with the delegation
- those with indirect relationships with the delegation
- determining the potential implications of the relationships identified

Threat analysis

Threats will have been identified during the situational analysis. The next step is to prioritize them on the basis of:

- ↘ frequency
- ↘ severity
- ↘ likelihood

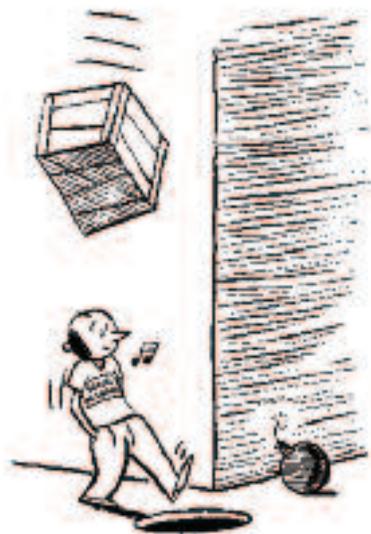


Remember! Assessments should be a continuous and proactive process. Existing threats must be evaluated to determine whether they have increased or decreased. New or potential threats must be identified and analysed. Both aspects may require the security management process to be adjusted.

Case study: identified threats

Using the background information provided for this case study, the following threats and their potential impact were identified:

- Road travel is potentially hazardous in the west – moderate to critical impact.
- The national airline has a poor safety record – potentially severe to critical impact.
- Potential health issues and poor health facilities in outlying areas – moderate to severe impact.
- High crime rate, particularly in towns and villages – moderate to severe impact.
- WNM attacks possible in remote areas at night – severe to critical impact.
- Buildings may be unsafe and collapse from earthquake aftershocks – severe impact.



Vulnerability analysis

Once you have identified the potential threats to security in the operational area, you must evaluate the delegation's vulnerability to these threats. Assess where and

why the delegation and its staff would be at greatest risk from the threats identified. The likelihood of impact is often determined by the:

- current attitudes within the country to international humanitarian organizations and the Red Cross and Red Crescent
- nature and structure of the delegation's operation (e.g., location of premises, distribution of staff and current procedures, planned activities, etc.)
- composition of the delegation including the number of staff, their nationalities and experience levels
- key working relationships with the government, partner agencies, the host National Society and with protagonists in any conflict situations

The assessment process should also evaluate how serious the impact of an incident resulting from a threat will be. This directly relates to determining your capacity to confront these threats and to determine the acceptable risk for your specific context.

Case study: Red Cross and Red Crescent response to the disaster

The Wainui Red Cross (WRC) branch located in the affected area immediately mobilized its relief team, comprising 30 volunteers, to provide rescue and first aid. The team, together with local residents and authorities, helped to rescue survivors of the earthquake.

WRC also helped local authorities to carry out a census and assisted in establishing temporary shelters. Based on this assessment, WRC asked the International Federation to launch an international appeal to help 20,400 people (3,400 families) in the emergency and rehabilitation phases. The priorities of the appeal were to provide sanitation, water, food, temporary shelter and permanent housing.

Recognizing that there is a need for greater information on the requirements of those affected by the earthquake, the International Federation assembled and deployed a Field Assessment Coordination Team (FACT). Given the urgent needs of the population, a number of Emergency Response Unit (ERU) deployments are being considered, including a relief ERU, logistics ERU, water and sanitation ERU, and a basic healthcare ERU.

A threat and vulnerability assessment can be conducted in different ways, but they all should answer the following questions:

Why?

could an attack happen (crime, political reasons, ransom, revenge)

Who?

poses the threat (criminals, army, armed factions, fanatics, dissatisfied workers, beneficiaries)

What?

are the likely targets (expatriate staff, visitors, family members or local staff)

How?

could an attack happen (weapons, ambush, bombs, robbery, hostage taking)

Where?

are we most vulnerable and where are the likely locations for any attacks

When?

could an attack happen and when does the possibility of an attack increase

Case study: vulnerabilities identified

- movement of relief stocks by road potentially dangerous due to the state of the roads and possible attacks at night
- vulnerable to activist elements in the community if there is a lack of communication with beneficiaries
- vulnerable to various health threats if reliance is placed solely on poorly resourced local health facilities
- vulnerable to high levels of crime, particularly in towns and villages
- vulnerable to WNM attacks if linked to government authorities, or located close to police stations or military facilities
- vulnerable to building collapse if offices or residence are located in a locally available building

Risk assessment

Having analysed the threats and vulnerabilities, the final stage is to assess the risks represented by a combination of these two elements, remembering that:

$$\text{threat} + \text{vulnerability} = \text{risk}$$

A useful tool for assessing risk is a risk-planning matrix, which is illustrated on the next page and which is available as a template in an electronic format on FedNet or from the security unit. This requires that various threat scenarios be plotted on the matrix

according to their likelihood of occurring. The potential impact they may have is clearly determined by the vulnerability of the operation. From this, we can assess the level of risk that the various scenarios present, ranging from low to extreme.

Each country and individual operation will be different. The threats and vulnerabilities will therefore be context-specific, as the risk will also be specific to a particular operation. However, in order to provide an example of how the matrix could be used, some threat scenarios have been inserted in the example shown here.

Risk-planning matrix

		Impact				
		negligible	minor	moderate	severe	critical
Likelihood	certain/ imminent					
	highly likely			Road traffic accident – major injury	Building collapse	
	likely				Burglary, theft, robbery	Attack by WNM at night on roads
	possible					
	unlikely					

Extreme risk: Immediate action required – Is the risk acceptable? Can it be mitigated by contingency plans? If so, they must be tested and rehearsed.

High risk: Priority action – Contingency plans developed and tested.

Moderate risk: Requires heightened awareness and specific procedures.

Low risk: Managed by routine procedures and covered in normal security regulations.

Descriptor	Definition
Certain/imminent	Will occur/ongoing active threat
Highly likely	A very high probability of occurring
Likely	A high probability of occurring
Possible	A reasonable probability of occurring
Unlikely	Unlikely to occur to Red Cross or Red Crescent
Descriptor	Definition
Critical	Death/severe injury/loss of vital equipment/ cancellation of activities
Severe	Severe injury, possible death/loss of important equipment or loss/major disruption to activities
Moderate	Injury/loss of equipment/delay in activities
Minor	Possible injury/possible equipment loss/ limited delay in activities
Negligible	Minor disruption to activities

Using a risk-planning matrix will enable you to identify risks, from the most serious to those that will have the least impact. These can then be taken into account when developing the security plan for your delegation.

A key aim of the security plan must be to reduce or to mitigate the risk to an acceptable level. From the matrix, it should be obvious that this can only be done by reducing the likelihood and/or by reducing the impact.

How to reduce the likelihood

- Avoid operations in certain areas (remove the threat).
- Acceptance level of Red Cross and Red Crescent is high.
- Communication and active dissemination with local communities.
- Operate transparently and in accordance with the fundamental principles.
- Behaviour is in line with regulations.
- Train staff in Movement principles, behaviour, use of vehicles and equipment, etc.
- Keeping visibility appropriate to the security situation (high versus low).

How to reduce the impact

- physical measures (such as 'hardening the shell' on Federation premises).
- training staff and conducting drills
- rules and guidelines that are appropriate to the context
- contingency planning



Case study: risk mitigation

Looking at the examples inserted in the risk-planning matrix, some options to be included in the security plan to mitigate the risks associated with each of these might be as follows:

Road traffic accident – major injury

- **Likelihood** could be reduced by avoiding operations where road conditions are dangerous, employing local drivers who know the conditions and establishing driving rules.
- **Impact** could be reduced by providing training for driving, having strict movement control procedures and formulating a medical evacuation plan.

Attack by WNM

- **Likelihood** could be reduced by focusing on acceptance and neutrality, avoiding operations at night and locations close to government premises.
- **Impact** could be reduced by hardening of premises, implementing a security phase system and sound relocation plan, as well as close monitoring of the situation.

Building collapse

- **Likelihood** could be reduced by ensuring buildings are checked by an engineer before occupation, using temporary accommodation (tents) located away from buildings until they can be certified as being safe for use.
- **Impact** could be reduced by carrying out good earthquake drills, teaching people to leave buildings quickly and in an orderly manner.

Crime

- **Likelihood** could be reduced by having good site security measures, employing guards and ensuring that staff maintain high security awareness.
- **Impact** could be reduced by having a guard response capability and ensuring a redundancy capacity in vital equipment.



Security planning broadly encompasses all the work that goes into ensuring effective field security. The assessment of threats facing your particular operating environment – discussed in the previous chapter – was one of the first steps in the security planning process.

In this chapter, we will show you how the information gathered in the assessment is converted into a security plan specific to the operational environment. We will also outline the main elements to be included in each component of the security plan.

In line with the International Federation's preventative approach to security, which aims to eliminate unnecessary risks, your security plan provides a detailed map of how to address the threats revealed by your security assessment. Security strategies are expressed through each delegation's security plan.

A security plan will, therefore, not normally comprise a single document, but will instead consist of a number of components, typically including:

- security strategies
- security regulations
- contingency plans

- operational security phases
- security guidelines and advice
- welcome pack
- security briefing and debriefing programmes
- critical incident management plan

A key aspect of security planning is awareness. Every staff member must know what is expected of them, what the rules are and how to implement procedures in emergency situations. The limits should be clearly defined and consistent guidance must be provided for everyone to ensure that each employee has a full understanding of the boundaries, as well as the penalties for overstepping those boundaries.

When formulating a security plan, the various threat levels (see operational phases on page 21 for more details) and a method for prioritizing potential security measures must also be discussed.

In areas where the International Committee of the Red Cross (ICRC) is also operating, the International Federation should coordinate security planning with ICRC, although each organization should have its own security plan. The International Federation's senior manager in the field (usually the head of delegation) has ultimate responsibility for all Federation personnel. Regularly scheduled meetings should take place between the International Federation, ICRC and the host National Society regarding security.

If Participating National Societies are working bilaterally in your area, they should be encouraged to operate under the International Federation's security umbrella and be fully briefed on all security-related matters. If a Participating National Society comes under the Federation security management then it should be included in contingency plans. Awareness of the location of Participating National Society operations and their field-based staff (including residence details and contact information) must be maintained and regularly updated.



Remember! Security planning is not a static process and it must always be revisited, especially after any security-related incident in your operational area or if new threats have been identified or changes relating to existing ones occur.

Exit plan

It is important when planning to also consider an exit plan as no operation will last indefinitely and, at some stage, the International Federation must plan to withdraw or at least scale down its operations. Security needs to be considered in this planning, and, while the plan must be specific to the situation, a number of key aspects must also be considered. These include:

- **Dissemination** – The fact that the operation is being scaled down or is closing down should be announced and reiterated early on so that beneficiaries know what is happening, otherwise it will cause ill feeling and could result in threats and security issues.
- **Local staff** – You have an obligation to your local staff and, as a good manager, you should keep them updated of your intentions to scale down or close down.
- If there is a requirement to move assets from outlying areas to the central office, then this must be carefully planned and movement procedures must be applied and followed.
- If equipment is to be disposed of in-country, then ensure correct procedures are applied in accordance with logistics procedures to avoid any accusations of corruption, etc.
- If equipment is to be handed over to the host National Society, then ensure correct procedures are followed.
- As the operation starts to wind down, a reduction in staff will mean a reduced capacity to observe. It is, therefore, important that those remaining have a heightened level of security awareness.

Security strategies

The three security strategies were outlined in Chapter 1 of *Stay safe: The International Federation's guide to a safer mission*, Security framework. To summarize, they are:

- 1. Acceptance** – Reducing or removing the threat by gaining acceptance for our presence and work. Acceptance cannot be assumed: it has to be earned and actively maintained.
- 2. Protection** – Reducing the risk and not the threat by using protective procedures and devices – ‘hardening’ the target.
- 3. Deterrence** – Countering threats with legal, political or economic sanctions and/or armed actions that may remove elements of the humanitarian aspect and reduce the level of acceptance.

While security planning will typically focus more on the acceptance strategy, an effective security plan will normally involve elements of all three strategies. It is important that security planning considers how the different strategies can be utilized to enhance the security plan. To do this, planners must clearly understand the differences between the various strategies and how they can influence the specific situation faced by the operation.

Security regulations

Although we know that the degree of risk will vary from country to country, security incidents can occur in all delegation offices. This is why all delegations are required to have written security regulations. Contingency plans for relocation and medical evacuation may be included as annexes to the security regulations or be drafted as separate documents.

The security regulations that you develop in the field and require all personnel to follow are specific to the context and working environment of your assigned operation and location. They should be clear, functional and up to date.

The International Federation takes the security rules very seriously and believes that security begins with a knowledge of procedures, strict respect for them and self-discipline by each and every staff member. Compliance with the security rules and regulations is mandatory for all personnel (including dependants), and any breach will be considered misconduct or gross misconduct. Disciplinary measures will be applied in cases where the security rules and procedures are not followed.

Security regulations must be defined as regulations, and not as guidelines which allow interpretation. Terminology should be directive in nature, using terms such as 'must' and 'are to', rather than 'should', 'may', etc. However, there are no universal rules for every situation. Events can be hard to predict in hazardous situations. The way the rules are applied in a given situation should always be based on common sense combined with the personal understanding that comes with local knowledge of what is going on at the time. For this reason, security regulations must be drafted for the specific situation facing the operation.

Security also depends very much on appropriate behaviour, as stipulated in the Code of Conduct signed by all delegates, accompanying family members and locally recruited staff. Security regulations complement the code of Conduct.

The senior manager in the field is responsible for the security of all Federation staff within the delegation, including Participating National Societies working under the International Federation's security umbrella. He or she must ensure the rules are understood and that all members of the delegation know what to do in the event of an emergency. All security-related incidents, no matter how small, must be reported to the senior field manager as soon as possible.

Security regulations should cover the following areas:

- » situation/threat assessment
- » general conduct/behaviour
- » field movement control
- » driving regulations
- » communications/radio
- » incident reporting
- » contingency planning
- » medical procedures
- » office and site security
- » annexes (contact lists, map, relocation plan, etc.)

Contingency planning

Contingency planning is designed to ensure organizational readiness in anticipation of an emergency and to enable the organization to react effectively in such a situation. For managers, this readiness includes plans for the management of human and financial resources, emergency supplies, communications, etc.

Effective security management aims to anticipate and avoid risks. Contingency plans are components of the overall security planning process and outline pre-established protocols and procedures in response to a specific hazard situation or event.



Contingency planning should always be undertaken when there is an indication that there is a high risk or probability that a disaster or emergency situation will occur. These situations will be identified through the threat, vulnerability and risk assessment that must be undertaken at the start of any planning process. The risk-planning matrix (see Chapter 2) will enable you to identify the priority scenarios for which contingency plans should be developed.

National Society and Federation operations should also plan in the face of recurring natural disasters such as, for example, seasonal floods, hurricanes, cyclones, etc. Plans should be based on specific events or known risks at local, national, regional or even global level (e.g., civil unrest, population movements or potential epidemics such as avian influenza). At a minimum, the standard type of contingency plan to be developed in your delegation should include relocation and medical evacuation plans.

The contingency planning process

Regardless of the scale, there is a clearly defined process for developing a contingency plan. The steps you need to take when formulating contingency plans are to:

- analyse the current situation by conducting a threat, vulnerability and risk analysis
- identify high-risk scenarios (in some cases, these will be pre-defined)
- determine options to address the situation created by the scenario
 - seek advice and direction from regional or global resources
 - formulate programme scenarios
 - brainstorm with programme managers and staff
- select the best option for the context
- identify activities related to the option chosen in terms of:
 - personnel – identify any required adjustments or specific skill requirements
 - logistics – ensure readiness of specialist equipment, emergency supplies/stocks
 - transport capacities
 - communications equipment and procedures
 - security – personnel, finance, logistics
- assign roles
- examine control/coordination considerations
- consider trigger points
- draft the plan

All contingency plans should detail the:

- situation – describe and provide local and regional perspectives
- aim/mission – what the contingency plan aims to do
- execution of the plan
 - general outline
 - phases
 - tasks
 - coordination details (routes, key locations such as assembly points, timing, etc.)
 - security aspects – cash, storage, etc.
- logistics requirements – specialized storage, food and water stocks, transport availability, etc.



Remember! Contingency planning is a dynamic process. A contingency plan is never entirely finished: there is only the latest version.

Relocation plans

Relocation plans are a type of contingency plan. Each delegation should have one developed as a stand-alone document that is an annex to the security rules and procedures for the specific, operational context. Plans must be simple and realistic. It is important that the plan is clear and understood by all Red Cross and Red Crescent personnel.

While a forced relocation can occasionally take place in undemanding circumstances, it often occurs in an atmosphere of crisis, chaos, confusion and uncertainty. Many people and tasks need to be dealt with at the same time. Experience has shown that it is best practice to establish a crisis management team and allocate tasks and responsibilities in advance (see chapter 4 for detailed information).

The crisis management team has a central coordinating function and will be convened by the senior field manager or his or her designate when the situation requires it. The team's initial task is to decide:

- who – and at what point in a crisis – will be in charge of what
- where staff will go
- who goes and who stays

- how staff will go
- what goes and what stays
- whether personnel will exit on their own or in groups
- whether those who stay continue to manage programmes, and if so, how
- what will happen to those relocated once out of the country

Assembly points, 'safe houses' and hibernation locations are sites that have been chosen for hibernation and/or as gathering points for relocation. These sites should be secure and large enough to accommodate many people and vehicles. As the operational security phase level changes to yellow, these facilities must be clearly identified and, before the phase changes to orange, these facilities should be equipped and made ready with a back-up generator, VHF radio communications and emergency stocks (including medical supplies, food, water and fuel). This would be an example of an action point in the relocation plan for the head of support services (or similar position) in the delegation.

The head of support services (or equivalent), assisted by the administration and human resources departments, will also update information in terms of how many staff and their dependants qualify for relocation.

The head of delegation or his or her designate must make it clear, to all the staff, precisely who qualifies for international relocation or assisted in-country relocation and who does not, and what those not qualifying can expect from the International Federation's delegation. A priority list will be drawn up which distinguishes not only between essential staff and non-essential staff, but also who will go at what phase and in what order, in the event that staff cannot be relocated at the same time.

In cases of relocation where it is difficult to move with assets and stocks, preparations must be made in advance with the host National Red Cross or Red Crescent Society for the possible temporary handover of assets and stocks, ensuring that everything is documented and that a memorandum of understanding is drawn up and signed by both parties. It is important to keep track of outstanding financial obligations, e.g., towards landlords, suppliers, contractors, staff, rented vehicles, etc. Updated records such as these should be taken along during relocation.

Essential and non-essential staff

The purpose of categorizing staff in times of heightened tension or crisis is to reduce overall vulnerability by cutting the number of people at risk and, thereby, making a crisis-time relocation more manageable.

Who is considered non-essential staff?

- All dependants of international staff and all international staff not in senior management positions.
- International personnel that are not essential to the continuation of a programme, determining how likely it is that certain programme components – or any programme at all – could be maintained. It is, therefore, also necessary to prioritize programmes in terms of which will close first should the situation deteriorate.
- Staff having difficulties coping with tension. A staff member may be in a key operational position and have important technical skills but may find it difficult to deal with rising insecurity. Such staff members should be withdrawn, as maintaining their presence in a deteriorating situation may eventually cause more problems than their early departure.
- Staff at higher risk. Certain nationalities may be a potential target because of resentment over their government's foreign policy, action or inaction.

Internationally recruited staff

Relocation is mandatory for all international staff and their dependants. This is clearly articulated in the International Federation's security rules and regulations. Any breach of this clause will be considered gross misconduct.

Nationally recruited staff

In principle, nationally recruited staff can seldom expect to be relocated across international borders. However, assistance will be provided, at the International Federation's expense, for in-country relocation (more often than not, nationally recruited staff will demand relocation to their original homes). The delegation will prepare a list of relocation sites (original homes of local staff) in advance and will inform staff accordingly. Contractual provisions will continue.

However, it would be wrong to assume that all national staff may want to move. Some may want to stay to protect their own dependants and assets. Dialogue must be initiated well in advance with national staff for practical purposes and in order to reach a consensus.

Certain national staff may genuinely fear persecution and may, therefore, request relocation. The delegation should use the legal instruments and national procedures available to provide asylum to people with a genuine fear of persecution. Discussions with ICRC, the host National Society and the UN in this regard are important.

Non-contracted domestic staff

The responsibility lies with respective internationally recruited delegates or staff members who are their direct employers. Disturbance allowances (mutually agreed upon between the parties) must be paid in full to these domestic assistants. No relocation across international borders will be considered for this category of personnel and the International Federation assumes no responsibility for them. A copy of any agreement signed, or even a termination of contract, should be handed over to the country representative or the head of support services.

Nationally recruited staff can be asked to continue running programmes. This situation must be planned for in advance and discussed thoroughly with staff.

Particular attention should focus on the following:

- allocation of tasks and responsibilities in the areas of financial management, administration, security, logistics, internal and external communication, personnel management and programme activities
- allocation of authority in line with responsibilities
- limits of responsibilities, e.g., it should be made clear that staff welfare/well-being comes first and that they should not put themselves at risk trying to protect the delegation's assets
- clear demarcation of authority, e.g., regarding the sale and purchase of assets, hiring or firing of staff, taking disciplinary action, entering into new contracts, liaising with authorities, deciding on changes within the programme, use of offices and vehicles, etc.
- communication channels, confidentiality and protocol of communication
- access to the delegation's bank accounts
- requirements for representation of the International Federation in country

The following list provides a quick reference of the minimum contents that should be included in any relocation plan:

- security phase indicators and actions required during each respective phase
- list of personnel to be relocated
- location of staff residences and contact numbers
- management structure, responsibilities and tasks
- assembly points
- mode of relocation and route(s) to be used
- means of transport to exit location/convoy procedures
- communications system and reporting procedures
- situation monitoring and information networking

- ✦ external liaison network with ICRC, the host National Society, UN agencies, embassies and non-governmental organizations (NGOs) on the ground
- ✦ Federation assets to be relocated and those to be handed over to the host National Society
- ✦ individual preparation tasks
- ✦ luggage restrictions
- ✦ local staff management
- ✦ liaison with the Federation secretariat in Geneva
- ✦ delegation's standby system (if deemed appropriate)

The delegation will include in its relocation or emergency close-down plan a procedure for bringing out the following records:

- ✦ the most recent financial, computer system back-up diskettes/tapes
- ✦ a list of computer passwords used in the delegation
- ✦ the current fixed assets register
- ✦ employment contracts for national staff
- ✦ payroll records for national staff (on computer system back-up diskettes/tapes if payroll is automated)
- ✦ the current register of delegation staff

The delegation will also include a procedure for the storage of files in anticipation of its return to the area of operation.

There are a number of steps to be considered once relocation has started:

- ✦ Contact the Federation secretariat immediately and provide a detailed update on staff, contact numbers, security, finance and expected movement plans.
- ✦ Organize psychological support and counselling for the group immediately as relocation is likely to give rise to a variety of disturbed feelings, stress, health problems, emotional exhaustion, a sense of failure, anger, guilt, misunderstanding, a feeling of being unappreciated, etc.
- ✦ Contact officials in the country of arrival, including the embassies, host National Society, ICRC (if present), and the local authorities.
- ✦ Establish or re-establish contact and communication with staff left behind and continuing to run the programmes.
- ✦ Consider scenarios on who can usefully stay in the region (in a neighbouring country) and who should go home (on an 'annual leave' or 'end of contract' basis).

- Organize medium-term accommodation and access to finance as evacuees will stay in a hotel for a maximum period of one week only; in the event of prolonged stays beyond one week, suitable accommodation should be identified for evacuees.
- Prepare a report for the Federation secretariat and donors with detailed updates on personnel, assets, stocks and finance, outstanding liabilities, contact numbers, etc., at the moment of relocation.
- Debrief relocated staff and address all questions openly in a group setting; provide advice on the plan of action, administrative arrangements, accommodation, general country profile, activities, steps taken so far, etc.

Responsibilities in another country

If staff are relocated to another country that has a Federation delegation, then the senior field manager in that country assumes responsibility for the relocated personnel when they arrive in his or her operational area.

Decision to return

In trying to determine whether a return to the country of operation is feasible, the key questions will be related to finding out whether it is safe to return and who will take the responsibility for the decision to conduct an exploratory mission. The decision to return to a lower alert phase will be taken by the head of zone and the manager of the security unit in Geneva on the advice of the senior field manager. Close cooperation and coordination as well as information-sharing with ICRC is essential.

Assessment criteria to determine potential return

- the actual security situation
- whether the threat has been eliminated or reduced
- the existing political situation, changes to it, any military presence, action of disturbed population or groups, renegades, etc.
- action of other agencies and international humanitarian organizations, particularly ICRC, the UN and diplomatic missions
- status of logistics and infrastructure following the crisis
- whereabouts of staff not relocated, particularly of national staff
- freedom of movement for local people
- availability of essential commodities and provisions, i.e., food, water, fuel, communications, etc.

- » ensuring that relocation facilities still exist
- » information from the host National Society



Remember! The decision about when to return is difficult as everybody (delegates, National Society, donors, media, etc.) is usually pushing and trying to bring about a speedy return. Make sure you are certain of the security situation and do not let anything or anyone else influence you. We do not want to end up in a situation where we go back too soon and then have to relocate again. Avoid shifting delegates back and forth unnecessarily.

Operational security phases

A four-colour system of alert phases was developed by the security unit in Geneva to standardize the terminology referring to operational phases used in all of the International Federation's delegations around the world. The four phases in this system are:

White phase	Situation is normal	No major security concerns
Yellow phase	Situation of heightened tension initiated	Some security concerns Heightened security awareness
Orange phase	Emergency situation	Access to beneficiaries limited Risk to Red Cross and Red Crescent personnel severe, and tight security management needed
Red phase	Relocation or hibernation	Conditions do not allow work. Risk to Red Cross and Red Crescent personnel extreme

Associated with these phases, the following terms are defined here to ensure common understanding.

Hibernation

- » Staff staying behind in one or more fortified sites (so-called safe houses) in a crisis zone because the extraordinary event is assumed to be temporary, or relocation is impossible or perceived too dangerous to undertake.

Relocation

- **Internal** – The physical withdrawal of staff and/or their eligible dependants, family members, spouses and authorized visitors and assets from a crisis spot to a safer location within the same country.
- **External** – The physical withdrawal of internationally recruited staff and their eligible dependants, family members, spouses and authorized visitors from a crisis spot across an international border.

Phase	Descriptor/triggers
<p>White Normality</p>	<p>Ideal working conditions, no limitations to operations.</p> <ul style="list-style-type: none"> → Rare incidents in the field; occasional armed and/or violent contact. → Passenger and freight vehicles moving more or less freely throughout the area of operation. → No restriction on movement imposed by the security forces. → No indication of civil unrest. → Low crime rate.
<p>Yellow Heightened tension</p>	<p>Working conditions allow programmes to continue, although there are some security concerns; a situation of heightened security awareness is initiated.</p> <ul style="list-style-type: none"> → Almost daily localized incidents are reported in relation to civil, political and/or organized conflict. → Passenger and freight vehicle services disrupted at times due to security issues. → Checkpoints active and increased presence of persons carrying arms. → Local disaster causes disruption to activities and requires adjustment to and possible enhancement of security procedures. → Civil unrest, political and social conflict increases. → Higher incidence of violent crimes.

Actions

Provided working conditions are not limited as described, then no particular measures have to be taken into consideration. Security incident reports should be sent to the security unit on occurrence.

- Normal security regulations apply but with a heightened sense of security.
- The senior field manager, in consultation with the security focal point and the security unit in Geneva, may consider introducing a travel restriction for visits by external personnel if the situation deteriorates.
- Any incident is to be reported to the senior field manager/security manager as soon as possible for further follow-up.
- Security updates are provided to the security unit in Geneva on a regular basis.

Phase	Descriptor/triggers
<p>Orange Emergency situation</p>	<p>Working conditions do not allow proper access to beneficiaries; need to reduce number of expatriates and activities; tight security management is required.</p> <ul style="list-style-type: none"> → Regular and widespread armed contacts and security force sweeps. → Heightened tension throughout the operational area. → Civilian transport considerably reduced due to security concerns. → Checkpoints active and increased presence of persons carrying arms. → Red Cross and Red Crescent personnel experience difficulty accessing all areas. → Expatriates' movements restricted to key base locations without clearance to move to field. → Incidence of riots, political and social breakdown. → State of natural disaster declared. → State of emergency declared by authorities. → Incidence of violent crimes committed against expatriates gets out of control.
<p>Red Relocation or hibernation</p>	<p>Security conditions do not allow work to be carried out; presence of delegates is a liability and their relocation is necessary.</p> <ul style="list-style-type: none"> → Widespread armed confrontations. → Armed assaults against staff of international humanitarian and non-governmental organizations. → Government orders expatriates to withdraw. → Diplomatic and humanitarian community evacuates its personnel and dependants. → Direct attack on or against Red Cross and Red Crescent staff or premises. → Total breakdown of law and order.

Actions

- Activities continue close to the respective offices, but expatriate level is reduced to acceptable minimum, allowing operations to continue.
 - No major road movements to take place unless explicitly authorized by the security forces after submission of movement notification.
 - Expatriate personnel not remaining in skeleton group are relocated to safe area.
 - Depending on the situation, transport organized (e.g., small plane, helicopter, etc.) or authorization given for vehicles to move towards base/safe location.
 - All personnel carry essential phone numbers with them.
 - Personnel remaining must ensure they have four to five days worth of food and water reserves available.
 - All communications equipment (e.g., phones, radios and spare batteries) is kept fully ready.
 - Steps should be taken to harden premises with sandbags around walls, tape/blast film applied to windows and access to facilities restricted.
 - Regular security updates provided to the security unit in Geneva.
-
- Vehicle use minimized and staff to stay put in their respective offices.
 - Thorough security checks completed before any road movement is allowed.
 - Staff ensure they have communications equipment and await further instructions.
 - Each expatriate should have one bag ready with all his/her essentials (e.g., travel and identification documents, some clothes, personal computer, etc.), weighing not more than 10 kilograms.
 - Constant contact between delegation and the security unit in Geneva.
 - Where possible, relocation to be undertaken from any of the field locations to a location from where people will depart straight out of the province/country, etc.
 - Handover procedures in accordance with the Delegates' Handbook undertaken on relocation.

1

2

3

4

5

6

Hibernation

When security conditions make it impossible to relocate personnel, they will be directed to remain indoors at a predetermined location until the situation stabilizes.

Considerations when preparing for hibernation include:

- hardening the hibernation location as much as possible with sandbags and blast film on windows
- establishing and maintaining communications mechanisms with the regional delegation and the security unit in Geneva, with a back-up communications system
- clearly marking the hibernation location with the International Federation's logo and by flying the red cross or red crescent emblem, unless the security situation is such that this will create added risk
- maintaining a minimum 14 days' supply of food, water and fuel reserves at the designated site
- maintaining a minimum 14 days' supply of first-aid and hygiene supplies at the designated site

The following is a list of what should normally be kept in stock. You should feel free to expand or adapt the list according to local needs and standards:

- stocks of water and food are most important
 - separate drinking/cooking-water and water for washing
 - keep a supply of water purification tablets as well as water filters
 - food should be dry food and of a type not requiring a long time to cook (to save fire fuel)
 - some common foods are not appropriate: rice, pasta and dry beans all require lots of water and a fair amount of cooking time
 - avoid excessively salty foods, which make you thirsty and deplete your water reserves
- hygiene items such as toilet paper and soap (individuals should have their personal supply including toothbrush and toothpaste, shampoo, etc.)
- toilet facilities (improvised toilet facilities if no toilet exists within the shelter)
- communication possibilities (radios, mobile or satellite phones, etc.)
- power supply – generator, batteries for torches and radio
- fuel stocks – both for generator and fire fuel (gas, firewood, etc.)
- heat tablets – where not enough wood is found

- ✎ lighting, including torches and spare batteries, candles and matches
- ✎ plastic rubbish bags
- ✎ medical and first-aid kits
- ✎ sleeping mats/mattresses and sleeping bags
- ✎ can-opener, paper plates and bowls, disposable cups, plastic forks, spoons and knives
- ✎ mosquito netting
- ✎ maps of the area and a compass
- ✎ basic tools (spade, axe, knife, rope, nails, hammer, etc.)
- ✎ red cross or red crescent flags
- ✎ extra clothing – each delegate should have prepared a bag with a change of clothes, etc.



Remember! The hibernation location must be known to all Red Cross and Red Crescent personnel that are supposed to use it. The location must also be easily reached and accessible. Map and GPS coordinates should be available and known to all.

In terms of how the various phases are announced, the following guidelines apply:

- ✎ The security phases may be implemented in sequential order or as the situation dictates.
- ✎ Different operational areas within the same country may have different security phases if the security situation is not the same as other parts of the country.
- ✎ Yellow phase may be declared by the senior manager in the field at his or her own discretion, following which he or she will notify the security unit in Geneva.
- ✎ Orange phase may be declared by the senior manager in the field in consultation with the manager of the security unit in Geneva.
- ✎ Red phase will normally – if time permits – be declared by the senior manager in the field following the authorization of the director of the coordination and programmes division, in consultation with the manager of the security unit in Geneva.
- ✎ A return to normal may be declared by the senior manager in the field with respect to yellow and white phases. If orange or red phases are in force, the decision to return to a lower-risk security phase will be taken by the head of zone office and the manager of the security unit in Geneva on the advice of the country representative.

Security guidelines and advice

Guidelines should be developed when staff face situations where directed actions such as regulations are inappropriate or may be dangerous because the situation requires actions that are situation-specific based on an awareness or analysis of the situation. Where such situations are known to occur, guidelines should be provided to help staff cope. Typical situations and topics that may be covered in guidelines could include:

- behaviour at checkpoints
- what to do if fired upon
- what to do in the event of an explosion
- actions during natural disasters (floods, earthquakes, mudslides, etc.)

Where the operation faces a changing situation which requires a temporary adjustment to the way we operate, then advisories should be put in place to provide direction to staff. For example, if demonstrations or protests are expected to take place in one part of the city, then restrictions should be imposed instructing staff to stay away; or, if road conditions have become dangerous due to winter snowfalls, then staff should be directed to alternative routes or prevented from travelling on the affected route.

Welcome pack

It may be unreasonable to expect that staff visiting the operation for a short period become fully aware of everything in the security plan. In these cases, consideration should be given to producing a briefing or welcome pack that provides an overview of the key elements of the security plan that visitors should be aware of. This might include:

- short summary of the in-country situation
- principal threats and risks in the area
- key regulations, noting especially any curfews, restricted areas, field movement control procedures, communications requirements, etc.
- key actions to undertake in emergency situations
- key contact numbers for delegation personnel

Security briefings and debriefings

It is important that all Red Cross and Red Crescent staff know and understand the security plan. A security briefing should be a mandatory requirement of an induction programme and staff should receive a briefing on key elements of the

plan upon their arrival. This should, typically, cover similar elements to those included in a welcome pack with the aim of ensuring the individual is aware of the situation, is able to follow procedures and regulations, and stays safe while settling in and becoming familiar with the operational situation. Staff should also receive an updated briefing if the situation changes. Security should always be an agenda item at management meetings. These briefings should cover the situation and any measures being taken as a result of any changes.

Equally important is the requirement for debriefings. Debriefing should be conducted at the end of any crisis or incident, while one-to-one sessions should be held for staff who are finishing a mission.

General security debriefing

Topic areas to be covered during a general security debriefing include:

- ❏ current security situation as viewed by the individual and perceived changes over the period of deployment
- ❏ any security issues or incidents during deployment
- ❏ identification of lessons learnt during deployment
- ❏ any suggestions for changes to the existing security plan

Incident debriefing

A debriefing of any security incident should take place as soon as possible and include the following:

- ❏ a recounting of the sequence of events surrounding the incident
- ❏ discussion of the actions taken
- ❏ mistakes made and how they could have been avoided
- ❏ identifying any security or safety breaches
- ❏ discussion of lessons learnt and ways of avoiding any recurrence of the incidents
- ❏ identification of any required changes to existing security regulations or procedures
- ❏ identifying any need for stress counselling

The security unit has developed standard templates to assist in the creation of the various documents required in your security planning. You will find them in the security section on FedNet. Alternatively, they can be obtained directly from the security unit.



Incident management, as referred to in this manual, is the handling of crisis situations or any event that threatens – or has impacted on – the safety or security of Federation personnel, assets or operations.

In recent years, incidents involving vehicles accounted for over half of all security-related incidents reported to the security unit. Vehicle safety and security were, therefore, discussed in more detail in Chapter 3 of *Stay safe: The International Federation's guide to Safer Mission*. Incidents involving general crime such as burglary, theft and robbery, accounted for over a third of all security-related incidents. Many of these incidents could have been avoided through better security management and higher security awareness on the part of individuals.

This chapter emphasizes the importance of reporting any incident that occurs in the field, why it is important to analyse these events, and the basics of managing critical incidents.

Incident reporting

A manager's ability to understand the current situation and to adapt to any changes in the situation is a key factor in ensuring the safety and security of the International Federation's operations and its staff members. The accurate and speedy reporting of *all* security incidents contributes to a manager's ability to do this and is, therefore, a key element of the International Federation's security framework.

Incident reporting allows the security situation to be mapped more accurately, an analysis of operational security trends to be carried out and the security of the International Federation's staff and its material assets to be improved. Reporting also helps to determine how resources are deployed and to identify topics to be covered in future security training and briefings. Even though the incident itself may seem insignificant, it may be indicative of mounting tension or a possible trend of threats. It is therefore imperative that this be well documented and available for use by senior management at the Federation secretariat.

Remember also that the International Federation is responsible for keeping Participating National Societies informed of all specific incidents concerning their delegates and the overall security situation in the area of operation. To avoid a situation where National Societies and families learn about a security incident through the international media and to ensure adequate follow-up by the responsible Federation secretariat departments, delegations are obliged to inform the security unit immediately when an incident has occurred.

In order to improve the International Federation's reporting procedures and the collection of incident data, field managers are required to follow the procedures set out below. As managers, you need to ensure that your staff are both familiar with these procedures and that they adhere to them.

Defining a security incident

The International Federation has a broad definition of what constitutes a security incident. It is important to include even minor incidents and to report 'near misses' (i.e., situations in which an accident or incident was narrowly avoided). If in doubt, the incident should be reported to the security unit.

The Federation defines "security incident" as follows:

"Any situation, occasion, or incident in which:

- (a) The safety or well-being of those coming under the Federations security management is compromised or put at risk in any way,
- (b) Those coming under the Federations security management are injured or threatened with harm of any kind,
- (c) Any third party is injured or harmed in the course of the Federation's or other under the Federation's security management activities, or is put at risk of injury or harm.

- (d) Federation property and property of those coming under the Federation's security management, property of third party working on Federation/PNS programs or operations, or the private belongings of Federation personnel are damaged, stolen or put at risk.

All breaches of a delegation's security regulations constitute security incidents and must be reported. Depending on the circumstances, breaches of the Federation's *Code of Conduct* and of other Federation policies and procedures may also constitute security incidents."

Federation personnel includes all delegates and staff-on-loan and accompanying family members, visiting Federation staff, delegation visitors, regional disaster response team delegates, Participating National Societies working under the International Federation's security umbrella, locally employed staff, and National Society staff and volunteers in the course of their duties when working for the International Federation.

Examples of security incidents

It is not possible to define the whole range of situations that may constitute a security incident. The term is, therefore, defined very broadly and includes, but is not limited to:

- all crimes involving Federation personnel and property (including, theft, burglary, robbery, carjacking, kidnapping and so on)
- all instances where Federation personnel are threatened with weapons or with acts of violence
- all instances of harassment or threatening behaviour of any kind
- acts of war such as shelling, mines, gunfire or military aggression
- looting, attacks on property and vandalism
- any accident involving vehicles (whether serious or not, and whether the responsibility of the International Federation's driver or not)
- all cases of medical evacuation or relocation of delegates
- all cases in which Federation personnel may be involved in unlawful activities
- all breaches of the delegation's security regulations



Remember! In cases where you are uncertain about whether a situation should be reported, you should err on the side of caution and submit an incident report.

Using the security incident report form

All security incidents must be reported to the security unit using the security incident report form (see Annex 2 of this manual for the template), which has been designed to provide a summary of all relevant information concerning the incident.

In terms of timeframe, security incidents are to be reported as follows:

- All incidents involving death, serious injury, kidnapping or which are particularly sensitive, must be reported to the security unit by telephone immediately. A completed incident report must follow within 24 hours.
- All incidents in which Federation personnel or property are involved, including:
 - any physical injury to any person
 - any significant damage to property (whether Federation property or not)
 - any situation in which there was a serious risk of injury or damage must be reported to the security unit by telephone or e-mail within 24 hours. A completed incident report must follow within 48 hours of the incident.
- All other security incidents of any kind must be formally reported to the security unit, using the security incident report form, within 48 hours of the incident.

Once the security unit receives a report, it will assess what measures should be taken (if any). This may involve follow-up with the delegation, with other departments within the Federation secretariat or with our Movement partners.

While information contained in the incident report form will be handled carefully by the security unit, you should call directly to discuss any situation that is especially sensitive or delicate. The most appropriate way of managing the situation can then be determined.

Incident analysis

After a security incident occurs, it is important that an analysis of the actual event as well as the events leading up to it takes place. It is important to determine why an incident occurred and how it can be prevented in the future (e.g., through adjustments to security regulations or procedures).

Some common reasons for security incidents include:

- ✎ ineffective security management and ignorance of procedures
- ✎ lack of basic security awareness
- ✎ profile of the Red Cross and Red Crescent in the country and how it is viewed by the local population (e.g., provocative behaviour, cultural insensitivity, etc.)
- ✎ interpersonal relations and personal problems
- ✎ lack of information
- ✎ taking unnecessary risks
- ✎ stress-related security incidents

An analysis of incidents should focus on the following areas.

- ✎ Leading up to the incident, were procedures followed and, if so, is there something that needs to be changed?
- ✎ Were you targeted? Is this because you did something to provoke an attack? Were you perceived as being wealthy or a soft target? Is the Red Cross or Red Crescent no longer accepted in the area?
- ✎ Were the procedures in dealing with the incident appropriate?

Identifying trends

This essentially involves looking at whether there are common elements between the incidents.

✎ **Are these incidents occurring in certain areas more often?**

Recording the incident(s) on a map may identify specific areas where certain incidents – higher level of traffic accidents, higher level of residential burglaries, carjackings, etc. – are occurring. This will enable action to be taken to reduce the risk by avoiding certain areas.

✎ **Are incidents occurring at certain times?**

For example, if more car accidents occur at night or during certain hours, then we can avoid travelling at that time.

✎ **Are the circumstances of the incident or the outline of events similar?**

For example, if carjacking of four-wheel drive vehicles travelling alone occurs, we can perhaps reduce the risk by implementing a two-vehicle policy for any vehicle movements.

Critical incident management

Defining a critical incident

A critical incident is defined as: A situation that, threatens, or has impacted on, the safety / security of Federation personnel, assets or operations to the extent that there is the potential to be a significant disruption or even incapacity to continue to operate. **Such incidents¹ could involve:**

- the death of a delegate or third party caused by Federation personnel
- accidents resulting in serious or multiple injuries
- violation of the status agreement with the host country's government
- attacks on staff or assets
- kidnapping

Immediately any incident occurs the first step is to establish what has happened and gather as much information as possible as quickly as possible. This, in turn, enables a decision to be made as to whether this is a simple incident and can be managed according to normal procedures, or whether this is a critical incident and will therefore need to be managed as such. For example, a vehicle accident with minor injuries would normally be managed through standard procedures; however, a vehicle accident involving the death of a third party could have significant implications both legally and for the International Federation's operation and could therefore be considered a critical incident.

Depending on the incident, either the senior field manager² manages the incident with advice and direction from the Zone or through the appropriate Under Secretary General (USG) in Geneva as determined by the Senior Management Team, if required; or the incident is managed through the appropriate USG in Geneva with either the zone or country delegation providing information and acting as directed.

In any critical incident a critical incident manager (CIM) should be appointed. A CIM may be appointed by, the country manager, Director of Zone or the appropriate USG dependent on the level of the incident. The CIM is responsible for assembling the Critical Incident Management Team (CIMT) and then managing the response to the situation, and is relieved from the responsibilities of their regular position for the duration of the response. The CIM will have the del-

1. The list of examples provided is not exhaustive, but designed to be indicative. Field managers must make an assessment and, if in doubt, liaise with the security unit to confirm.

2. The term senior field manager is used as a generic term, dependent on the situation in the field this could be a Head of Operations, Country Representative, Regional Representative, or a FACT/ERU Team Leader.

egated functional authorities necessary in order to commit the appropriate personnel, equipment, finances and other resources to ensure an effective and timely response to the situation, or incidents related to the crisis.

Critical incident management team

A critical incident management team is to be set up once the details of the incident have been confirmed. From the moment an incident is confirmed, the critical incident management team takes over all line management and operational responsibilities for the incident. The lines of command should be as short as possible and the authority of the team sufficiently strong to allow immediate, urgent decisions to be made; but also equally restrained as far as the potential liability of the organization as a whole is concerned. The critical incident management team works for the manager, who retains executive authority.

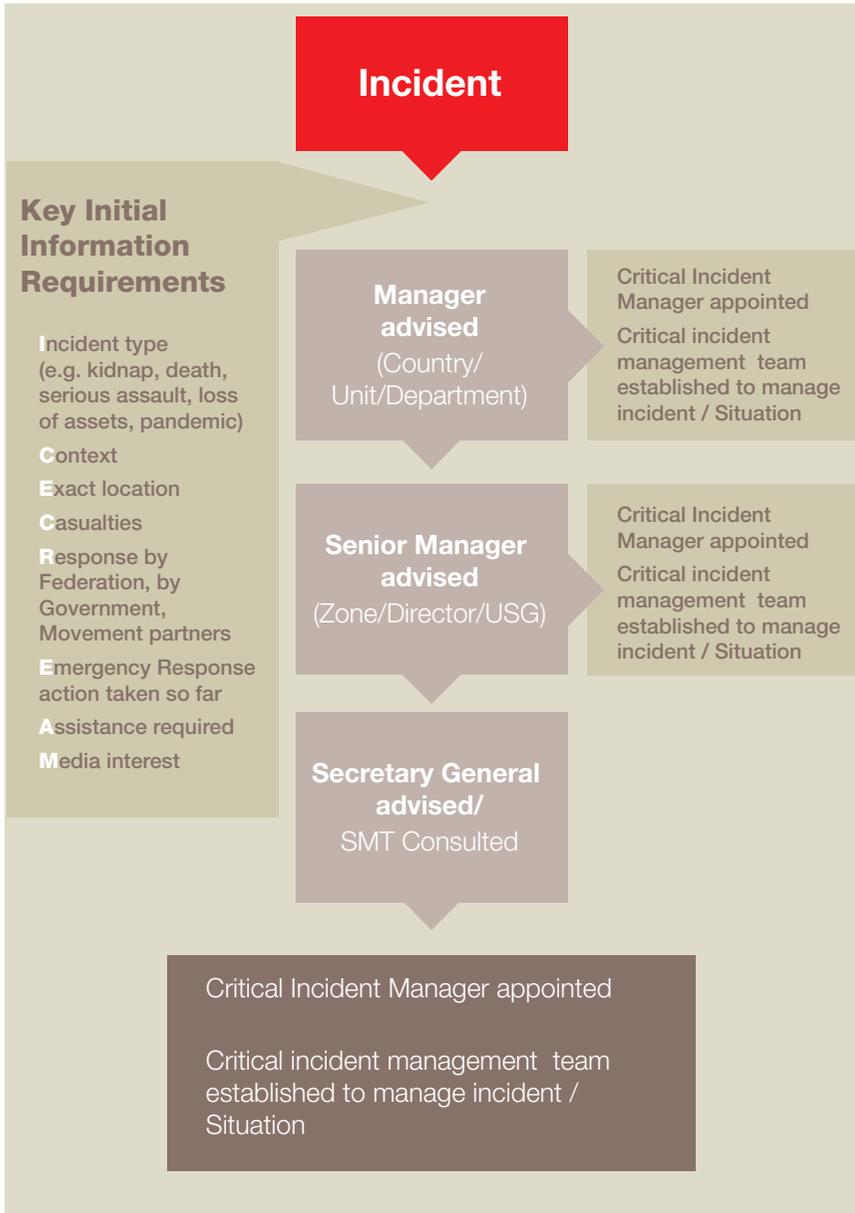
Critical incident management team composition

Ideally, the critical incident management team should comprise between three and five experienced staff from the key departments involved.

In the field, it could be the head delegation, operation or sub-delegation; head of support services (human resources, information/media), security; programme coordinator; and FACT/ERU team leader or Participating National Society head of mission (if the incident involves these entities). In Geneva, this will typically be staff from the Programmes and Services division, the human resources and legal departments, and the security and public communication units.

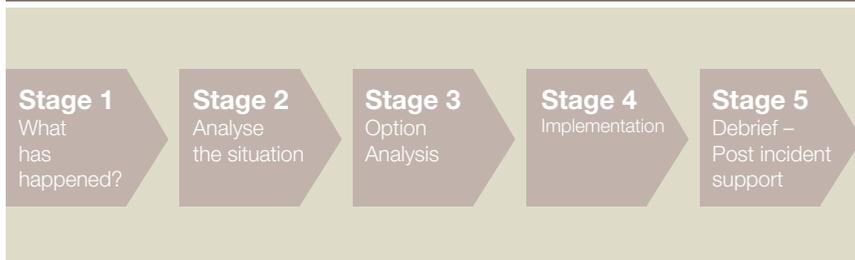
Others may be seconded for specific planning or execution tasks. It is vital, however, that the team does not get too big and become ineffective in planning and making decisions. Members of the critical incident management team are only there because they have specific technical expertise to contribute.

The diagram summarises the sequence of events that should be followed initially.



CRITICAL INCIDENT MANAGEMENT PROCESS

To resolve the incident a five stage process will normally be worked through.



Stage 1. Establishing what happened

The first step must be to identify whether any immediate action is required to protect life. If this is the case, then action should be taken without delay. Note that this will normally be a simple extension of the action already taken to determine whether this was a critical incident or not. This process must be ongoing until the incident has been resolved.

Verifiable information must then be established outlining the details of the incident, and this must be recorded. In the early stages, it is vital to establish a system to record the chronology of events, log phone calls, record notes of all meetings, and ensure that all documents are recorded and filed. This is done through an incident log that should be established by the CIM immediately after the incident is notified. A template for an incident log is shown at the end of this chapter.

Key initial information that should be collected includes:

- ✎ What happened?
- ✎ Who is involved? (internal and external parties)
- ✎ When did the incident take place?
- ✎ Where did the incident occur?
- ✎ Who has been made aware of the incident?
- ✎ What is the likely impact of this incident on the mission?
- ✎ What actions have been taken to date?
- ✎ Is the situation continuing or has it ended?
- ✎ Is the media present and what are they interested in?
- ✎ What category of incident is this?

1

2

3

4

5

6

A useful acronym to assist in this regard is ICECREAM:

- Incident type (e.g. kidnap, death, serious assault, loss of assets, pandemic)
- Context
- Exact location
- Casualties
- Response by Federation, by Government, Movement partners
- Emergency Response action taken so far
- Assistance required
- Media interest

In the event of an incident which requires input, support or management from the Federation secretariat in Geneva, the critical incident management team (CIMT) established by the USG would work with a field team established by either the Director of zone or the senior field manager in the host country. It is acknowledged that while strategic issues can be dealt with in Geneva, there remains a requirement for operational implementation that can only be achieved at field level. In essence, a global critical incident management team would be established, where the Geneva team works in conjunction with the field team. If needed, in extreme incidents, the field team may be boosted by elements deployed from Geneva.

A useful tool to be established and maintained throughout the incident/situation is four 'white boards' or flips charts titled:



These charts provide a useful record of how the incident is managed. They can be used to provide briefings to senior management and also as part of a handover brief for incoming personnel if team is operating for continued extended period that requires a team roster/change over.

Stage 2. Analysing the situation

The purpose of this stage is to identify the problem and the parameters surrounding the problem. This includes noting and considering:

- the Red Cross and Red Crescent Movement actors involved (ICRC, National Society or Partner National Society)
- the involvement of external actors
- country context, including the current situation (disaster, conflict, etc.), the infrastructure (transport, medical, food, water and sanitation), capacity of the government, status and capacity of the National Society in the country, status of the International Federation in the country and any limitations on its ability to act
- legal issues
- medical issues
- communications issues
- media presence and exposure
- determining the ultimate objective (e.g., evacuating the injured person, repatriating the body, releasing the hostage, etc.)

The CIMT must also decide:

- Whether due to risks to personnel, any programme activities should be suspended or whether personnel should be withdrawn to a more secure location.
- If additional support personnel should be deployed to any field location to assist.
- What information should be circulated internally and externally, and identify any limitations or confidentiality issues.
- If any additional personnel or external specialists should be included in the CIMT.

CIMT members may be assigned specific roles/tasks and responsibilities for managing relations with specific stakeholders.

Stage 3. Option analysis

At the start of this stage, two questions must be asked:

1. Is this situation covered by an existing contingency plan? If so, can it be implemented?
2. Does the International Federation have the internal expertise to address and/or manage the incident? If not, where can this be obtained?

Established contingency plans currently exist for numerous situations such as medivac or emergency relocation. Based on the initial assessment, if an appropriate contingency plan exists for the situation at hand it should be activated. Initiating a contingency or business continuity plan will normally replace Stage 3 (Option Analysis) and Stage 4 (Implementation) in this process. However, Stage 5 – Debrief / post incident support must still be initiated. at the completion of the end state objective.

If there are no existing contingency plans or no existing continuity plans that can be adapted, then a response plan must be developed. This requires the identification and analysis of options to reach the end-state objective. During this stage the following should be considered:

- Only options and factors that contribute to the identified end-state should be discussed and analysed
- Options should have technical input from all members of the CIMT
- If technical input is required that is not available from CIMT then this must be obtained.
- Options tested against
 - Fundamental principles
 - Code of conduct
 - Limitations imposed by country context
 - Resources available to implement
- Preferred option is identified and presented to the DoZ, USG/Director or Secretary General as appropriate for executive decision.

During this stage additional personnel may be utilised to provide specific technical information, or members of the CIMT may utilise additional personnel from their departments to assist with work involved in option analysis; for example the media advisor may use members of the media department to assist development of press lines and proposed media releases. However, the CIM is to adopt a disciplined approach to those that are part of the CIMT so that the team does not expand and develop into a task force or committee.

A list of some key planning considerations for a range of what would normally be considered as critical incidents is shown in Annex 3 Note that this list is not exhaustive and there may be other considerations that are identified as part of the process.

When considering options and having identified the preferred option the CIMT must always consider the fluid nature of the situation and the potential implication this might have – the question ‘**What if?**’ (something changes or something new happens) should constantly be tabled.

Stage 4. Implementation

Implementation of the preferred option should be in the form of a plan. This plan should:

- clearly define the objective/mission
- assign roles
- detail clear coordination aspects: timings, reporting requirements, interaction with other players (ICRC, Partner National Societies or host National Societies, and external actors)
- clearly define the command and control framework

The CIMT’s role is to monitor the implementation and to be prepared to adjust it if required.

Management of the situation also requires constantly looking ahead to the future and working through ‘what if?’ scenarios.

Depending on the type of incident, it should be accepted that the situation may continue for some time. For example, a hostage situation could go on for months or years. After the initial intensity, things may slow down, in which case a sustainable management framework will have to be implemented to enable other business to be conducted without any impediment.

Stage 5. Review/follow-up

After the incident has been resolved, a debriefing process should be implemented.

In the first instance the incident and situation surrounding the incident is to be fully investigated to determine why it occurred and whether it could have been prevented. Secondly the debrief is to examine how the incident or situation was managed to determine what can be learned and whether the manner in which it was managed could be improved; lessons learned are to be identified and documented.

This process is to work through the incident from start to finish and examine actions taken at each stage.

- Confirm the incident log and sequence of events is accurate
- Were the actions taken appropriate?
- Were existing procedures followed and are these procedures appropriate or do they need changing?
- Lessons should be identified and recorded
- Are there any on going follow up requirements: e.g. counselling, legal, insurance requirements should be actioned.

Lessons learnt should be identified and recorded, while any required changes to existing procedures and regulations should be implemented without delay. It is also important to assign actions for follow-up requirements such as personnel counselling, legal proceedings, insurance claims, etc.

Dos and don'ts of dealing with the media

Some incidents and crises may attract the attention of the local or international media. Some important tips are given below to bear in mind when dealing with the media.

Do:

use advice from the media unit at the Federation secretariat

stick to known facts

tell the truth

use everyday language

keep your cool

Don't:

speculate

lie

assign blame

offer information off the record



Remember! While strong emotions are a natural response to critical incidents, it is vital that emotions do not influence the critical incident management process as any action must contribute towards and not detract from managing the incident.

Conclusion

During times of crisis, there is generally a lot of confusion and even panic. Sometimes, the most rational individuals have difficulty thinking clearly. All crises are different but have similar characteristics

- ✦ an element of surprise
- ✦ insufficient information
- ✦ escalating flow of events that may outpace response
- ✦ important issues resulting in outside scrutiny
- ✦ loss of control (real or perceived)
- ✦ disruption to normal decision-making processes
- ✦ those directly affected tend to adopt a short-term focus

International Federation operations, by their very nature, deal with crisis situations so our processes and structures are designed to operate and cope with these characteristics. However, when an incident or critical incident occurs within the operation, these characteristics are intensified and our ability to cope with everyday issues as well as with the incident may be stretched.

The purpose behind incident management is to reduce the effects of the above-mentioned characteristics and enhance our ability to cope. Additionally, security awareness, threat, vulnerability and risk analysis, effective procedures, the holding of safety drills, extensive networking with partner and external agencies and good contingency planning are all proactive ways of dealing with potential crises.

Although policies will not always cover every eventuality, having contingency plans and regularly updating them to work through 'what if?' scenarios, as well as having effective crisis management procedures in place, will go a long way towards keeping a situation under control and maintaining safe operations.

Incident Log Template

The log should record all activities and actions under taken. The second column should record details of any updates received or advice on developments with any actions then taken recorded in the third column. Action may also be initiated as part of normal planning/management of the situation not in response to a change or update in which case the second column is left blank and the actions taken simply inserted in the third column.

The Critical Incident Manager should regularly review the log and initial it signifying the logs accuracy.

Date/Time	Information Received	Response or Initiated Action	Responsible	Initials



There are times when the various components of the International Red Cross and Red Crescent Movement enter into a relationship with military bodies – either in a national or international context. This relationship can arise in all kinds of situations: non-emergency peacetime, armed conflict, internal strife or other violence, and during or in the aftermath of natural or technological disasters.

You should be aware that in an increasing number of contexts, armed forces are using humanitarian assistance as a way of attaining strategic or tactical military goals and advantages, as well as for force protection (by gaining acceptance). For example, the military barter assistance to the civilian population in exchange for intelligence, to improve the protection of its own forces, to gain sympathy for its cause, or as a means of coercing or rewarding cooperation.

Always bear in mind that the military has a political reason or agenda for being used by humanitarian organizations to help distribute aid.

This worrying trend is serving to ‘blur the lines’, so that providing aid is not always seen as a purely impartial and neutral act. Instead, the lives of humanitarian workers and volunteers are increasingly being endangered, while the people most in need are being made even more vulnerable.

There are numerous initiatives and discussions under way involving noted humanitarian bodies and the UN on how aid organizations and the military should cooperate. This chapter does not aim to discuss the wider issue of civil and military cooperation, but merely reflects the position of the International Red Cross and Red Crescent Movement.

The Movement's humanitarian mission is to prevent and alleviate human suffering wherever it is found, by means of independent, neutral and impartial humanitarian action. This makes it especially necessary for the Movement's components to gain the acceptance and trust of all parties to a conflict in order to have access to the people affected and to be able to provide them with protection and assistance.

This chapter will explain the decisions taken by the Movement concerning its relations with military bodies to help preserve our identity and to coordinate activities as much as possible without compromising respect for our fundamental principles.



Remember! Your understanding of the need to use military assets and/or profile of the military involved may be perceived differently by the local community and beneficiaries. An assessment of their understanding and dissemination of your intentions may help avoid tensions.

Using military assets

The use of military assets by a component of the Movement, particularly in countries affected by armed conflict and/or strife or other violence, should always be a last resort. It can be justified only by the serious and urgent need for lifesaving humanitarian action and when there is no alternative means of taking that action.

It is essential for the Movement to retain its identity as an independent, neutral and impartial humanitarian force. In operational contexts where there are military operations, the components of the Movement need to clearly delineate their humanitarian activities from those carried out by military bodies and to explain their *modus operandi* to the latter¹.

In particular, relations between the Movement's components and military bodies must always be conducted within the following framework:

1. Action 15 of the Strategy for the International Red Cross and Red Crescent Movement. The implementation of this action does not affect the obligations of National Societies working as auxiliaries to the medical services of the armed forces, in accordance with Article 26 of the First Geneva Convention (see Part III.1).

- the Fundamental Principles of the International Red Cross and Red Crescent Movement
- international humanitarian law (IHL), particularly the four Geneva Conventions of 1949 and their Additional Protocols
- the resolution adopted by the Council of Delegates in November 2005 on relations between the components of the Movement and military bodies
- the Statutes of the International Red Cross and Red Crescent Movement
- the Code of Conduct for the International Red Cross and Red Crescent Movement and NGOs in Disaster Relief
- the Principles and Rules for Red Cross and Red Crescent Disaster Relief
- the *Seville Agreement*² and other mechanisms in force for coordination within the Movement
- other relevant resolutions and regulations adopted by the International Conference of the Red Cross and Red Crescent and the Council of Delegates, in particular on armed escorts³ and the use of the emblems⁴
- International Federation/ICRC *Report on the Use of Armed Protection for Humanitarian Assistance*

On the basis of their mandates, the components of the Movement often interact with military bodies. Examples of appropriate interaction include:

- working with military bodies in disaster preparedness and disaster response (especially in terms of logistics), in accordance with the policies and framework set out at the national level
- health and social welfare services, as well as first-aid training
- tracing services, restoring family links and ascertaining the fate of missing persons
- disseminating knowledge of IHL (including provisions on the emblems), the fundamental principles and the mandates and activities of all Movement components
- helping military bodies to implement IHL

All Movement components involved in international activities must safeguard the neutrality and independence of their work and clearly distinguish themselves from the military at all times. It is critical to maintain a distinction between humanitarian activity and politically motivated aid.

2. *Agreement on the Organization of the International Activities of the Components of the International Red Cross and Red Crescent Movement, Council of Delegates Resolution 6, Seville, 1997*

3. *Resolution 9, Council of Delegates, Geneva, 1995*

4. *Resolution 5, Council of Delegates, Budapest, 1991*

Movement coordination agreements and mechanisms must always be observed. National Societies working internationally (other than in the situation described by Article 26 of the First Geneva Convention) in the same theatre of operations as their national military forces take special care that they are not – and are not perceived to be – part of that military operation. This is particularly important if the armed forces in question are – or are perceived as being – party to the armed conflict.

Components of the Movement may participate in military training and exercises. When doing so, the purpose should be to raise awareness among the military of the mandate(s) and activities of the Movement's components,⁵ the Fundamental Principles and the protective role of the emblems and to promote IHL. Whenever more than one component of the Movement is engaged in an exercise, they should keep each other informed and coordinate activities. Participation in exercises must also serve to promote mutual understanding between components of the Movement and military bodies.

Components of the Movement must promote the correct use of the emblems by all, including military bodies, and make widely known the provisions of IHL regarding their legitimate use.

Guiding principles

- Be wary of any proposed use of military assets.
- The use of military assets is always a last resort.
- Use should always be guided by need – not opportunity.
- The need to observe the fundamental principles, especially the principles of independence, neutrality, impartiality and humanity.
- Always consult with other components of the Movement, especially ICRC if present in the same operational area.
- Authorization to use any military assets/support must be provided by the director of the coordination and programmes division.
- Consult with the Federation secretariat's focal person (who can be contacted through the security unit) for all matters relating to military cooperation and the use of military assets.

5. In particular, relating to the role of National Societies in disaster preparedness and disaster response.

Always consider

- ✎ Is there an armed conflict?
- ✎ How urgent is the need?
- ✎ Is there no comparable alternative?
- ✎ Will such use of military assets pose a threat to the perceived neutrality, impartiality or independence of the operation?
- ✎ What could be the effect on other components of the Movement, perhaps in the longer term?
- ✎ Will we have overall control of the operation?
- ✎ What is the time period?
- ✎ Is such use of military assets in keeping with International Federation's operational strategy?
- ✎ Which military force is involved (national army or military from a country that is seen as an occupying force or a likely terror target), and what is the acceptance and perception of this force by the local population?
- ✎ Should the military assets and personnel bear the red cross or red crescent emblems in order to clearly identify their humanitarian activities or will this have a negative impact on the Red Cross and Red Crescent Movement?

Absolute limits

- ✎ Never use armed military transport.
- ✎ Never use assets of a party to an armed conflict.
- ✎ Never use military assets simply because they are available.

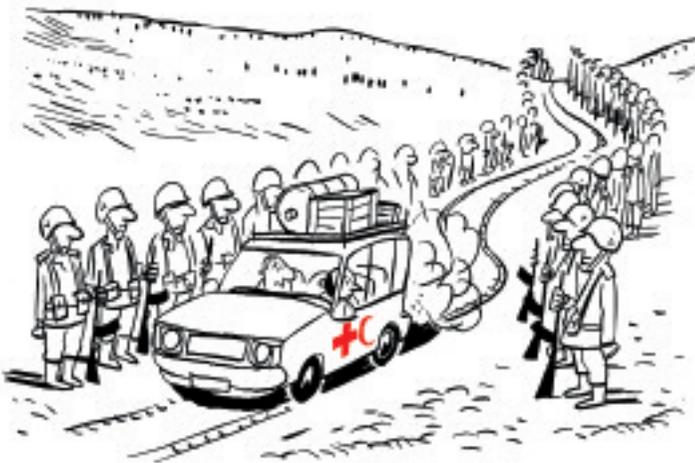
If military assets are used by the Movement, it must be purely for humanitarian purposes and 'neutralized' accordingly:

- ✎ All weaponry must be removed and any potential automatic means of defence must be deactivated.
- ✎ Surveillance equipment should be uninstalled.
- ✎ A Movement call sign should be allocated.
- ✎ A full packing list should be compiled with no ex-military/military-style items.

Using armed escorts

The basic principle to remember is that the use of armed escorts by components of the Movement is not permitted unless under exceptional circumstances and with Federation secretariat approval.

The guidance document on relations between the components of the Movement and military bodies clearly states that components of the Movement may not resort to armed protection. Exceptions can be considered only in cases defined by Resolution 9 of the 1995 Council of Delegates.⁶



Remember! There is a general misconception when using armed escorts that as long as you have someone with a gun escorting you, then you will be safer. It is important to understand that the use of armed escorts is mainly for deterrence purposes and protection. In principle, you would need more and bigger guns than those of the force that is likely to attack if armed escorts were to have a foolproof deterrence function. It is also important that the ones protecting you are well trained and professional so that they do not run away if any problems arise. Should this happen, then the escort has not only given you a false sense of security, taking you to a place you normally would not go without an armed escort, but it has also escalated the situation where your attacker may shoot you because you were travelling with 'the enemy', or because they are afraid that you still have weapons.

6. The criteria are set out in the Report on the Use of Armed Protection for Humanitarian Assistance, adopted by the Council of Delegates (1995, Resolution 9). The Council of Delegates endorsed "the guiding principles laid down in Section III of the report and particularly the minimal criteria laid down for the exceptional use of armed protection of humanitarian convoys".

In practice...

In a recent operation, the government insisted that all international and non-governmental organizations working in a certain area of the country should use either military or police escorts due to insurgents and bandits. The International Federation defended its policy against this practice and, after some discussion, the government allowed us to move in the area without escorts.

Several large organizations that did use escorts experienced several extremely dangerous situations. At least two incidents took place where international organizations' convoys using armed escorts came under fire and were caught in the cross-fire between the police and the attackers. In one of these incidents, the shooting lasted almost four hours and some of the trucks in the convoy were hit by bullets.

Analysing this and other incidents, we frequently see situations where aid organizations are not initially targeted but become indirect targets and get caught up in extremely dangerous situations because they are using armed escorts.

Extreme and exceptional situations can include:

- when the safety of Red Cross or Red Crescent personnel is endangered
- when the protective value of the emblem is no longer respected
- when the refusal of an armed escort would lead to the potential death of beneficiaries

If access to victims is compromised by security risks, armed protection may only be used as a safety measure against ordinary crime and banditry (danger of theft, kidnapping or murder). The use of armed escorts must not have any detrimental effect on the beneficiaries. All possible long-term consequences must be considered.

Criteria for the use of armed escorts:

- extremely pressing needs (e.g., lifesaving operations)
- no added security risk to beneficiaries
- no one else can meet the humanitarian needs
- armed protection is for deterrence, not firepower
- parties controlling the territory are in full agreement
- offers protection against bandits and criminals

Procedures for the use of armed escorts:

- select a contractor (private company, police or military – in that order)

- no UN military escort when it is, or could be, considered a party to the conflict
- no International Red Cross and Red Crescent Movement staff in the escort
- no use of emblem by the escort
- escort vehicles should be visibly different from Movement vehicles
- escort is under the particular Movement actor's direction
- use of weapons authorized only for self-defence
- consult with all Movement components on the ground before final decision
- obtain written authorization from the director of the coordination and programmes division at the Federation secretariat in Geneva

Though somewhat less problematic than convoys, the same principles apply when considering whether to use armed forces to guard residences, warehouses and distribution sites. Law-enforcement authorities (e.g., the police) should be the first to be considered to provide security and, if that is not possible, then a private security company.

In conclusion, the use of armed escorts or guards is generally neither viable nor wise. They should only be used as a last resort and if urgently needed – not just because of their availability. The use of armed escorts will have a serious effect on neutrality and impartiality if not carried out in line with procedures. The benefits, if any, should therefore be seriously weighed against the risks.

In operations where the host country's government or host Red Cross or Red Crescent Society insist on our using military assets or escort, then the headquarters of the secretariat and ICRC may issue an official memorandum or guidance paper to address the issue, and give clear directives to field managers and the host government or National Society.

The question to ask is, if the security situation is such that it is deemed necessary to use armed escorts, then should you really be operating there? You should explore other ways of conducting your operation without exposing yourself to any threats.



Remember! In most cases an armed escort escalates the violence and the chances of firearms being used against you. For example bandits or rebels that would normally only stop your convoy to rob you, may now shoot at you in order to neutralize the threat (the armed escort) and then rob you since they do not want to risk being shot at themselves.



The decision to use security guards to ensure the security of Federation offices, warehouses or residences must be made on an individual basis and depends on the context you work in. The International Federation does not have a specific policy for delegations hiring security guards directly through Federation contracts or hiring an outside security company (usually a locally or regionally based one).

Clearly, there may be various country-specific circumstances that warrant different considerations when deciding between these two options. These could include the quality of the company, its history, ownership and ties or affiliations within the community, and any other specific issues that might make it a worse choice than hiring guards directly.

In general, delegations should preferably use the services of a professionally contracted company rather than Federation-employed security guards for the following reasons:

- Liability/insurance issues (injuries to guard or inflicted by guard on a third party, etc.).
- If the guard does not show up for work for any reason or is sick, the delegation has the responsibility of finding a replacement.
- Accountability and contractual issues are better left to an outside company.
- Various other practical issues relating to employee and employer relations.

This chapter examines the various considerations to be taken into account when selecting and hiring guards for any Federation premises. The main points to remember are that:

- ➔ The Red Cross and Red Crescent does not employ armed guards.
- ➔ A written contract must be drawn up detailing responsibilities.
- ➔ Guards are our first line of defence and, as such, they should receive the necessary in-depth training to be able to perform their duties accordingly (e.g., information on the fundamental principles and the code of conduct).
- ➔ Guards need careful briefing, equipping and strict management.
- ➔ Instructions to guards should be clear and include a detailed job description and pre-defined security procedures.
- ➔ Guards should have the appropriate communications equipment in order to be able to alert the police or call for other back-up.



Remember! In most of the places where we work today, we have some form of guard service to ensure maximum security and safety for our delegates, staff and assets.

Considerations prior to employing guards

Red Cross and Red Crescent image

- Make sure you know how the use of guards may affect the International Federation's image and the public's perception of it. Consider whether we are the only ones in the area using such services and what the crime pattern is in the area (i.e., how violent, use of arms, etc.).
- The company's staff – both the managers and guards – must be briefed on the Movement's fundamental principles and the code of conduct (see section on minimum training standards later in this chapter).

Background information

- Prior to deciding whether to use the services of a particular company, a thorough background check must be carried out. Some companies may be involved in ethically questionable activities in the country or other parts of the world. In addition to security services, others may offer military advice or be involved in combat activities as private armies for hire.
- The security unit may be able to assist in providing background information or gaining references from other organizations.

- Enquire about the company's other clients, for example, ICRC, non-governmental organizations (NGOs), embassies, the UN and others to assess their quality of service. Check the internet and various other sources to obtain maximum information about the company.
- Before making a selection, you should do all you can to make sure that you do not choose a company that might harm the Red Cross and Red Crescent Movement's image.

Contractual issues

- All issues regarding liability and insurance in the event of injury or death need to be addressed. Liability towards any person injured or killed by a guard while trying to attack Federation property – and liability towards his or her family – must be clear. If the perpetrator of such an attack is injured or killed, then consider what the International Federation's liability is.
- Does the company maintain an adequate public liability or professional indemnity policy to cover costs against any potential loss, or costs incurred as a result of any negligence on the part of the company's employees?
- A security company contract template should be requested from the legal unit or the security unit at the Federation secretariat; bear in mind that every contract must address liability/insurance and third party claims.
- The contract must comply with the host country's labour laws. Security staff should work no more than 12 hours a day and a maximum of 60 hours a week.
- Is the company a fully registered security provider in the country?
- Include contractual stipulations forbidding the use of alcohol while on duty and forbidding guards from having additional jobs during the day, for example, as this could affect a guard's performance while on duty at the delegation.
- All issues regarding shelter, equipment, clothing, meals, etc., must be clearly covered in the contract with the security company. Procedures should be in place (clearly stated in the contract) for when a guard falls ill or does not appear for duty, in order to ensure that the premises are never left unguarded.
- It is recommended that the contract includes a clause to the effect that guards assigned to the International Federation will not rotate with those of other clients. This is to help ensure that our image is not tarnished by the same guards working for less reputable clients such as local criminals, or others that might be questionable in the eyes of the public.

- A clause regarding the line of command should be included in the contract. Specify that the security company has the authority to command and control actions on the job. Leave disciplinary actions to the contractor.
- Unless authorized in advance in writing by the International Federation, the security company should not advertise or otherwise make public the fact that it is a supplier to the International Federation.
- The company must not use the name or emblem of the International Federation and/or of any National Red Cross or Red Crescent Society or any abbreviation of the International Federation's name and/or of any National Society for advertising or any other purposes.

Maintenance services

- It is important to insist that the company undertake continuous remote electronic monitoring and testing of any systems and equipment it has installed at any of our locations.
- All problems identified during this monitoring should be addressed immediately.
- The company should also provide software updates free of charge for the systems it installs.
- Labour fees should be waived by the company for any auxiliary services related to the repair of the installed systems and equipment.

Guard selection criteria

A clause for guard selection criteria should be included in the contract and should cover (if possible or realistic) the following criteria:

- appropriate age
- health
- literacy
- the prohibition of drugs and alcohol
- the requirement that guards do not undertake other employment



Minimum training standards

It is important to stipulate that all guards employed to guard Federation premises are properly and fully trained prior to assuming their duties. This will ensure they are able to carry out their work effectively and in line with the International Federation's security methods and rules of conduct.

Training should include the following:

- ✎ security techniques and procedures
- ✎ communication lines and methods
- ✎ searches (including body searches) and other access point controls
- ✎ the appropriate use of force and how to defuse tension
- ✎ firefighting basics
- ✎ laws applicable to the country's security personnel

Guards should be briefed clearly and thoroughly on their tasks. Do not assume that anything is obvious. This may be the first time the guards have encountered the Red Cross and Red Crescent Movement. Explain what the delegation does and the values that it upholds (based on its fundamental principles, the code of conduct, etc.).

Describe to the guards the kind of reputation we wish to develop among the local population. Make sure the guards understand that their role is not only to protect the office, warehouse or residence, but also to protect the image of the International Federation. Encourage them to feel part of the delegation.

Detailed briefing points should include:

- ✎ most of the normal induction points that other staff receive
- ✎ their routine duties
- ✎ hours and shifts to be worked
- ✎ the importance of remaining at their post if the guard due to take over from them does not appear
- ✎ how to communicate with their manager (this is most likely to be the head of delegation, programme manager or logistics coordinator) and with other staff
- ✎ how to respond to an incident (i.e., action to take in the event of a robbery, accident, fire, etc.)
- ✎ training in fire prevention and becoming familiar with the delegation's fire safety procedures
- ✎ how to deal with visitors to the office, warehouse or residence

- the need for prompt incident reporting
- an explanation of the disciplinary system and a warning that disciplinary action will be taken if a guard neglects assigned duties
- stressing the fact that guards should not risk their lives trying to protect property: their role is to detect intrusion and to raise the alarm

Equipment

Guards provide both physical and procedural boundaries and the equipment issued to them should be appropriate to and based on the delegation's threat and risk assessment. The following considerations should be addressed in terms of the equipment used by guards:

- conditions of the guard's shelter, access to toilet facilities, etc.
- name cards or identification badges
- uniforms or distinctive clothing to clearly identify the guard and give an air of authority
- reliable means of communication and adequate back-up using VHF radios, mobile phones (with batteries and battery charger), landline phone, etc.
- torches and batteries
- whistles
- raincoats, appropriate footwear and clothing
- logbook (if appropriate to the context)

Other considerations

Raising the alarm

Clear procedures must be in place covering how to react in different situations. For example, if an intruder is in your residence, how is the guard alerted? Should it be a silent alarm or a loud intruder alarm? Is the alarm intended to alert the guard only, or is it also connected to the security company and police? Perhaps both alarms can be activated manually in the event of a residence burglary.

It is also important to consider how the guard alerts his or her control room or the police. Make sure the control room is staffed 24 hours a day and that the company has rapid response capabilities. What are their capabilities in terms of providing back-up guards in case of emergency? VHF radio is often the preferred option (the contract should include the provision that the company supplies the guard with a radio). It is also important to know what the police's response time is.

Managing guards

An experienced, nationally recruited staff member is likely to be the most appropriate line manager for the guards. He or she should keep a close eye on guards' performance and should make random checks (pass by the office in the evening or at night).

In some situations, you may observe that it is almost standard practice for guards to sleep during the night. If this is the case, 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 and appoint a supervisor to be held responsible for ensuring that all guards stay awake.
- ❖ Remove anything that could be used as a bed.
- ❖ Summarily dismiss any guard found asleep while 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.

Guard procedures

Depending on the type of premises being guarded and the level of security required, guards will be responsible for carrying out certain procedures that aim to control access as well as to protect Federation property and staff. Whatever is decided in your delegation, it is important that guards are given clear instructions and are briefed on their responsibilities. Some typical procedures are given below as examples.

Access control procedures for visitors

- ❖ clear instructions on how to behave and what to say to visitors (e.g., guards should not give out information about who is working in the office, etc.)
- ❖ procedures about verifying who can enter the premises
- ❖ identification check
- ❖ body check (in this case, there is a need for male and female guards)
- ❖ describe how to control visitors when entering and leaving
- ❖ visitor waiting area should be in view at all times
- ❖ check with receiver of visitor if the visitor is expected

- badge system (hold ID until visitor's departure in exchange for badge)
- escort to office of staff member being visited
- how to behave if problems occur
- mail and package control – how to process and forward once checked
- vehicle access control

Logbook maintenance

- Instructions should be given on how to register information into the logbook and make sure it contains a list of key contact numbers.
- All interventions, as well as any unusual occurrences, should be noted in the logbook.
- The time at which the guard's patrols were conducted should be noted in the logbook.
- The logbook should be signed by the departing guard when handing over to the next shift.

Area of control and patrol instructions

- Provide clear instructions about monitoring the surroundings, patrolling the compound, the rules regarding gates, doors, windows, keys, etc.

Guards' reporting lines and supervision of guards

- Depending on the delegation's structure, the guards may report directly to the head of delegation, the programme coordinator or the logistics coordinator.
- Whatever the reporting line, it has to be clear to the guards and they need to know whom to contact, when and how.

Guards' responsibility in case of emergency

- What will be the responsibility of the guards in the event that an accident occurs? Whom should they contact and how should they react? Provide the guards with a list of important phone numbers.
- Make sure guards are familiar with fire safety procedures for the office, warehouse or residence, how to react and whom to contact in case of fire.
- In the event of a robbery, there is no need for heroic behaviour; the police and the International Federation's head of delegation should be contacted immediately.

- When dealing with break-ins, cases of violence or forced entry or demonstrations, there should be guidance on how guards should react (i.e., either to try to stop any intruders or not to attempt to stop them and to alert the police and the country representative).



Remember! Brief staff on the guards' job responsibilities and what they expect of them.

Armed guards

The use of armed response to a life-threatening situation involving Federation delegates or staff should generally be organized in cooperation with and through the local authorities, (i.e., the police or military). In certain countries, the authorities may not have the capability or resources to provide adequate response, or they may not be trusted for other reasons. These reasons could include corruption within their ranks, unreliability, involvement in criminal activity, or the possibility that they may be employing suspected war criminals. In these cases, a preferred option may be to contract a private security company to handle armed response.

In exceptional circumstances, the head of delegation, in consultation with the director of the coordination and programmes division via the security unit, can authorize the use of armed guards as a part of a rapid response service in emergency situations (as back-up). This applies to areas where the level of crime is such that armed response is deemed necessary.

Armed protection is not to be used in conflict areas; rather, it is to be used purely for protection against common criminality.

The sole purpose of using armed response is to protect the lives of those in an immediate, life-threatening situation, not to protect the loss of or damage to any property, assets or commodity of the International Federation.

There are a number of issues that must be considered when contracting the services of armed guards relating to policy, services performed, training and contractual issues.

1

2

3

4

5

6

Policy issues

There must be clear rules of engagement. What is the company's policy regarding the use of arms? Specify the circumstances and extent of force that may be used in certain situations. This policy must be set out in writing and correspond to the Red Cross and Red Crescent's fundamental principles.

Services

Many security firms promise rapid response. Make sure that the response time is in accordance with your needs and expectations.

What does the firm's response team consist of? How many vehicles, guards, weapons, etc? Are the vehicles clearly marked with their logo?

Specify the type of weapon that may be used in your employ, such as handguns, rifles or larger weapons. Also, make sure that both the company and individual guards have the necessary licence to carry firearms.

Training

What does the guards' training include? Is their training programme internationally accepted and accredited? Training should include, among other things:

- the use of force and deadly force
- firearms training
- laws applicable to security personnel
- security techniques and procedures

Remember that employing armed guards as a part of a rapid response service should be considered as a last option and that the International Federation does not employ armed guards as part of its regular or normal security approach.

Contractual issues

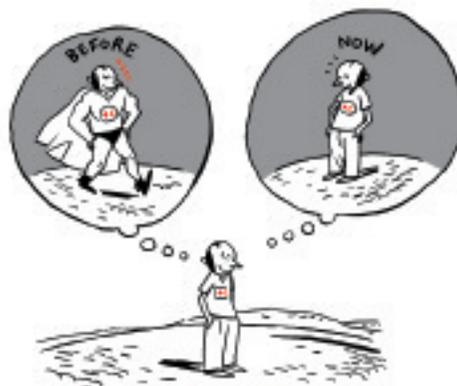
A written agreement must be drawn up with the security firm that includes the same contractual stipulations as when hiring unarmed guards.

All issues regarding liability and insurance in case of injury or death as a result of the use of arms need to be addressed. Liability towards any person injured or killed by a guard while trying to attack Federation property – and liability to-

wards his or her family – must be clear. If the perpetrator of such an attack is injured or killed, then consider what the International Federation's liability is.



Remember! A security company/guard contract template has been developed by the legal department and the security unit at the Federation secretariat, and can be requested when considering contracting security services.



1

2

3

4

5

6

Security framework and Minimum Security Requirements (MSR) for Federation field operations

Document reference number: 001

Document authorization

Stakeholder	Name	Position	Date approved
Author	Lars Tangen	Security unit	05/10/07
	John Dyer		
	Karl Julisson		
Document owner	Lars Tangen	Manager security unit	05/10/07
Document authorizer	Markku Niskala	Secretary General	15/10/07
Stakeholder	Thomas Gurtner	Director CP division	05/10/07
	Stephen Ingles	Director SS division	08/10/07
	Christophe Lanord	Legal unit	05/10/07

Version 1

Table of contents

1. Purpose and scope	89
2. Federation security framework	90
3. MSR personal conduct	91
4. MSR training and preparation	91
4.1 Senior field managers	91
4.2 Federation staff	91
4.3 Host National Societies	92
5. MSR security management	92
5.1 Briefings	92
5.1.1 In each field operation, senior field managers are to	92
5.1.2 Briefings are to include	92
5.2 Information sharing	92
5.3 Regulations and contingency planning	92
5.4 Security phases	93
5.5 Critical incident management	94
5.6 Field movement control	94
5.7 Office and warehouse security	94
5.8 Residential security	94
5.9 Communications	95
6. MSR finance	95
7. Abbreviations/acronyms	95
8. Related documents	96
9. Document revision history	96

1. Purpose and scope

The security framework and MSR improves the safety of all Federation staff by clarifying the roles and responsibilities of individuals included within the Federation security system as well as setting the minimum operational security requirements for all field operations.

The security framework and MSR applies to all field operations. All delegates, local staff, volunteers working with the Federation, visitors, Federation engaged consultants, and any other personnel operating under the Federation umbrella in the operational area are included in the term “Federation staff” for the purpose of the MSR.

PNSs that have an Integration or Service Agreement with a security component with the Federation operate under the Federation's security umbrella, but each PNS Head of Mission is responsible for his/her personnel's full compliance with the Federation's Code of Conduct and Security Regulations and Plans. PNS delegates, local staff, volunteers, visitors operating under an integration agreement or service agreement with a security component are also considered Federation Staff for the purposes of the MSR.

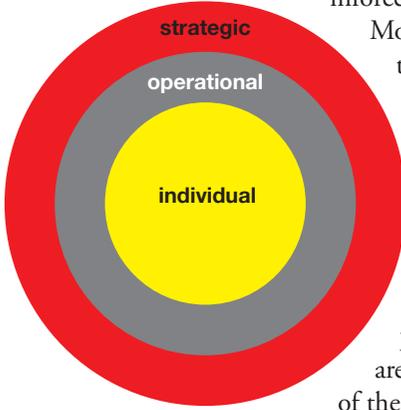
All Federation staff are individually responsible for their accompanying family members' and visitors' knowledge of and compliance with Federation security regulations, plans and procedures.

The Federation's security management is independent from the UN or the NGO community's security management structure and procedures. The Federation, National Societies, and the ICRC, each maintain their independent security structures, collaborate and provide one another with security support. In situations for which Article 5 of the Seville Agreement requires a Lead Agency other than the Federation, the Federation must conform its security structure to the guidelines provided by the Lead Agency while maintaining its own security structure and possibly further restrictions.

The implementation and maintenance of the MSR are an integral part of all senior field managers' (Head of zone, regional representative, country representative, Federation representative, team leader) responsibilities. While specific roles and duties may be delegated, the ultimate responsibility and accountability for MSR implementation and maintenance remains with the senior field manager.

2. Federation security framework

At a strategic level the Federation and National Societies are responsible for ensuring effective procedures are in place to protect and reinforce the image of the Red Cross Red Crescent Movement. They achieve this by ensuring that they operate within the boundaries of the Fundamental Principles, the Code of Conduct and have effective security policies and procedures in place to guide field operations. As employers the Federation and National Societies are also responsible for ensuring that they have effective recruitment, training and management processes in place to ensure that personnel are capable of undertaking the roles demanded of them.



Effective security is also dependent of ensuring that the image and reputation of the Red Cross Red Crescent movement is maintained at an operational field level. Senior regional, country and operations managers are responsible for ensuring that effective security planning is conducted and that sound security management structures are established. The successful implementation of these plans will also be dependent on effective monitoring of situations and maintaining working relations with other organisations and key players operating in the area.

It is expected that individuals will undertake their duties in a competent manner and be respected for the work they do. Individuals are responsible for ensuring they understand their responsibilities within the operation. They must also have a clear understanding of security plans and comply with security procedures. As field operators on the ground they are also closest and therefore should be most attuned to the environment. Not only must they therefore ensure that they maintain a high level of awareness but also that they report any changes they observe, in order that if required, plans can be adjusted.

Under this model it should be apparent that the layers are mutually supporting and therefore at each level Minimum Security Requirements must be implemented. Overall security will be diminished if any of the layers are weak.

3. MSR personal conduct

- All Federation staff are to comply fully with the Fundamental Principles of the Red Cross Red Crescent, the Federation Code of Conduct and Security Regulations.
- All Federation staff must inform themselves of the political, social, religious, cultural, and security environment, act appropriately and remain aware of and respond to changing situations.
- All Federation staff are to protect the integrity of the Federation and promote correct institutional and personal conduct/behaviour so that the acceptance of the institution is not jeopardised nor its image tarnished.
- Federation staff are to report all breaches of security regulations, including the Code of Conduct, and especially any forms of abuse, to line managers.

4. MSR training and preparation

4.1. Senior field managers

- Senior field managers are to participate in the security management training conducted by the Federation.
- All senior field managers are to receive a briefing by the Security Unit in Geneva prior to each deployment.

4.2. Federation staff

- Before Federation delegates assume their duties in field missions they are to have participated in a Basic Training Course, Field Induction Course or other Red Cross Red Crescent movement training approved by the security unit in Geneva that involves security training and explains the Federation's security framework.
- All Federation staff must know what to do in case of accidents or security incidents.
- Federation staff are to be given additional training in the specific needs of the field operation to which they are deployed. This might include, but is not limited to, telecommunication, driving, mine awareness, first aid, fire safety, and language.
- If Federation staff believe they have not been adequately briefed or trained for the operational environment in which they are asked to work, they have a responsibility to request additional information and/or training.

4.3. Host National Societies

- Senior field managers are to actively liaise with and consult the host National Society on possible security risks. They are to keep the National Society well informed about the Federation's security framework in the country of operation.

5. MSR security management

5.1. Briefings

5.1.1. In each field operation, senior field managers are to:

- Establish a security briefing system for new staff, delegates, dependants and visitors;
- Establish an induction program for new delegates; and
- Debrief delegates before departure from the delegation.

5.1.2. Briefings are to include:

- The security situation in the country and specific threats to the Red Cross Red Crescent, based upon security analysis and risk, threat and vulnerability assessments;
- The security regulations, contingency plans, incident management procedures, Code of Conduct and other security related regulations, plans and papers; and
- The security hierarchy and line management.

5.2. Information sharing

- Senior field managers are to establish a culture of information sharing and allocate time in meetings for security issues to be discussed as well as hold additional security meetings when necessary.
- The senior field manager is to maintain a record of the current location and contact details of all Federation staff under his/her security management.
- If Federation staff find that the MSR is not in place or maintained they have an obligation to inform the senior field manager responsible.

5.3. Regulations and contingency planning

- Security Regulations are mandatory in all locations where the Federation operates. The regulations must be based on sound security analysis and threat, vulnerability and risk assessments.

- Senior field managers in all locations where the Federation operates are to draft contingency plans as necessary including, at a minimum, relocation and medevac plans, and attach all contingency plans to the current security regulations as annexes.
- Senior field managers are to base security regulations on the standard Federation template, review them if the situation changes (and at least every six months), update them if required, and send a copy of the security regulations and any revisions to the security unit in Geneva.
- Federation staff are to report security incidents to their managers immediately, and senior field managers must report them to the security unit in Geneva within 48 hours, using current incident reporting procedures.

5.4. Security phases

White phase	Situation is normal	No major security concerns
Yellow phase	Situation of heightened tension initiated	Some security concerns. Heightened security awareness
Orange phase	Emergency situation	Access to beneficiaries limited. Risk to Red Cross and Red Crescent personnel severe, and tight security management needed
Red phase	Relocation or hibernation	Conditions do not allow work. Risk to Red Cross and Red Crescent personnel extreme

- The Federation operates under a standard four phase security classification system across all field operations.
- The senior field manager will establish the phase level and undertake security planning in accordance with that level.
- The senior field manager will declare red phase following (if time permits) authorisation of the director of the coordination and programmes division, in consultation with the Manager of the Security Unit in Geneva.

- If orange and/or red phases have been declared, the decision to return to a lower phase will be taken only following consultation with the Manager of the Security Unit Geneva.

5.5. Critical incident management

- Senior field managers will establish critical incident management procedures in each field location based on Federation procedures .

5.6. Field movement control

- Security regulations will include field movement regulations that direct the manner in which all field movements are to be conducted, including a definition of the operational base and approval procedures for field movements outside the operational base.
- Operational field movements must correspond to an operational goal.
- Vehicle movements are not to occur outside the operational base during the hours of darkness.
- Vehicles are to be road worthy and clearly identified in accordance with the Fleet Manual.
- All operational field movements are to have a primary and secondary means of communicating with the base location.

5.7 .Office and warehouse security

- Office and warehouse premises are to be located in a safe area based on a risk assessment.
- Office and warehouse premises are to be marked with the Federation logo, unless an exception is granted due to security concerns.
- Senior field managers are to implement security measures and access control appropriate to the risk assessment as well as suitable fire precautions.

5.8. Residential security

- Residences are to be located in a safe area based on a risk assessment.
- Residences are to be located close together if practicable and apartments on the ground floor or above the fourth floor are to be avoided.
- Senior field managers are to implement security measures and access control appropriate to the risk assessment as well as suitable fire precautions.

- Only Federation staff and accompanying family members may live in Federation residences.
- Federation staff are to ensure a minimum of seven (7) days food and water supplies are maintained in residences.

5.9. Communications

- The senior field manager is to ensure that communications is established between operational field sites and the operational base that enables real time two way communications 24/7.
- Where the general risk assessment indicates that there is a possibility of having to consider declaring yellow or higher security phases, the senior field manager is to ensure that the communications is not dependent on public or private commercial providers (e.g., land or mobile phone lines).

6. MSR finance

- Senior field managers are to include security needs/costs when planning budgets.
- Senior field managers are to implement clear rules on finance security management, covering storage, cash transport, payments etc., in accordance with financial procedures.

7. Abbreviations/acronyms

Abbreviation	Meaning
MSR	Minimum security requirements
NS	National Society
PNS	Participating National Society
HoZ	Head of zone
Reg.rep	Regional representative
Country rep.	Country representative
Fed.rep	Federation representative

8. Related documents

File number	Name	Version
	Model Security Regulations	18-10-06
	Critical Incident Management	2
	Relocation Plan Template	2007
	Security Management Training Course	2007
	Code of Conduct	Latest version
	Fleet Manual	Latest version

9. Document revision history

Version	Date	Details
001	15/10/07	Final approval by Secretary General

Security incident report



All incidents involving death, serious injury, kidnapping, or which are of special sensitivity, must be reported to the security unit by telephone immediately. A completed incident report must follow within 24 hours.

All incidents in which Federation personnel or property are involved in:

- any physical injury to any person,
- any significant damage to property (whether Federation property or not),
- any situation in which there was a serious risk of injury or damage,
- must be reported to the security unit by telephone or e-mail within 24 hours.

A completed incident report must follow within 48 hours of the incident. All other security incidents of any kind must be formally reported to the security unit, using this form, within 48 hours of the incident.

1. Country: _____
2. Delegation: _____
3. Name of movement personnel involved, and their status: (*e.g. delegate, local staff, volunteer, National Society, visitor*)

4. Length of stay in country/mission prior to incident:

5. Date, time and place of incident:

6. Type of incident: (*e.g. burglary, theft, robbery, car accident etc*)

7. Description and cause of incident: (*State all relevant details in chronological order. Attach additional pages, maps and/or sketches if applicable.*)

8. Names of Red Cross Red Crescent staff injured, details of medical treatment and current status:

9. Details of Red Cross Red Crescent assets damaged, details of nature and extent of damage, and whether insured:

10. Details of any injuries or damage sustained by third party: *(State details of injury/damage, and current status)*

11. Were local authorities (e.g. police, military, government agencies) involved at the scene or afterwards? Has the incident been reported?

12. Were staff and/or assets involved clearly marked with Red Cross Red Crescent emblem? Was Red Cross Red Crescent targeted specifically?

13. Were operational and security procedures/guidelines followed? *(If not, provide details of departures from procedures/guidelines)*

14. Was the incident the first of its kind? *(State previous incidents in chronological order and indicate date of reports)*

15. Is there any remaining threat of harm, or security risk?

16. Actions taken in response to incident and additional actions required:

17. Does the incident raise any issues of special sensitivity, importance or confidentiality?

Yes/No – If “yes”, please telephone the security unit urgently to discuss.

Signature: _____

Name: _____

Title: _____

Date: _____

Critical incident – Planning considerations

The following is not exhaustive but outlines some basic considerations when looking at the situation and developing options.

Natural disasters

- ↘ Locations of personnel
- ↘ Identification of casualties
- ↘ Evacuation of casualties
- ↘ Identification of safe areas
- ↘ Movement of personnel to safe areas
- ↘ Communication options
- ↘ Media management
- ↘ Current contingency plans
- ↘ Actions of National Society
- ↘ Deployment of FACT
- ↘ ERU deployments

After initial actions to stabilise and address the immediate concerns typical disaster management mechanisms should be initiated.

Missing persons

- ↘ Activities being undertaken at time
- ↘ Last know location
- ↘ Assessment of likely reason – hostile forces action, road action
- ↘ Search options
- ↘ Need to restrict other activities – road movement, no go areas etc
- ↘ Notification requirements
- ↘ Use local authorities
- ↘ ICRC involvement
- ↘ National Society involvement
- ↘ Liaison with home National Society/families
- ↘ Media management

Vehicle accident

- ↘ Details of accident – *photos if possible*
- ↘ Status of Red Cross Red Crescent personal – injured, in custody
- ↘ Status of other parties
- ↘ Medical evacuation requirements
- ↘ Status of Red Cross Red Crescent property involved
- ↘ Legal implications/requirement for local representation
- ↘ Liability implications
- ↘ Involvement of local authorities – police report required for insurance
- ↘ Involvement of National Society
- ↘ Liaison with home National Society/families
- ↘ Liaison with embassies
- ↘ Insurance
- ↘ Media management

Abduction/hostage

- ↘ Details of abduction
- ↘ Identification of abductors
- ↘ Assessment of rationale behind abduction – why are personnel being abducted in the country (ransom, political message)
- ↘ Involvement of local authorities
- ↘ Communications means with abductors
- ↘ Involvement of National Society, ICRC
- ↘ Requirement for specialist negotiators
- ↘ Liaison with home National Society/families
- ↘ Involvement of home embassy/governments
- ↘ Insurance
- ↘ Media management

Death of a delegate

- ✎ Details of circumstances
- ✎ Notification requirements
 - ✎ Home National Society
 - ✎ NOK
 - ✎ President
- ✎ Liaison with National Society
- ✎ Liaison with ICRC
- ✎ Police investigation if required
- ✎ Legal
- ✎ Insurance
- ✎ Post mortem if required
- ✎ Release of body
- ✎ Repatriation of body
- ✎ Protocol
 - ✎ Lowering of flags
 - ✎ Funeral attendance
 - ✎ Memory book
- ✎ Media management
- ✎ Safety and Security issues/changes to procedures if death by accident

Serious injury

- ✎ Current status – location, condition
- ✎ Professional medical input requirement for CIMT
- ✎ Medevac requirements
 - ✎ Internal/external - location and mode of transport
 - ✎ Requirement for stabilisation
- ✎ Insurance cover and notification requirements
- ✎ NOK notification
- ✎ Requirement for accident investigation
- ✎ Need for counselling
- ✎ Involvement of local authorities
- ✎ Involvement of National Society

Rape/sexual assault

- ✎ Support person identified
- ✎ Medical support – (doctor of same sex)
 - ✎ Evidential medical examination
 - ✎ urgent treatment for STD, HIV, pregnancy, injuries
- ✎ Police advised – (with victim's consent)
- ✎ Counselling – short and long term
- ✎ Witnesses or other members of the delegation support requirements
- ✎ Relocation from area
- ✎ Notification – (with victims consent)
 - ✎ NOK
 - ✎ National Society

Political/religious - Threats/violence

- ✎ Activities being undertaken at the time
- ✎ Location
- ✎ Identification of threats/violence
- ✎ Identification of perpetrators
- ✎ Assessment of likely reason. Why?
- ✎ Involvement of local authorities
- ✎ Communication means with the perpetrators
- ✎ Need for specialized (VIP) intervention
- ✎ Liaison with the National Society
- ✎ Media management

The Fundamental Principles of the International Red Cross and Red Crescent Movement

Humanity

The International Red Cross and Red Crescent Movement, born of a desire to bring assistance without discrimination to the wounded on the battlefield, endeavours, in its international and national capacity, to prevent and alleviate human suffering wherever it may be found. Its purpose is to protect life and health and to ensure respect for the human being. It promotes mutual understanding, friendship, cooperation and lasting peace amongst all peoples.

Impartiality

It makes no discrimination as to nationality, race, religious beliefs, class or political opinions. It endeavours to relieve the suffering of individuals, being guided solely by their needs, and to give priority to the most urgent cases of distress.

Neutrality

In order to enjoy the confidence of all, the Movement may not take sides in hostilities or engage at any time in controversies of a political, racial, religious or ideological nature.

Independence

The Movement is independent. The National Societies, while auxiliaries in the humanitarian services of their governments and subject to the laws of their respective countries, must always maintain their autonomy so that they may be able at all times to act in accordance with the principles of the Movement.

Voluntary service

It is a voluntary relief movement not prompted in any manner by desire for gain.

Unity

There can be only one Red Cross or Red Crescent Society in any one country. It must be open to all. It must carry on its humanitarian work throughout its territory.

Universality

The International Red Cross and Red Crescent Movement, in which all societies have equal status and share equal responsibilities and duties in helping each other, is worldwide.



The International Federation of Red Cross and Red Crescent Societies promotes the humanitarian activities of National Societies among vulnerable people.

By coordinating international disaster relief and encouraging development support it seeks to prevent and alleviate human suffering.

The International Federation, the National Societies and the International Committee of the Red Cross together constitute the International Red Cross and Red Crescent Movement.