Security Risk Management for EMTs
(Guidance for the EMT Toolkit)

Contents of this Section:

Guiding Standard Statement and Descriptor (matching Blue Book and Red Book texts)

General Reading Links (for the basis throughout Toolkit text, relevant to every subsection)

1 Security Risk Management as a Collective Responsibility
- 1.1 A Key Pillar of Duty of Care
- 1.2 Organizational Approaches to Security Risk Management
- 1.3 Writing a Security Policy
- 1.4 Building a Positive Culture of Security
- 1.5 Developing a Risk Vocabulary

2 The Security Risk Management Process [suggest to embed as pop-up text boxes within the overall diagram]
- 2.1 Establishing the Context
  - 2.1.1 External Context
  - 2.1.2 Internal Context
- 2.2 Identifying Security Risks for EMTs
  - 2.2.1 Asset Criticality Assessment
  - 2.2.2 Threat Assessment
  - 2.2.3 Vulnerability Assessment
- 2.3 Security Risk Analysis
- 2.4 Security Risk Evaluation
- 2.5 Risk Treatment Options for EMTs
  - 2.5.1 Risk Acceptance
  - 2.5.2 Risk Avoidance
  - 2.5.3 Risk Transference
  - 2.5.4 Risk Reduction
    - 2.5.4.1 Security Coordination with Partners
    - 2.5.4.2 Image and Acceptance
    - 2.5.4.3 Hardening Measures
    - 2.5.4.4 Deterrence
    - 2.5.4.5 Communications Equipment and Procedures
    - 2.5.4.6 Vehicles and Driver Procedures
    - 2.5.4.7 Information Security
    - 2.5.4.8 Staff Security Training, Briefing and Rehearsals

3 Security Plans
- 3.1 Team Security SOPs
- 3.2 Physical Site Security for Fixed EMT Facilities
  - 3.2.1 Site Selection
  - 3.2.2 Enhancing the Facility
- 3.3 Mobile Operations and Road Movements
- 3.4 Crowd Management
- 3.4 The Use of Armed Protection for EMTs
- 3.6 Team Contingency Plans

    - 3.6.1 Relocation / Evacuation Plan
    - 3.6.2 Hibernation Plan
    - 3.6.3 Medevac Plan

4 Security Incident Management

- 4.1 Incident Logging and Reporting
- 4.2 Incident Analysis
- 4.3 Security Briefs
- 4.4 Crisis Management Planning
    - 4.4.1 Distinguishing Features of a Security Crisis
    - 4.4.2 Activating a Crisis Management Plan
    - 4.4.3 Immediate Lifesaving Actions
    - 4.4.4 Establishing a Crisis Management Routine
    - 4.4.5 Information Management Tools During Crises

Guiding Standard Statement *(note: SRM is a cross-cutting theme and touches on the following two Standards in the latest Blue Book, and equally applicable to Red Book):*

1. Administration & Organizational Management: EMTs will maintain administrative and finance systems that allows them to rapidly and safely deploy teams, and maintain headquarters office support from their home base throughout missions.

2. Team Field Management & Operations: EMTs must be able to manage their day to day operations while deployed including contributing to their own safety and security management, and liaison with relevant local authorities and other stakeholders involved in the response.

Descriptor *(taken directly from the two relevant Blue Book Standards, and equally applicable to Red Book):*

1. **Security Risk Management (at Institutional Level):**

    - As codified in international and national law, the EMT organization is legally bound to provide its staff with an acceptable level of due diligence in relation to their safety and wellbeing during deployment.

    - As part of its Duty of Care approach, the EMT organization has a security risk management policy, framework and process in place that ensures security risks are systematically identified, assessed, and treated to protect staff as might be reasonably expected without unduly restricting their sustained access to affected communities which is necessary to achieve the EMT's operational objectives.

    - Based on its mandate, culture, structure and capacity, the EMT organization defines its risk appetite and makes every reasonable effort to achieve informed consent with all management and staff.

2. **Security Risk Management (at Field Level):**

    - EMT management must have the capability to conduct field-level security risk assessments and apply appropriate risk treatment measures that are captured in a written security plan for each EMT facility or working location. Additional security contingency plans are put in place for mobile operations, travel, medical repatriation, hibernation and relocation/evacuation.

    - The EMT makes provisions to deal with critical incidents and security crises that may potentially surpass routine operations.

    - Coordinate and exchange information on security matters with local authorities, other EMTs and response stakeholders as appropriate for the emergency context.

    - A designated security focal point may be assigned to prepare and implement security planning, however this is a responsibility of mainstream EMT management and best achieved through a collective planning process involving each EMT sub-team.

    - EMTs provide deploying staff with the best available information about the operational environment, security risks and associated measures, and they ensure that team members understand and accept them.

- EMT staff is supported by a team stress management plan which includes provision for both cumulative and critical event stress. Referral to specialist psycho-social support is made available, where necessary.

General Reading Links *(for the basis throughout Toolkit text, relevant to every subsection):*

Voluntary Guidelines on the Duty of Care to Seconded Personnel, 2017

For Government Teams:

- ISO 31,000 International Risk Management Standard – https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-1:v1:en
- Handbook 167 Security Risk Management – https://infostore.saiglobal.com/en-au/Standards/HB-167-2006-568733/

For ICRC/IFRC teams:

- link to Safer Access Framework

For United Nations teams:

- UN Security Management System Overview
- Programming in Access Constrained Environments (Health Cluster)

For NGO teams:

- Link to EISF/InterAction Frameworks e.g. Good Practice Review 8 Operational Security in Violent Environments

IASC Non-binding Guidelines on the Use of Armed Escorts for Humanitarian Convoys

1 Security Risk Management (SRM) as a Collective Responsibility

1.1 A Key Pillar of Duty of Care

This Toolkit recognizes that EMT organizations have a legal and moral obligation to strive towards a reasonable level of judgement and care in safeguarding the safety and wellbeing of their deployed team members as well as other counterparts within the EMT facility, such as patients and local contractors.

The core question for EMTs is how far is it worth risking a person's wellbeing – or even life – under specific circumstances in order to achieve organizational objectives.

In many cases, this is answered in routine times through regular health and safety legislation in the EMT's parent country. However, the case law around liability is inconsistent when staff are placed in exceptional circumstances, such as on deployment to a large-scale disaster, outbreak or conflict, and particularly on overseas missions.

The specifics of legal demands and expected measures will differ from one country and organization to another, and will vary from one context to another, and from one deployment relationship to another.

This makes it even more important for the EMT to follow good practice in terms of its SRM approach.

1.2 Organizational Approaches to Security Risk Management

Proximity to affected populations is a prerequisite of effective humanitarian action. The objective for EMTs and other response actors is not to avoid risk altogether, but to manage risk in a way that allows them to remain present and effective in their work.

A mature approach, representing two decades of evolution in the aid industry, recognizes that safety of relief personnel does not constitute an end in itself, but is rather a key prerequisite for gaining access to affected communities. Security, access and humanitarian action therefore share the same overarching purpose.

This Toolkit accepts that a wealth of guidelines and operational practices exist across the humanitarian SRM profession. Practices vary, leading to differences in terminology and methods which reflect the nature of the EMT.

The major SRM approaches available to EMTs are:

- The International Risk Management Standard, ISO 31000, and Handbook 167 Security Risk Management, adopted most often by government agencies
- The United Nations Security Management System (UNSMS)
- Common NGO models, outlined most notably by the European Interagency Security Forum (EISF) and InterAction
- The Safer Access Framework of the Red Cross and Red Crescent Movement

While each EMT is encouraged to adapt the most relevant guidelines and methodologies according to its own needs, the Toolkit focuses on the general considerations and good practices that apply to all EMT deployments.

1.3 Writing a Security Policy

A security policy is the starting point for the EMT's security risk management framework.

As a minimum, a security policy should contain the following:

- The organization's fundamental values and principles in relation to Duty of Care and appetite for risk
- A statement of commitment towards staff safety and wellbeing, plus the safety of other counterparts within the EMT's facility and umbrella
- A clear outline of management and individual responsibilities for staff safety, including the importance placed on compliance with security measures

1.4 Building a Positive Culture of Security

Mainstreaming a security culture means considering the security implications involved in everything the EMT does (or chooses not to do), from discussions about programme design and public messages to funding decisions and the hiring of external contractors.

People 'think security', and act accordingly because they understand the importance of it, and are respected for doing so.

The importance of security is continually reinforced, not just in written policies but also in actions.

Informed consent is achieved by providing EMT staff with the best available information about security risks and treatment measures on mission, and ensuring that staff understands and accepts these.

Tools for building a positive security culture within an EMT include:

- Holding team management accountable for decisions that impact positively or negatively on overall staff security during deployments
- Involving staff members in risk assessment and security planning processes
- Regular security briefings throughout a mission
- Integrating security awareness within the EMT's induction training
- Ensuring compliance with security measures by reinforcing good practice and penalizing non-compliance.

1.5 Developing a Risk Vocabulary (note: might be placed in a separate text box):

Definitions vary according to the framework being used and the EMT organization should agree on a risk vocabulary that is consistent with the model it adheres to.

The following key terms are those as used within the ISO 31000 risk management standard:

- Risk = the effect of uncertainty on objectives. The effect is a deviation from the expected, which can be positive and/or negative. Risk can be expressed in terms of a combination of the consequences of an event (its impact) and the associated likelihood of those consequences (its impact likelihood).

- Security risk management (SRM) = the culture, processes & structures that are directed towards maximising benefits & minimising disbenefits in security, consistent with organisational objectives.

- Security risk assessment = the combined process of security risk identification, security risk analysis and security risk evaluation.

- External context = the external environment in which the organisation seeks to achieve its objectives.

- Internal context = the internal environment in which the organisation seeks to achieve its objectives.

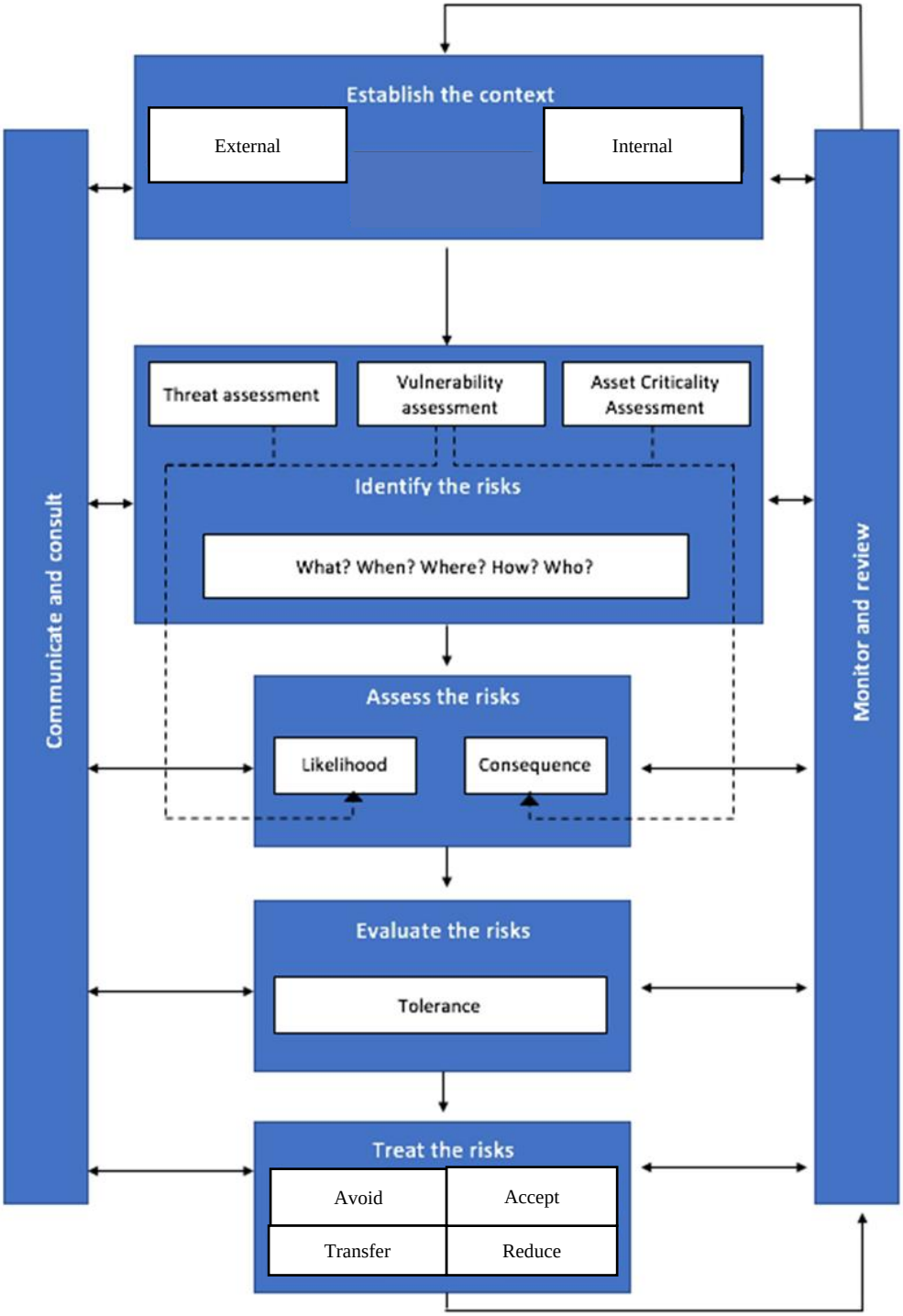
- Criticality = the importance or dependence that an organisation has on an asset.

- A threat / hazard = anything that has the potential to prevent the achievement of objectives. It can arise from either the external and/or the internal context. A security threat is a source of potential harm caused by deliberate actions. A safety hazard is a source of potential harm caused by non-deliberate actions.

- Vulnerability = the intrinsic properties (or weaknesses) of assets making them susceptible to an event with a consequence.

2 The Security Risk Management Process

Security application of the the Risk Management Process (as outlined in the ISO 31,000 International Standard and HB 167):



It is essential to both communicate and consult throughout each step using two-way dialogue with other stakeholders, and to monitor and review the outputs of each step so they remain relevant to the changing situation on the ground.

2.1 Establishing the EMT's Context

Establishing the context for EMT deployments is vital because it sets the basis on which all subsequent security risk management activities and decisions are conducted.

Assessment of SRM context can be divided into external and internal factors.

2.1.1 External Context

The aim of an external context assessment is to understand:

- Where the EMT is deployed
- The drivers underpinning the emergency and therefore the risk environment in which we are working
- The indicators for potential changes in the environment

As a minimum, the EMT needs to consider the following five topics:

a. The history and politics of the affected region / country / province / district
b. How the society and culture are structured – including local norms / codes, religions, ethnicities, ideologies – and any conflicts of tensions in play
c. The economy, infrastructure & crime levels
d. The physical geography, infrastructure & climate
e. Actor map of the local, national and international stakeholders involved in the response

2.1.2 Internal Context

The aim of an internal context assessment is to understand the deployment organisation's inner environment and any issues that may influence exposure to security risks or the activities being undertaken to manage them.

Key elements to review include:

- The current mandate, structure and capability of the EMT organization as outlined in its security policy documents
- Values and culture intrinsic to the EMT organization – in particular, what the prevalent attitude towards risk is, and how consistently this is applied. Each EMT will sit on a spectrum; at one end are those teams which appear to be completely risk averse, while at the other end are those which recognize and prepare for the risk of serious harm and even death.
- Mission statement specific to the deployment, including:
    - The intended humanitarian impact of the EMT's deployment
    - What activities this may involve
    - The time period for operations
    - The geographical areas where it will take place
    - Key limitations that may impinge on the deployment

2.2 Identifying Security Risks for EMTs

Based on a solid assessment of the external and internal context, the EMT is then able to identify security risks that will affect its operations.

Risk identification is intended to give a more accurate understanding of the interaction between:

a. The EMT's critical assets
b. The security dangers these assets face
c. Any inherent weaknesses of the EMT which may potentially be exploited.

2.2.1 Asset Criticality Assessment

The asset criticality assessment identifies all properties of the EMT that may be exposed to, or harmed by, a security threat.

The aim is to place a descriptive value on each asset in terms of its importance to the EMT's mission objectives, as well as determine the capability of the EMT to resume normal operations if that asset was damaged (i.e. its resilience).

EMT assets might typically include:

- Personnel e.g. number of team members, types of expertise
- Vehicles e.g. number of carriers for personnel versus goods / equipment
- Equipment e.g. medical equipment, relief items, fuel, food, water, refrigeration, power supplies
- Pharmacy and medicinal stock
- Infrastructure e.g. physical medical structure, accommodation,
- Finances e.g. available cash-flow to use locally, access to broader financial resources
- Information e.g. confidential patient records, epidemiological data, computer servers
- Organizational reputation e.g. with other response actors, with the affected communities and general public

In assigning the criticality ratings, ask:

- How critical would it be to the mission objectives if that asset was damaged or lost completely?
- What would be the immediate consequences?
- Would the mission find ways to succeed?
- Would there be unseen, secondary effects?

2.2.2 Threat Assessment

A good threat assessment aims to clearly identify the range of potential dangers arising from the external and internal security environments, and their relevance to EMTs assets during a deployment.

The categorization of threat sources varies according to the assessment methodology used, but typically those within the following broad categories would be considered:

Armed conflict	**Terrorism**	**Crime**	**Civil unrest**	**Hazards**
Small arms attack	Car bomb	Hostage taking	Peaceful protest	Vehicle accident
Artillery fire	Hostage taking	Sexual assault	Violent demonstration	Illness / disease (list specifics)
Landmine strike (anti-personnel)	Political assassination	Carjacking	Looting	Natural disasters (list specifics)
Landmine strike (anti-vehicle)	Suicide bomb	Robbery	Patient aggression	Fire in hospital

Each threat might be directly targeted towards the EMT, or indirectly affecting their operations by virtue of being in the wrong place at the wrong time.

The output of the assessment is to write a series of threat event statements that include the "what, when, where how and who" for each potential danger.

It is vital to remember that decisions should not be made (and security measures should not be introduced) on the basis of "threat," but on "risk". In other words, it is entirely possible to be confronted with a high threat level that poses low risk to the EMT in a given area, depending on the EMT's vulnerability profile.

2.2.3 Vulnerability Assessment

The purpose of vulnerability assessment is to provide a better understanding of the weaknesses of the EMT's critical assets in relation to each threat event.

Every EMT organization in an area may face a similar threat environment, however their internal composition means they are rarely vulnerable to an equal degree.

Likewise, local health workers will have a different vulnerability profile from EMT staff who have deployed in from other areas, even though they might be working alongside each in the same clinical facility.

The most common approach for examining vulnerability is to assess the effectiveness of existing controls in managing each of the identified threats.

It is important here to remember that the concept of vulnerability can extend beyond physical controls and a thorough assessment will need to consider soft measures as well as hard ones. The following checklist of vulnerability factors is a good start.

Hard (physical) security controls:

- Location(s) of EMT operations
- Degree of exposure to identified threats
- Physical barriers in place
- Vehicles
- Communications equipment
- Other equipment, such as personal protective equipment

Soft (non-physical) security controls:

- Degree of image and acceptance towards the EMT
- How visible are the assets
- Perceived value of assets
- Information security measures in place
- Standard operating procedures (SOPs) in place
- Level of staff training
- Level of staff compliance
- Internal response capacity
- Access to outside help

Comparing how the EMT rates against other organizations operating in the same area will yield useful information when moving on to the next step in the process, risk analysis.

2.3 Risk Analysis

The purpose of risk analysis is to assign an overall level for each risk that was identified through the EMT's asset criticality, threat and vulnerability assessments.

A concise summary of the risk analysis stage would be to rank the risks in categories from 'very high' through to 'very low,' and state how many risks belong in each category, before any additional security measures have been put in place.

This is commonly done by assigning a value or descriptor to:

1. The *consequences* of each risk event (its impact), which may be either negative and/or positive*
2. The *likelihood* of those consequences (its impact likelihood)

Note that security risk analysis is not an exact science; rather, it is a process of structured subjectivity. It is therefore vital to view the final findings of risk analysis as a baseline for informed further discussion, not as a precise mathematical certainty.

*Traditionally, aid organizations tend to focus risk analysis exclusively on the negative impacts of security risks, but the same ranking process can be applied to positive impacts. Examples of benefits to security risks for EMTs include:

- Reputational enhancement
- Positive media coverage
- Improved security coordination and response planning

- Improved organizational resilience
- Building an esprit de corps amongst team members
- Stronger relations with affected communities
- Improved conditions for future access

2.4 Risk Evaluation

The purpose of risk evaluation for EMTs is to decide which of the security risks are tolerable as they are, and which require further management action so that the EMT's organizational objectives can be met.

Each EMT will have a different amount of risk that it is able to absorb. For example, one team might consider that serious injury or death sustained to a staff member on mission, while clearly not a satisfactory event, would nevertheless not deter the EMT from achieving its mission. Another EMT might feel that it would be unable to absorb such a situation. A third team might make a different decision depending on whether the cause of the incident was a car accident, for example, as opposed to a politically-motivated, targeted attack from a terrorist group or a high-profile infectious disease such as Ebola.

The negative risks of a deployment should be proportionate to the expected humanitarian gains, as implied within the mission objectives. For example, sending a mobile EMT into an isolated area to provide life-saving medical assistance for unattended casualties would justify a greater level of risk than a routine trip to meet with local partners, which might easily be postponed.

The EMT must also refer back to its statement of risk appetite and internal context assessment so that field-level decisions are made in a manner consistent with the organization's mandate, culture, structure and capacity.

2.5 Risk Treatment Options for EMTs

Where a security risk has been determined as intolerable, some form of additional treatment may be required to manage it.

It will never be possible or even desirable to completely remove all forms of security risk. The aim of a treatment plan is to manage the negative consequences of risk to a tolerable level, while exploiting any potential benefits or opportunities that may arise.

After treatments have been implemented there will usually be some degree of residual risk. The EMT must decide whether this residual risk is tolerable and can be retained, or if further treatment is required.

Risks should be treated in priority order, starting with those with the highest risk level.

In general, there are four main options for treating risk.

2.5.1 Risk Acceptance

Retaining the risk is a valid strategy when the risk level is tolerable, or the positive opportunities created by accepting this risk outweigh the potential harm.

The EMT may actively exploit the situation further by generating positive publicity and support, or by using it as an opportunity to build stronger relationships and systems.

Alternatively, risk acceptance may be the preferred option in circumstances where adding more security measures would slow down operations unnecessarily.

In other cases, the risk may be acknowledged as intolerable, but at the current time, capability or resources are unavailable, or treatment is not cost-effective. Therefore, the only option may be to retain the risk and to continue to monitor it through regular updating of the security risk assessment.

2.5.2 Risk Avoidance

Broadly, this option has three forms:

• Reduce geographic exposure by limiting or curtailing operations in certain high-risk zones, declaring no-go areas, etc.

• Reduce temporal (time) exposure by limiting hours of operation in sensitive locations, limiting time of travel to daylight hours, establishing curfews etc.

• Reduce staff exposure by setting overall staffing ceilings or establishing limitations based on categories of staff (due to sensitive nationality, gender, national/international status etc.)

The extreme forms of risk avoidance is requesting a different tasking or, ultimately, refusing or cancelling the deployment altogether.

2.5.3 Risk Transference

This refers to measures designed to shift dangers to another party, such as another EMT, or a local health authority, hospital or clinic. In these cases the danger does not go away, rather it is distributed more widely so that it becomes acceptable for all.

Risk transference may be appropriate for EMTs when:

- The party to whom risk is transferred is mandated or better equipped to deal with the risk
- A number of parties are sharing in the benefits of a particular programme it may be appropriate for them to share the risks equally

However, risk transference for EMTs also has disadvantages:

- It may result in loss of control
- It may result in transference of some of the benefits, such as from positive publicity or acceptance

- There may be issues of responsibility and accountability, both moral and legal, to be considered. This is especially relevant for EMTs during the final handover phase if they are expecting local partners to continue absorbing risks with limited capacity to manage them

2.5.4 Risk Reduction

This is the most varied and comprehensive bracket of measures, aimed at lessening the risk by introducing extra control measures.

Prevention measures are aimed at reducing the likelihood during the period leading up to the risk event. Mitigation measures are aimed at reducing the harmful consequences following the event.

EMTs have a broad range of measures at their disposal, and a balanced and comprehensive security strategy will almost always include a blend.

Below is a description of some common prevention and mitigation control measures that may be selected by the EMT to reduce a particular risk.

When introducing a new measure, the EMT should take care to monitor how this affects the effectiveness of its other measures. Sometimes, an EMT that makes itself safer in relation to one threat can unwittingly increase its vulnerability to a different threat.

2.5.4.1 Security Coordination with Partners

Coordination measures serve two important security functions:

- It can help the EMT obtain important information that affects security before it is too late
- It can facilitate quicker and more effective response in the event of a security incident

Improved exchange on security matters can be sought with the following partners:

- The national Health EOC
- Local government counterparts, such as the district health authority, local emergency management authority, and/or police
- Other EMTs
- Other nearby humanitarian/development agencies
- Local leaders and patient communities

2.5.4.2 Image and Acceptance

Image measures aim to decrease the likelihood of an attack by reducing the potential attacker's desire to do harm to the EMT. For many EMT organizations, especially NGOs and Red Cross / Red Crescent organizations, this is the preferred strategy.

Common image enhancing measures include:

- A clear and proactive public information campaign to explain the EMT's programmes
- Regular and positive interaction with the local population, including patients, families and community leaders
- Services that are seen to benefit the population and that distribute benefits fairly and transparently, in alignment with humanitarian and EMT guiding principles
- Staff behaviour within the EMT facility that respects cultural norms

Although every EMT must seek at least a moderate level of acceptance within the affected population in order to deliver clinical care, the degree to which an EMT relies on image and acceptance will depend on the operational context and organizational ethos. In settings where terrorism is a high risk, for example, acceptance strategies alone are not recommended.

2.5.4.3 Hardening Measures

Hardening measures are intended to make it more difficult for an attacker to reach the EMT's critical assets by creating a physical barrier.

EMTs must balance the advantages and disadvantages of each possible measure in the context of their specific situation and the operation as a whole. Nevertheless, some degree of hardening measures is almost always a part of a comprehensive security strategy.

Typical hardening measures for EMTs are outlined in detail under sections 3.2 (Physical Site Security for Fixed EMT Facilities) and 3.3 (Mobile Operations and Road Movements).

2.5.4.4 Deterrence

Deterrence measures are actions that the EMT might take to reduce the likelihood of threat events because of negative consequences for the attacker.

Common deterrence measures for EMTs include:

- Overt displays of professionalism and rigour, thereby encouraging potential attackers to seek easier targets
- Unarmed guards, either recruited locally or provided by a reputable security firm
- Overt relations with local security forces, such as police, military or peacekeepers

- Closed-circuit television (CCTV)
- In certain cases, the threat of suspending an EMT's operations can be a form of deterrence to threatening behaviour

Note that the use of deterrence measures come with a number of important considerations, including the level of training and awareness of the guards or security forces, the impact on the EMT's mission and mandate, and the impact on perceptions of impartiality and neutrality.

2.5.4.5 Communications Equipment and Procedures

These could arguably be included under "hardening measures" but their importance for field-based EMTs merits special mention.

It is recommended to ensure a mix of the following communications equipment is used:

- Landline telephones
- Mobile telephone and mobile data
- VHF and HF radios (are you familiar with the range/terrain limitations? Are additional base stations or repeaters needed?)
- Satellite telephones (is there appropriate satellite coverage in your area?)
- Various data transmission systems

Important considerations include the following:

- Does the EMT have an assured means of communicating with all staff in an emergency, and vice versa?
- Does the EMT have a way of communicating with critical partners and headquarters?
- Do staff working in areas at risk have a means of communicating with each other?
- Does the EMT have reliable communications with staff during road travel or on mobile operations, where they are often particularly vulnerable?
- For all of the above, is there a backup means of communications?
- Is communications equipment well maintained and do staff know how to operate it?
- Are there appropriate communications protocols/procedures in place, and do staff know and comply with them?

2.5.4.6 Vehicles and Driver Procedures

Like communications equipment, road vehicles deserve special attention due to the vulnerability of staff during travel.

Key questions include:

- Are EMT vehicles appropriately chosen and equipped for the threats in that area?

- How do the vehicles impact on how the EMT is perceived by potential aggressors?
- Are they appropriate for the terrain and natural hazards?
- Are there appropriate procedures in place, such as a mission tracking system?
- Do staff know emergency actions in the event of a road incident?
- Who are the drivers and do they have appropriate training?

Special considerations will apply to EMT operations involving other means of transport e.g. boat travel.

2.5.4.7 Information Security

Security of information should be part of the EMT's routine operational planning and reporting, particularly in relation to data confidentiality and organizing patient transfer to/from other health facilities.

For team safety purposes, it is recommended to introduce a social media policy for all staff during deployment.

The EMT may also choose to safeguard the following information:

- Names of staff
- Locations and movement plans
- Routes and timings of travel
- Storage arrangements for other (non-staff) critical assets such as pharmacy, food or fuel
- Financial matters
- Staff casualties in the event of an incident

Another aspect of information security is to ensure that the EMT always maintains safe back-up of key operational information, ideally off-site, that can be retrieved in case of emergency.

2.5.4.8 Staff Security Training, Briefing and Rehearsals

EMT staff members who are knowledgeable and alert about security risks and procedures are more likely to avoid security incidents, or to handle them effectively if they occur.

It is important to include regular briefings and rehearsals during deployment as part of the team SOPs – see section 3.1

Briefing and rehearsals should also be a continuation of the staff member's prior training on security-related topics. A menu of security modules is offered in the common training package for EMTs, which

each organization can select from and adapt according to learning needs. Training topics available include:

- Overview of organizational security
- Personal security
- Field movement
- Crowd management
- Dealing with specific threats:
    - Communications and navigation
    - Defusing hostility
    - Isolating incidents
    - Mines and explosives
    - Natural hazards
    - Sexual assault
    - Vehicle checkpoints
    - Weapons awareness

3 Security Plans

Good practice requires that every fixed EMT facility or mobile operation should have a team security plan each time it deploys, although the level of detail within the plan may vary greatly according to the threats and other factors.

Security plans fulfil the following important functions:

- They allow team leadership / security focal point to communicate important security information and procedures to others
- They facilitate discussions of important security issues within the team
- They improve staff understanding and awareness, and therefore compliance
- They reduce coordination and response time in an emergency
- They guide decision making
- They support managerial accountability by showing due diligence
- They provide a level of reassurance to staff

For EMT security plans to be truly effective:

- They must flow from a good understanding of the context – and be tailored to fit this
- Be consistent with the security risk assessment and selection of treatment measures
- They must be well understood by all staff members, practiced and enforced, and the content regularly reviewed. The value gained from the planning process itself – meeting with partners, identifying problems, brainstorming options – is often more important than the document that results from it
- Although the plan may be prepared by a designated security focal point, it should be approved by team leadership, who must be very familiar with its contents
- Plans should be drafted at the very start of the deployment and updated regularly – especially if there is a significant change in the threat context (e.g. one or more high impact events occur) or vulnerability profile (e.g. the team's mission locations change to focus on new geographical areas)
- They are generally considered sensitive documents and should be maintained in a safe place; however, all staff must be aware of the basic elements of the plan that will affect them

The format for a written security plan will differ according to organizational norms, however the following elements are typically included:

- An overview of the context and security risk assessment
- Identification of key personnel in the team's security risk management chain and their contact information
- Updated staff lists
- A communications plan, including mobile phone numbers, radio frequencies in use, call signs, satellite telephone numbers or other means
- Maps, of both the country and locality, showing transport routes, no go areas, safe locations, embassy offices, airports, ports, and hospital facilities among other features
- Team security SOPs (see section 3.1 below)
- Contingency plans (see section 3.3 below)
- A continuity plan to safeguard local staff and partners in the event that the EMT is relocated at short notice, and to enable medical operations to continue

3.1 Team Security SOPs

Team security SOPs are preventative risk control measures that require individual understanding and compliance by EMT team members.

Team members should be briefed and trained in SOPs at the start of each deployment.

Security SOPs are recommended for the following topics as a minimum, although the EMT should add its own according to the context:

- Personal security & safety
- Personal protective equipment (PPE) for clinical or waste management duties
- Chemo-prophylaxis and protection from vectors
- Access to safe water and food
- Avoidance of specific threats and hazards within the environment
- Local laws & customs
- Communication procedures
- Staff tracking system
- Incident reporting
- Site security (see section 3.2 below)
- Vehicles, travel & movements (see section 3.3 below)
- Stress management plans, including the buddy-buddy system
- Financial security
- Information security, including social media and media

3.2 Physical Site Security for Fixed EMT Facilities

3.2.1 Site selection

To a greater or lesser degree, the EMT may be able to influence the selection of its assigned work and/or living sites.

When assessing the location of a potential new site the EMT should:

- Investigate levels of crime in the area, the types of incidents that have occurred and whether response actors in that area been targeted before.
- Establish whether the site is located near other agencies facilities, as there may be an increased risk in being more isolated.
- Check if the area or property is affiliated with a particular group as this could either increase the security risks or provide a level of protection.
- Determine whether the site is close to potential targets, e.g. government buildings or military installations.
- Determine whether the site is in close proximity to potential areas for demonstrations or civil unrest, e.g. markets, religious buildings, universities, diplomatic areas.
- Consider distances and routes between the site and your other structures (residences, office or warehouse) as there may be security risks associated with moving between these sites.

- Examine how accessible the site is, i.e., whether access is restricted or open to the general public. Check that there are multiple access routes to facilitate evacuation from site in an emergency.

As well as considering the security risks associated with a particular location, the EMT must evaluate the physical structures of the site. Where possible, prior reconnaissance should be conducted by the EMT security focal point in collaboration with an overall team leader, clinical operations expert and support logistician.

In some cases, a facility may be already fully or partially established, in other cases the EMT may construct its own structures. A thorough site survey will help to identify vulnerabilities to threats and possible ways to reduce these. It is recommended to survey first the site exterior and then the interior, approaching the task through the eyes of a potential attacker or threat source.

Key considerations include:

- Assess the physical condition and strength of the buildings or tents. Also consider their susceptibility to any likely hazards (fire, flood, strong winds, and earthquakes).
- Examine the boundaries of the site, make sure there is a well-defined boundary and that perimeter walls or fences are secure.
- Inspect the condition of access points, including doors, gates and windows. Ensure all have adequate locks and there are separate entry/exit points for staff versus patients.
- Make sure that the site is well illuminated, particularly access points, parking areas and the area immediately surrounding the site.
- Check the condition of key services such as electricity, gas and water supply. Ensure that appliances are safe and that electricity sockets and wiring are in good order. Consider possible escape routes in the event of a fire.
- It is important to have a secure parking area, ideally within the facility site, to avoid the need for parking vehicles outside.

It may be necessary to change the location of where the team lives and works if the site is inadequate or if the security situation deteriorates.

3.2.2 Enhancing the Facility

Finding an appropriate site is only the first step. Depending on the security situation, every EMT facility may need additional protection measures and procedures to improve safety.

The team should ensure it has permission to carry out such alterations to the site in order to improve security.

Any new physical measures must reflect the threats that could affect the facility, and be proportional to the risks identified. A systematic risk assessment process helps to justify decisions. Upgrades to physical security measures should be anticipated and included within the team's deployment budget.

Options for physical enhancement of the EMT facility include:

- Strengthening the perimeter walls, fencing and gates
- Razor wire
- Ballistic resistant barriers
- Expanding the stand-off distance between entry points and staffed locations inside
- Clearing debris surrounding the facility
- Creating more extra entry / exit points – every building or compound should have more than one
- Providing additional lighting
- Installing alarms
- CCTV
- Fitting locks, bars or grills to access points, stores and pharmacy
- Fortifying a safe room / safe haven (see Section 3.5.2 Hibernation Plan)

Physical security measures are only useful if they are backed up by good procedures to control access to the site and specific parts of the site. The following are common procedures that are used to support physical security measures:

- Guards - In order for guards to be effective, due care and attention should be paid to the conditions under which they are recruited and subsequently managed. There are a number of important issues to be considered including guard selection, contract and agreement, equipment, training, and engagement.
- Crowd management – see Section 3.3 below.
- Visitor Procedures – EMTs often receive a lot of visitors beyond patients from the affected community. All visitors should show identification before entering. Guards should be briefed on who can enter the office and who should be told to wait outside. All visitors should be accompanied while on the premises.
- Signing in Book – Staff and visitors should be sign in and out of a compound. This not only records who has been on site but is also used to ensure everyone is accounted for in the case of emergency.

- Key Control – all keys should be tightly controlled. Stolen or lost keys should be reported immediately, and locks changed.
- Neighbours – If the escape route involves passing through a neighbouring property, make sure that this has been discussed prior to it being needed.

Remember that the choice of site facility and the protection measures an EMT adopts will affect its image and profile. Over-fortification can undermine the image of a team's activities by the wider community or attract too much attention.

The EMT should also consider the profile of other partners, organizations and facilities operating in the local area before introducing site enhancements of its own. Does the EMT have obvious vulnerabilities when compared with other potential targets? Will any new physical measures influence how partners are perceived?

3.3 Mobile Operations and Road Movements

By definition, mobile EMTs will spend a significant amount of time working at, and moving between, temporary project sites within their designated zone of coverage. This must be reflected in the team's vulnerability assessment and the blend of risk treatment measures decided upon.

Even fixed EMT teams will need to manage frequent road movements as staff must attend coordination meetings, liaise with neighbouring medical providers and organize resupply of consumables.

Special attention should therefore be given to how overland road travel is planned and conducted.

3.4 Crowd Management

By nature of their mandate, both mobile and fixed EMTs will often be required to attract crowds of patients in order to deliver emergency healthcare. EMTs have a responsibility, therefore, to incorporate good crowd management planning to ensure operational effectiveness and apply proper Duty of Care for its team members.

There are different types of crowds, each with its own level of danger. It is important to understand the factors which may lead to an escalation; these include:

- A lack, or conflict, of information e.g. community are expecting food supplies, not medical care
- A worsening of the physical conditions e.g. no shade or water in the waiting area
- Poor organisational planning e.g. unnecessary waiting times
- Fear of missing out on assistance
- Trigger events e.g. a small number of patients taking matters into their own hands

Before delivering assistance, EMTs should consider:

- How many people are likely to arrive en masse?
- What are their needs?
- Who are the most vulnerable groups?
- What is likely to influence the crowd's behaviour?
- How will people arrive, and from which direction?
- How is the community hierarchy organized? Are there natural leaders who might be useful in managing the crowd?
- What are the crowd's perceptions and cultural norms in terms of triage and waiting?
- Are there rival tensions (e.g. ethnic, religious, political) involved?

Controlling the physical environment:

- Where possible, EMTs should avoid making patients and their families wait in unsheltered conditions during the hottest/coldest part of the day
- Use infrastructure or fencing to channel the flow of people and prevent the build up of crowd density in one space
- Controlling entry and exit points
- Removing heavy or sharp objects from public areas that may be used as weapons
- Ensuring good communications, observation and back-up between staff members in different roles

Coordination activities:

- Discuss with local partners, security authorities and other parties in advance
- Physical rehearsal of EMT staff in how to respond to crowd escalation
- Pre-identify the conditions for withdrawing staff from the crowd situation and have exit plans in place beforehand. Consider:
    - What will be the method of communications for staff to leave the site across multiple locations
    - How the team's vehicles are parked
    - Where the drivers and keys are located
    - What the exit routes will be – primary and back-up
    - What will be the role of local authorities during the team' exit

3.5 The Use of Armed Protection for EMTs

The use of armed protection for EMTs in conflict settings should be used only as a last resort, in exceptional cases, and then only when a set of key criteria is fulfilled.

3.6 Team Contingency Plans

Contingency plans can be defined as a forward planning process in a state of uncertainty in which scenarios are agreed, and potential response systems put in place to respond to an emergency.

The aim is to outline the detailed actions and procedures of mitigation to take in the event of foreseeable high-risk incidents, to reduce response time.

The EMT should prioritise those risks that:

- Are most likely to happen and could have the greatest potential impact
- Require a lot of information and preparation in order to respond
- Which require the response to be carried out quickly and in a coordinated manner

Contingency plans can be included in the main body of the EMT's security plan or attached as separate annexes.

Contingency plans should:

- Be written in clear, simple language listing the necessary actions in a step by step manner
- Assign likely roles and responsibilities, and identify coordination mechanisms
- Identify shortfalls in equipment or other resource categories (people, training, funds) to accomplish these steps
- Involve likely partners in the process. Doing so can facilitate a common understanding of the problem, reduce duplication and gaps, increase efficiency by allowing pooling of resources, and improve coordination and response time in a crisis.
- Be shared with all personnel who need to know its contents. Briefing and training are ways to accomplish this but live rehearsals of plans are best of all. Create a contingency culture within the EMT.

Supporting documents for team contingency plans include:

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

It is impossible to predict all aspects of every security scenario, however there are some common contingency plans that can be adapted for each deployment – see sections 3.6.1 to 3.6.3 below.

3.6.1 Relocation / Evacuation Plan

A relocation plan relates to the unscheduled, hasty withdrawal of an EMT from its tasking location to another part of the same country, due to abrupt deterioration of the security conditions. Relocation plans are recommended for both national and international EMTs.

An evacuation plan involves the repatriation of the team out of the country altogether, and thus only applies to international EMTs. There are some additional considerations for international evacuation, however most considerations are equally relevant to relocation plans.

Operational continuity is an important feature of an EMT's relocation and evacuation planning process, and must be included.

The purpose of operational continuity planning is to preserve essential activities so that the EMT's organizational objectives may still be achieved, despite the withdrawal of most/all EMT staff.

The following are key considerations for operational continuity planning:

- What essential activities need to keep running?
- What activities can operate with skeleton teams?
- What local capacity is available to deliver medical care following the EMT's unscheduled withdrawal?
- What is the best possible outcome and what should be the minimum outcome?
- What moral challenges apply in terms of transferring risk to other parties who remain?
- Are there ways for the withdrawing EMT to continue providing remote support e.g. with logistics, donated items or technical expertise?
- Are alternate delivery methods or new ways of working available, such as the redistribution of patients to other areas?
- What role will the Ministry of Health's coordination arrangements play?

3.6.2 Hibernation Plan

Voluntary hibernation can be a good option when staying is safer than moving, or when time is needed to evaluate the ability to move. However, bear in mind that hibernation can also put staff at risk: just because an EMT has not been targeted in previous crises does not mean that it is forever secure.

Forced hibernation can result from a rapid unfolding of indirect threat events (e.g. protests at a nearby food distribution depot) that could not be anticipated, or can be imposed if withdrawal becomes impossible (e.g. the scheduled plane does not arrive).

Both voluntary and forced hibernation involve a temporary suspension of clinical service delivery.

3.6.3 Medevac Plan

4 Security Incident Management

4.1 Incident Reporting and Logging

Timely, sufficiently detailed collection and dissemination of security information during a deployment contributes to the safety of all.

A simple incident log should be maintained throughout the mission to help monitor security trends within the EMT's operating area, to inform security briefings and – potentially – to act in support of the EMT's legal defense.

At the start of a new deployment, it is also recommended for the EMT to decide on the types of security reports it will use, as well as the thresholds for including incidents within each type.

As a general recommendation, EMTs should report the incident immediately if:

- The incident involves the arrest, detention, serious injury or death of a staff member
- A staff member was injured or property was damaged in a malicious act
- Staff had to take immediate actions to prevent possible serious injury/property damage
- The incident could have a serious and immediate impact on the safety of staff
- The incident involves a personal threat to a staff member
- The incident is likely to receive substantial media cover

An incident should be included in a periodic report if:

- It indicates a general tendency or trend in the security situation
- It could impact the EMT in the medium/long term
- The incident involves partner organizations not directly related to EMT activities
- The incident is minor (no injury/minimal damage) and has no impact on EMT operations.

It is recommended not to report the following:

- Random incidents not involving EMT staff or partners that indicate no significant trends
- Information that will make the EMT's report appear to be a military or intelligence report

4.2 Incident Analysis

A common problem with security incidents is the human tendency to either ignore information or over-react in the immediate aftermath.

A balanced approach to post-incident analysis is therefore important for EMTs to see whether they indicate changes in the level of threat or risk and to revise existing procedures.

4.3 Security Briefs

Security briefs are important tools for:

- Supporting the arrival of newly-arrived staff
- Handing over operations to other EMTs or local health providers
- Sharing security information with neighbouring partners
- Managing VIPs, media and other visitors the EMT facility

The amount and type of information included within a security brief may have to be tailored to different audiences. Not all information may be suitable for wider circulation at a given point in time.

4.4 Crisis Management Planning

4.4.1 Distinguishing Features of a Security Crisis

The majority of security events during deployment are normally dealt with through the EMT's existing management structure. Generally this is defined as incident management.

Occasionally, a crisis event may occur. Crises are recognized by the following features:

- Exceptional severity which goes beyond the scope of routine EMT management procedures
- Widespread implications for the whole organization
- An element of novelty which does not follow a predictable path
- High impact on mission objectives and reputation
- Uncertain or ambiguous causes or effects
- Information may not be too little, too much, or difficult to verify
- Lifesaving decision making is required urgently
- High pressure situation
- Communication is difficult to manage
- Outside actors are involved, both directly and indirectly

4.4.2 Activating a Crisis Management Plan

The successful management of any crisis situation is dependent on the preparedness of the EMT organization and its ability to respond effectively to the challenge.

At the field level, it is recommended for the EMT to activate alternative management arrangements to temporarily coordinate and make any critical decisions. As a general principle, the closest management structure to the crisis should take the lead. Then as the situation evolves, decisions will typically move further up the organizational ladder.

To support the field-level crisis management team, a written Crisis Management Plan (CMP) is recommended. The CMP will:

- Define what security events would constitute a crisis for the EMT
- Identify a crisis management team at the field level which can coordinate and analyse the on-site response to a crisis
- Clearly outline the roles and functions of this crisis management team, including authority to make decisions

- Outline relevant in-country operation support (e.g. other entities who can contribute or take ownership of certain aspects)
- Identify support from headquarters level, including the activation of any higher Crisis Management Team
- Provide details of immediate lifesaving actions to consider – see section 4.4.2
- Provide details of actions to consider once the crisis management phase has reached routine status – see section 4.4.3
- Identify information management tools – see section 4.4.4

4.4.2 Immediate Lifesaving Actions

The following actions should be considered within the early stages of a crisis response:

- Formally trigger the crisis management plan
- Determine what information you need to know
- Determine what decisions need to be made and when
- Decide who needs to be notified immediately
- Confirm information/identity of casualties
- Account positively for all staff
- Limit movement of non-affected staff or relocate as necessary (designate no go areas)
- Restrict communications to essential information flow, ensure team members comply with communications restrictions including social media
- Log key events
- Send initial incident report
- Request priority support assets
- Alert authorities
- Alert other partners in area

4.4.3 Establishing a Crisis Management Routine

The following actions should be considered once the crisis management phase has reached routine status:

- Establish rotation of the crisis management team, including duty manager
- Establish liaison channels with other parties
- Establish appropriate liaison channel with next of kin

- Activate media strategy
- Consult specialists
- Establish meeting and reporting routines
- Redistribute non-essential tasks
- Ensure operational continuity
- Begin planning for psycho-social recovery
- Start “lessons learned” process

4.4.4 Information Management Tools during Crises

The following tools will help an EMT in managing the crisis:

- A separate operations room / area where coordination can occur
- A staff tracking system
- A system for communicating with all team members, including primary and secondary means of communications
- A system for communicating with external entities
- An updated contact list
- An incident log
- An established security reporting system
- Access to team security contingency plans
- Area mapping
- Access to specialist advisors