Annex A

POLICY AND CONCEPTUAL OVERVIEW OF THE SECURITY RISK MANAGEMENT PROCESS

Introduction

1. The purpose of this section is to explain the SRM and SRA process and clarify the responsibilities of those involved in the preparation and review of SRAs. In order to do this, however, it is necessary to outline those activities of the wider SRM process which connect with the stages of the SRA.

2. The UNSMS Security Risk Management model is the managerial tool of the UN for the analysis of safety and security threats that may affect its personnel, assets and operations.

3. The Security Risk Assessment (SRA) is an integral part of the Security Risk Management (SRM) process. All security decisions, security planning and implementation of security measures to manage security risks must be based on sound Security Risk Assessments. In addition to the Country/Area SRA, an SRA should also be completed whenever circumstances in a location or specific programme vary significantly from those pertaining to the rest of the country.

4. Overall responsibility for the safety and security of UN staff rests with the Host Government; however, accountability also rests with managers at all levels, and not with their security advisers. Security advisers must provide the technical security inputs and advice which allow UN managers to make informed decisions for managing security risks. Security Risk Management therefore requires good teamwork between those who plan and direct UN operations and those who advise on the security measures which enable them.

Key terminology

5. The definition of Security Risk Management is:

   SRM is an analytical procedure that assists in assessing the operational context of the UN; and identifies the risk level of undesirable events that may affect United Nations personnel, assets, and operations; providing guidance on the implementation of cost effective solutions in the form of specific prevention and mitigation strategies and measures with the aim of lowering the risk levels for the UN by reducing the impact and likelihood of an undesirable event.

6. The definition of Security Risk Assessment is:

   The process of identifying those threats which could affect UN personnel, assets or operations and the UN’s vulnerability to them, assessing risks to the UN in terms of likelihood and impact, prioritizing those risks and identifying prevention and mitigation strategies and measures.

7. Threat and Risk are defined as follows:

   Threat: Any factors (actions, circumstances or events) which have the potential or possibility to cause harm, loss or damage to the United Nations system, including its personnel, assets and operations.

   Risk: The combination of the impact and likelihood for harm, loss or damage to the United Nations system from the exposure to threats. Risks are categorized in levels from Very Low to Very High for their prioritization.
The Security Risk Management Model:

The model is organized in two distinctive phases:

The **Preparation Phase** is the SRA and includes:

Programme Assessment, defines the goals and objectives of the country programmes and operations of UN organizations, reviews the justification for programme activities ("programme criticality"), and identifies elements of the programme which may require security support.

Threat and Vulnerability Assessments, incorporates the collection and deduction of relevant information. They provide the essential information required to determine threats to the UN and their associated risk. The appropriate host government authorities must be consulted during this process.

The sum of the three assessments provides a clear description of the “UN Security Situation” or operational context in the country/area.

Risk Analysis, decisions on current risk levels for each specific threat are made based on the deductions provided from the assessments and are determined by the impact and likelihood of the event.

Risk Management Measures are identified after all available information and actions are analyzed and incorporated for its presentation to the decision makers. All measures presented must be logical, feasible and relevant. Thinking outside the box, using creativity, experience and judgment play a critical role in this step.

The **Execution Phase** includes:

Decision, the DO and SMT will select and approve the risk management measures to reduce the current risk levels associated to each threat to the UN. An Implementation Plan is also decided and approved.

Implementation of the selected risk management measures. Often overlooked, this step is a critical element of the SRM process. The DO and the SMT members must ensure that the risk management measures are budgeted and implemented in accordance with the plan. Accountability does not end with the analyses; it ends with full implementation of the required measures.

Review and Update of the SRA. Continuous monitoring of the security environment and updating the SRA is mandatory. As new information is received and analyzed, the risk level may change (either higher or lower) for the particular threat affecting the risk management measures employed.
Programme Assessment

8. The Programme Assessment is essential to the SRA, and it is a distinct and separate part of the process, which is a fundamental part of the Country/Area Operations Planning process. The Programme Assessment must be developed as a collaborative effort between the responsible officers of the AFPs and organizations (usually the programme officers) who will conduct the programmes and security advisers (including agency security officers where present) in order to ensure “mainstreaming” of security at the earliest stage of Country/Area Programme Operations Planning. It is critical that security officers are consulted early in all programme development to ensure that security is included to avoid delays when programmes are implemented.

9. The Programme Assessment should identify all of the UN Agencies, Funds, Programmes and Organizations, that can be affected by the threats. It should assess how and why particular threats could affect programmes, and also identify those threats, which although present, are less likely to affect the UN or may even be irrelevant to UN operations. A comprehensive picture of programme activities should be constructed to allow integration with security information.

10. The Programme Assessment should also contain the assessment of the “criticality” of the programme. “Programme Criticality” defines:

   a. The benefits of the programme.
   b. The consequences (inter alia political, humanitarian, development, security and safety) of not implementing the programme or cancelling an existing programme.
   c. The extent to which other UN activities/programmes are dependant on the programmes’ continued implementation.

The Security Risk Assessment (SRA)

11. The functioning of the SRA within the overall SRM process is illustrated in the diagram below:
12. A credible SRA is an essential pre-requisite to the effective management of risk; the objective of an SRA is to identify and assess the nature of the risks to a UN operation or activity so that those risks can be effectively managed through the application of mitigating measures.

13. The main risk management measures are prevention (lowering likelihood) and mitigation (lowering impact). Risk management strategies can also be categorized as follows:
   
a. **Accept.** The unmitigated risk is accepted without the need for any further mitigating measures.
   
b. **Control.** Implement prevention and/or mitigation measures to reduce the risk to an acceptable level.
   
c. **Avoid.** Temporarily distance the potential target (e.g. UN staff, vehicles etc) from the risk.
   
d. **Transfer.** Insurance, or sub-contracting implementation to other parties who can operate safely.

**Frequency of Completing and Updating Security Risk Assessments**

14. The Security Risk Assessment is a tool which is a living document and must be under constant review by the CSA, DO and SMT. In particular, a validation should be carried out at each SMT meeting when there is a change or development in the “UN Security Situation” (the PA, TA or VA) which could affect UN operations or activities, for example:

   a. There is a change in the political situation or an upcoming event of political significance (e.g. an election) that may impact on UN security.
   
b. There is a change in operations (i.e. new role for the UN or elements of the UN in country or region).
   
c. Or when planning for:
      i. A new mission to be deployed.
      ii. The consideration and selection of new offices or facilities.
      iii. An expansion of programmes into new areas of a country.
      iv. Operations resuming after a programme suspension, relocation or evacuation for security reasons.
      v. Special events or conferences.
      vi. New spending on security measures.

15. Validating the SRA must be a standing item on the agenda of every SMT meeting. If new information is reported that changes the SRA, it should be noted in the SMT minutes and the SRA matrix updated to contain the relevant changes, conclusions and new recommendations which were decided in the SMT.

**Security Risk Analysis Table**

16. The UN Security Management System has established the following table for the evaluation of “Risks Levels”
17. To support the Risk Analysis process and the identification of Risk levels for each threat, indicators have been developed as per the following guide;

**Risk Acceptability**

18. For risk levels identified as Medium, High or Very High; “Acceptable Risk” is a relative term which requires judgment, and not just the application of rules.

19. The determination of “Acceptable Risk” is a critical responsibility of senior managers within the UN Security Management System. The relationship between Programme Criticality and the risk to the safety and security of UN personnel must be considered in the determination of “Acceptable Risk”. Managers must constantly strive to balance these two critical functions and are accountable for their decisions within the Framework for Accountability.

20. In order to determine acceptable risk, here are some questions that can be discussed throughout the SRM process:

a. **Identify programme / project goals.** In higher risk situations there will be a need to prioritize these goals. More important goals may dictate that the organization accept a higher level of risk to achieve results.

b. **Identify and assess the threats faced.** These are the obstacles that threaten the achievement of programme goals.

c. **Identify the risk** by looking at the likelihood and impact of the threats affecting the UN and each agency. Impact assessment is very important. Understanding how bad something could be is essential to discussion of acceptable risk. In other words, how bad an event can we accept?

d. **Identify how to manage the risks identified.** In other words, this is putting in place measures that will lower the risk and evaluating if the measures are working.

21. Over all, there is a need to answer a number of critical questions.

a. "How important is the activity?"

b. "Will the anticipated gains justify accepting a high level of risk?"

c. "Has enough been done to lower the risk to a level that is reasonable to expect staff to take?"

d. "Do we think that the risks we have identified are manageable?"

22. If the answers to the above are “yes” then consideration should be given to implementing the programme. If the answers are “no” then alternative options should be considered to achieve the programme goals.
Approval and Finalization of SRAs (including dispute resolution process)

23. The process for approval and finalization of the SRA is contained in the SRA guidance in the SOM, however, the salient steps are:
   
a. CSA/SA submits draft SRA to DO/SMT, and copies to DRO Desk Officer informally.

b. DRO Desk Officer informally reviews the draft SRA and provides the CSA/SA with advice on the following:
   i. Compliance with format and process.
   ii. Consistency with recent history of the region/country.
   iii. Actions and decisions adopted in respect to any risk identified as High or Very High.

c. DO/SMT approves the SRA in the SMT minutes, which will include and explain any reservations or minority opinions and is submitted to DSS.

d. In the event of significant differences of opinion, consultations will be set up with DSS Headquarters and the concerned Agencies, Funds and Programmes.

e. DRO Desk Chief officially endorses and returns the SRA to the DO.

Training

24. As agreed by the Secretary General, Chief Executive Board (CEB) and the UNSMS Network, training in the SRM methodology is mandatory for all DOs, SMT members and security professionals.

25. All United Nations officials who have specific security responsibilities within the Framework for Accountability must be cognizant of the Security Risk Management model and the SRA process.
Annex B

Guidelines for Determining Acceptable Risk

Background

1. Security risk management is an integral part of all UN activities. Agencies, funds, and programs must normally decide, according to their mandates and programmatic responsibilities, what program activities are necessary and appropriate. They must adapt their internal procedures for delegating responsibility, bearing in mind the Framework for Accountability. Country-level representatives are expected to reflect the priorities and interests of their respective organization in the SMT.

2. The security risk management framework is in place to identify and manage risks of undertaking the activities determined to be necessary and appropriate. In most environments, it will be possible to manage risks to facilitate program activities. This becomes most important when emergency operations are needed, to save lives. The crucial question, however, is to identify at what point the DO, as the responsible decision maker on security at the country level, declares that the identified risks are not manageable and suspends all UN staff presence in the area.

3. At its January 2009 meeting, the IASMN proposed an improved model of Security Risk Management. The OWG examined this SRM model and fully supports its use as an analytical procedure for assessing the operational context, and thus providing guidance on mitigating and lowering risks. Key to this model is the process for determining acceptable risk, based on examining four areas and asking several questions. The four areas are:

- Identify programme goals
- Identify and assess the threats faced
- Identify the risks
- Identify how to manage the risks identified.

4. The following questions must be asked in order to consider whether the exposure to risks identified is acceptable or not:

- How important is the activity?
- Will the anticipated gains justify accepting a high level of risk?
- Has enough been done to lower the risk to a level that is reasonable to expect staff to take?
- Are the risks that have been identified manageable in that context?

Acceptable Risk Decision: Programme Priority, Risk and Decision Makers

5. The table below is the Risk Analysis table from the SRM document. One suggested change is to refer to the risk level described in the top right-hand corner of the matrix as “unacceptable”.

---

<table>
<thead>
<tr>
<th>Programme Priority</th>
<th>Risk Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Important</td>
<td>Low</td>
</tr>
<tr>
<td>Medium</td>
<td>Moderate</td>
</tr>
<tr>
<td>Low</td>
<td>High</td>
</tr>
<tr>
<td>Unacceptable</td>
<td></td>
</tr>
</tbody>
</table>

---
6. With this adjustment/new table, we can now more clearly discuss acceptable risk. First, any residual risk or unmanaged risk that is assessed as in the black is always unacceptable for UN presence. The only risk management option in this situation is to avoid the risk (evacuate). Programmes may continue if the UN transfers the work to a partner (who may be exposed to a lower level or risk). In this environment, the UN must invest in risk management and lower the risk until the residual risk is at least Very High.

7. Whether risk is acceptable at any level lower than “unacceptable” (black) is a question of programme priority. The table below suggests definitions of Programme Criticality, level of program decision making, and the highest level of risk at which this program is acceptable.

<table>
<thead>
<tr>
<th>Program Criticality (Determined by Agency)</th>
<th>Agency Decision Maker</th>
<th>Residual Risk (Established by DO)</th>
<th>Final Decision (Final Risk Acceptance)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secretary-General/Policy</td>
<td>Unacceptable</td>
<td>Secretary-General</td>
<td></td>
</tr>
<tr>
<td>Extreme</td>
<td>Executive Heads</td>
<td>Very High</td>
<td>USG/DSS</td>
</tr>
<tr>
<td>Critical</td>
<td>HQ + Representative</td>
<td>High</td>
<td>DO</td>
</tr>
<tr>
<td>Essential</td>
<td>HQ + Representative</td>
<td>Medium</td>
<td>DO</td>
</tr>
<tr>
<td>All</td>
<td>Representative</td>
<td>Low/Very Low</td>
<td>DO</td>
</tr>
</tbody>
</table>

8. Combining the risk matrix (see color code) and the new categories for programme importance and decision-maker, we now have a clearer understanding of who makes the decision on acceptable risk. Each box with the matrix shows the minimum level of programme criticality that would be acceptable.
### Acceptable Risk Decisions

(Each box within the matrix shows the minimum level of program criticality that would be acceptable)

(Colors represent risk levels in SRA table above as established by the Designated Official)

<table>
<thead>
<tr>
<th>Program Importance</th>
<th>All</th>
<th>Essential, Critical &amp; Extreme</th>
<th>Critical &amp; Extreme</th>
<th>Extreme</th>
<th>Unacceptable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Program Decision</td>
<td>Rep</td>
<td>Rep + HQ</td>
<td>HQ + Rep</td>
<td>Exec. Head</td>
<td>No UN Presence</td>
</tr>
<tr>
<td>Final Decision</td>
<td>DO</td>
<td>DO</td>
<td>DO</td>
<td>USG DSS</td>
<td>Secretary-General</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Program Importance</th>
<th>All</th>
<th>Essential, Critical &amp; Extreme</th>
<th>Critical &amp; Extreme</th>
<th>Critical &amp; Extreme</th>
<th>Extreme</th>
</tr>
</thead>
<tbody>
<tr>
<td>Program Decision</td>
<td>Rep</td>
<td>Rep + HQ</td>
<td>HQ + Rep</td>
<td>HQ + Rep</td>
<td>Exec. Head</td>
</tr>
<tr>
<td>Final Decision</td>
<td>DO</td>
<td>DO</td>
<td>DO</td>
<td>DO</td>
<td>USG DSS</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Program Importance</th>
<th>All</th>
<th>Essential, Critical &amp; Extreme</th>
<th>Critical &amp; Extreme</th>
<th>Critical &amp; Extreme</th>
<th>Critical &amp; Extreme</th>
</tr>
</thead>
<tbody>
<tr>
<td>Program Decision</td>
<td>Rep</td>
<td>Rep + HQ</td>
<td>Rep + HQ</td>
<td>Rep + HQ</td>
<td>Rep + HQ</td>
</tr>
<tr>
<td>Final Decision</td>
<td>DO</td>
<td>DO</td>
<td>DO</td>
<td>DO</td>
<td>DO</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Program Importance</th>
<th>All</th>
<th>Essential, Critical &amp; Extreme</th>
<th>Critical &amp; Extreme</th>
<th>Critical &amp; Extreme</th>
<th>Critical &amp; Extreme</th>
</tr>
</thead>
<tbody>
<tr>
<td>Program Decision</td>
<td>Rep</td>
<td>Rep</td>
<td>Rep + HQ</td>
<td>Rep</td>
<td>Rep</td>
</tr>
<tr>
<td>Final Decision</td>
<td>DO</td>
<td>DO</td>
<td>DO</td>
<td>DO</td>
<td>DO</td>
</tr>
</tbody>
</table>
POLICY FOR
UNITED NATIONS MINIMUM OPERATING SECURITY STANDARDS

Introduction

1. MOSS is the primary mechanism for managing and mitigating security risks to UN personnel, property and assets of the organizations of the UN. MOSS encompasses a range of measures designed to reduce the level of risk, as identified in the SRA, to an acceptable and manageable level. These measures are listed under categories which include: telecommunications, documentation, coordination mechanisms, medical, equipment, vehicles, premises, training and residential security measures.

2. A single MOSS system applies throughout the UNSMS. No distinction is made between Headquarters, the Field or Missions for the purposes of Security Risk Management. The Minimum Operational Residential Security Standards (MORSS) scheme will continue to be applied, and remains separate from MOSS.

3. In order to mitigate risks identified in the Security Risk Assessment (SRA), MOSS must be applied and maintained at all duty stations.

4. Experience in the development and application of Minimum Operating Security Standards (MOSS) in the UN since 2002 has identified a need for the MOSS system to be kept as simple as possible, with the flexibility and capacity to allow adaptation to differing scenarios and rapidly changing circumstances.

MOSS

5. Each country and/or duty station, regardless of Security Phase, type of operation or security environment, is to develop and maintain a Country MOSS Table based on the mandatory Global MOSS provided in Appendix 1.

6. Measures contained in the Country MOSS Table must be commensurate with the Security Risk Assessment (SRA) applicable to the country or location. The measures should be presented to the Security Management Team with an explanation of their rationale, and then approved as laid down in paragraph 14 below.

7. The SRA must clearly demonstrate that the MOSS measures proposed will reduce the risk to UN personnel in country to an acceptable and manageable level.

8. Mitigation measures selected must be logical, realistic, cost effective, and capable of being implemented within the context of the operation or country.

9. Where the SRA indicates that the security environment could change, the Country MOSS Table must include provisions for timely enhancement of MOSS.
Responsibilities and Standards

10. As outlined in the Framework for Accountability, responsibility for implementing MOSS rests with the heads of UN organizations in country.

11. Where a UN organization does not have a permanent presence in the country, the head of the organization should take measures to ensure that missions and staff visiting the country are briefed in advance on the MOSS requirements applicable. The DO and the Security Adviser or Country Security Focal Point should provide assistance to enable such staff to comply, including the loan of equipment from a pool maintained for such visits where appropriate. Costs of MOSS measures will be covered by the sending organization.

12. It is the responsibility of the executive head of each organization to take action with Member States for the appropriation of required resources for security; the executive head of each organization is also responsible for the allocation of appropriate resources for security within his/her organization.

13. The United Nations World Food Programme is the focal point for Security Telecommunications issues and in its capacity advises the Security Management Network on policy and implementation of Security Telecommunications standards and services.

14. The UN Medical Directors Working Group (UNMDWG) provides technical guidance to the UN Security Management System on the minimum medical standards to be included in MOSS.

15. Additional expert technical advice should be sought, if necessary, where the SRA indicates a need for mitigation measures outside the normal competence of the UN safety and security staff.

16. The approval process for each Country MOSS Table will be as follows:

   a. The MOSS Table will be approved by the DO at a formal SMT meeting. This will be a part of the SMT minutes.

   b. The approved Country MOSS Table will be sent to DSS through the appropriate regional desk for review.

   c. DSS will circulate to the respective headquarters of all IASMN member organizations, and will endorse if no objections are received within one month.

17. Once endorsed, the Country MOSS Table is binding on all IASMN members with a presence in that country (including missions and visitors), at both the headquarters and field level. Oversight and compliance of MOSS will be provided by DSS through the Compliance, Evaluation and Monitoring Unit (CEMU)
UNITED NATIONS MINIMUM OPERATING SECURITY STANDARDS (UN MOSS)

Country MOSS Tables must justify, through the rigorous application of the Security Risk Assessment (SRA) process, the inclusion or exclusion of each of the items listed below. While the intention is to maintain flexibility and management discretion, common-sense will dictate those measures (such as vehicle safety equipment and fire precautions) which should be mandatory in all locations regardless of the prevailing security situation.

1. TELECOMMUNICATIONS

1.1. Emergency Communications System
   a. Where the SRA indicates a need, establish an Emergency Communications System (ECS) throughout the country, and its operational locations, in order to:
      (1). Provide communications between DO, SA, SMT, Wardens and UN medical personnel within the Capital.
      (2). Provide communications between ASC and DO/SA and UN medical personnel.
      (3). Provide communications between the ASC and the Area SA, SMT within the Area.
      (4). To enable communications between the DO/SMT/SA and relevant UN Offices outside the country (including DSS).
   b. Mobile satellite telephones should be provided to all CCCs, DOs and CSA/SAs and Agency Security Officers as well as for other key managers as decided by the SMT.
   c. The ECS is to be tested and practiced at regular intervals.
   d. The ECS network should be capable of operating 24 hour/7 days per week (24/7) should need arise.

1.2. Radio Communications
   a. When VHF/UHF communications are employed (in accordance with need identified in the SRA), a Security channel for DO, SA and SMT members, and where applicable ASC, ASMT members, UN medical personnel and wardens, must be incorporated into radio networks.
   b. All UN vehicles are to be equipped with VHF/UHF radios. In addition, “Field Vehicles” (those which travel into the countryside or move between urban areas) are to have a second radio system, usually HF or an alternative communication system (e.g. satellite phone).
c. SOPs for regular radio checks at residences and while moving are to be established.

d. All international personnel, all drivers, all wardens and national personnel deemed “essential”, are to be issued with hand-held VHF/UHF radios. Radio checks are to be conducted routinely.

e. All personnel who work regularly outside office premises are to be trained to operate all forms of telecommunications equipment provided for Field Vehicles.

2. **SECURITY INFORMATION AND STRUCTURE**

2.1. **Documentation.** Each country, and each duty station in the country, will have the following documentation:

   b. UN Field Security Handbook (FSH).
   e. Country/Area-specific MOSS.
   g. Relevant country maps.

2.2. **Warden Systems**

   a. Established and operational.
   b. Exercised regularly.

2.3. **Crisis Management Plans and Building Emergency/Evacuation Plan**

   a. Established for all UN offices and facilities.
   b. Exercised every six months (or more frequently if SRA so indicates)

2.4. **SMT Meetings:** To be conducted and documented as per UN Security Policy Handbook.

2.5. **Security Clearance and Travel Notification:** System in place for approving security clearances into country, recording travel notifications, and tracking personnel movements inside the country.

2.6. **Incident Reporting:** System to ensure that all security incidents in country are reported using “SIRS”.

2.7. A common-system **Crisis Coordination Centre (CCC)** is to be established in the Capital and all UN locations in country which have an ASC.
3. **MEDICAL**

3.1. **Response to Medical Emergencies**

a. **Casualty Evacuation Plans.** All duty stations are to have a “CASEVAC Plan” which includes rescue, immediate medical attention, identification or procurement of appropriate means of transportation, and location of appropriate primary health care facilities. [CASEVAC: the process for the rescue and movement of injured or sick personnel from the place or incident site at which injury occurs, or the person becomes ill, to a primary care medical facility inside the country].

b. **Medical Evacuation Plans.** All Duty Stations are to have a “MEDEVAC Plan” which includes the medical and administrative procedures necessary for evacuation of sick or injured personnel from the country, including the authority for authorization of evacuation and use of an air ambulance service where necessary. [MEDEVAC: the process for movement of injured or sick personnel from the primary care medical facility to a hospital, advanced care facility or place of recuperation outside the country in which the injury or illness occurred. It may also refer to the repatriation or reassignment of a staff member from a duty station which is deemed by the medical authorities to be potentially damaging to the staff member’s health for reasons of climate, altitude or other environmental factors.]

c. Each country is to have a **MASS CASUALTY PLAN** appropriate to the risks in country and the response capacity of the local emergency services.

d. Register of locally available medical facilities, emergency response services, and contact numbers to be maintained up to date and made available in ECS and to all duty personnel.

e. Based on the country/duty station security situation an appropriate number of UN personnel will be trained in Basic First Aid.

f. Each country is to have a medical plan and PEP Protocol.

3.2. **Medical Equipment**

a. All vehicles to carry Vehicle First Aid kits (specifications as per Security Technical Standards Manual).

b. **Emergency Trauma Bags** (ETBs) distributed according to number of trained UN staff.

c. One Basic First Aid kit per building (or per floor in buildings with more than 50 personnel).

d. **PEP Kits** (which must be replaced by their due expiry dates) will be distributed through the country PEP Kit protocol (which is to be attached to the Country Security Plan as an annex, and available in all radio rooms and duty personnel folders).

4. **EQUIPMENT and SUPPLIES**

4.1. **Emergency power supply** available for charging and operation of common-systems communications equipment, office external security lighting and other essential equipment. Adequate reserve stocks of fuel to be maintained.
4.2. Emergency Food, Water, Medical, Sanitary and Shelter Supplies (in non-perishable form) to be stocked in preparation for use in concentration points, bunkers and safe rooms, storm shelters as appropriate for the country and situation.

4.3. All personnel to prepare Individual Emergency Bags, maximum weight 15 kg (33 lbs) containing essential documents, clothing, hygiene and medical supplies, ready for rapid evacuation or relocation.

5. UNITED NATIONS VEHICLES

5.1. All UN Vehicles
   a. Must be operated by properly licensed operators.
   b. All UN vehicles appropriately registered with the Host Government and properly maintained.
   c. All vehicles identified, where appropriate, with UN logos/flags/decals as determined by prevailing local conditions.

5.2. Non-UN Vehicles. Where UN staff travel in non-UN vehicles which are not MOSS compliant, every effort should be made to ensure that the UN personnel are MOSS compliant (i.e. equipped with communications etc).

5.3. UN Vehicle Equipment

5.3.1. All vehicles (regardless of location)
   a. First aid kit.
   b. Fire extinguisher
   c. Spare wheel, jack and appropriate tools.
   d. Reflector triangles, battery-powered lantern, seat belts.

5.3.2. All Field Vehicles (according to country situation):
   a. 5 metre rope, strong enough to pull another field vehicle.
   b. Shovel, hand-axe or machete.
   c. Fire-lighting materials.
   d. High visibility sheet/flag,
   e. GPS based tracking system for curfew, movement restriction and convoy monitoring.
   f. Adequate drinking water, food and necessities (including blankets/sleeping bags) to support all occupants for 24 hours (according to climatic conditions).

6. OFFICES, PREMISES AND FACILITIES PROTECTION

6.1. All UN Managed Buildings
   a. All buildings occupied by UN to be compliant, where feasible, with international building, safety and fire regulations or the applicable laws of the host country as appropriate (including construction for resistance to earthquakes or other natural hazards, according to local conditions).
   b. Appropriate access control measures based on size and location of premises.
c. Separate entrances for personnel and visitors, where feasible and appropriate, in compliance with established standards (if/where applicable).

d. Secured parking for authorized vehicles where appropriate.

e. Alternate/emergency exits from buildings and from compounds.

f. Security and/or Guard force trained on appropriate surveillance and reconnaissance detection and reporting protocols.

6.2. **Premises with Additional Risks.** Premises that are assessed to be at high risk from terrorism are to have:

a. Stand-off distance as estimated/advised by qualified expert (taking scale of likely threat, surroundings/approaches, construction etc into account)

b. Structural reinforcement, blast walls as required/advised by qualified expert.

c. Shatter Resistant Film on windows and frame catchers.

d. Bunkers/reinforced rooms.

e. Surveillance and access control systems.

6.3. **UN Personnel working in government (or other non-UN) facilities**

a. To the extent practical, the DO and concerned head of organization should request MOSS-compliant conditions, to UN standards, for personnel working in non-UN premises.

b. Where this is not fully possible, the security adviser should be asked to assess the premises to see if the security measures in place provide an equivalent level of protection from the risks identified in the SRA as that provided in UN-managed premises.

c. Where a MOSS-equivalent level of protection is not achieved, the DO and head of organization concerned should consider, and negotiate with the host government authorities, alternate means of enhancing mitigation, such as:

(1). Allowing physical modifications to the workspace actually occupied by the UN personnel.

(2). Re-allocating the work space used by the UN personnel (for example, to ensure that they are as far as possible from external walls or likely terrorist approaches).

(3). Adjusting work patterns to limit the exposure of UN personnel within the government premises.
7. **SECURITY TRAINING AND BRIEFINGS**

7.1. **All new UN personnel and recognized dependents, as applicable, briefed on/provided with:**

   a. Country-specific security orientation briefing
   b. Summary/Extract of Country Security Plan and Evacuation Plan
   c. Relevant Country/Area-specific Security Plan, SOPs and policies.
   d. Compliance with all UN security policies.
   e. Copy of current MOSS and MORSS applicable to the duty station.
   f. Briefing and written handout on medical arrangements available in country and how to access them or call for emergency medical assistance.
   g. A copy of the Country PEP Protocol, which should specify PEP custodian arrangements, location of PEP kits, and procedure for obtaining assistance in the event of possible exposure to HIV/AIDS.

7.2. **All personnel provided with:** UN “Security in the Field” booklet (latest version)

7.3. **Training:**

   a. All UN personnel to complete Basic Security for UN Personnel (BSUNP) and/or Advanced Security In The Field (ASITF) online or by CD-ROM, as required for the duty station.
   b. All personnel to receive cultural sensitivity briefings appropriate to country before or on arrival.

8. **RESIDENTIAL SECURITY MEASURES**

   a. Minimum Operating Residential Security Standards (MORSS) will continue to be approved as a separate country table, in accordance with MORSS procedures as updated from time to time.
   b. MORSS must take account of the relevant conclusions of the SRA with respect to the local law and order situation.

9. **ADDITIONAL MEASURES:**

9.1. Depending on the security environment and the SRA, the DO and SMT may have to consider special measures. Examples of these are:

   a. **Personal Protective Equipment** (helmets, body armour etc) to be stocked adequate for all personnel needs as indicated by the Security Risk Assessment, and SOPs establishing conditions for issue, carriage in vehicles and mandatory wearing.
   b. **Armoured Vehicles.** In addition to providing a means of evacuating personnel under fire in extremis, armoured vehicles are an option where access is needed to areas which are marginally under the “acceptable risk” threshold, and where there is potential for resumption of conflict or fluidity of nearby conflict areas.
**EXAMPLE COUNTRY MOSS TABLE FORMAT (for ILLUSTRATIVE PURPOSES/SUGGESTION ONLY)**

United Nations Minimum Operating Security Standards

[COUNTRY NAME]

[Date]

(Required standards/mitigation measures are linked to security risks as identified in the SRA)

<table>
<thead>
<tr>
<th>1. TELECOMMUNICATIONS</th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No.</td>
<td>Item</td>
<td>Standard Requirement</td>
<td>Country Specific Requirements, Equipment &amp; Procedures</td>
</tr>
</tbody>
</table>
| 1.1 | Emergency Communications System | **Emergency Communications System (ECS) to be established** throughout [Country], as well as in [Cities], to provide for communication links between the:  
- DO, CSA, SMT, Wardens and UN medical personnel;  
- ASC and DO/CSA and UN medical personnel;  
- ASC and the FSCO, ASMT;  
- DO/SMT/CSA and relevant UN Offices outside the country (including DSS). | a. Mobile satellite telephones to be provided to: CCCs, DO, ASCs, CSA, DSA, FSCOs, Agency Security Officers, as well as other key managers;  
b. BGAN and/or VSAT provided to at least two offices in main operational hubs;  
c. The ECS network operating 24 hours/7 days per week in [City] and all main operational hubs inside [Country];  
d. The ECS is to be tested and exercised **monthly**;  
e. ECS technical support, as required; | Requirements are mandatory |
| 1.2 | Radio Communications | VHF/HF communications employed to cover the entire territory of [Country], a **Security channel** for DO, SA and SMT members, and where applicable ASC, ASMT members, UN medical personnel and wardens, to be incorporated into radio networks. | a. All staff in [Country] to be issued with hand-held VHF radios;  
b. All UN vehicles are to be equipped with VHF radios;  
c. UN Vehicles used for field missions to have a second radio system, usually HF or an alternative communication system (e.g. satellite phone);  
d. Radios provided to drivers of rented/non-UN vehicles;  
e. Radio Rooms established in all main operational hubs;  
f. Back-up radio system in bunkers/safe rooms; additional back-up system in secondary concentration point (where applicable).  
g. VHF base stations installed in all agency field offices;  
h. Repeater systems established for coverage of larger urban/rural areas; where appropriate;  
i. SOPs for regular radio checks at residences and while moving are to be established;  
j. All staff to be trained to operate all forms of telecommunications equipment;  
k. Radio checks in field locations to be conducted daily. | Requirements are mandatory  
Exemptions require the approval of the DO (e.g. community embedded staff in remote areas as per Section 9.7) based on alternative mitigation measures recommended in a specific SRA. |
## 2. SECURITY INFORMATION AND STRUCTURE

<table>
<thead>
<tr>
<th>No.</th>
<th>Item</th>
<th>Standard Requirement</th>
<th>Country Specific Requirements, Equipment &amp; Procedures</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1</td>
<td>Documentation</td>
<td>a. Country/Area-specific Security Risk Assessment b. UN Field Security Handbook (FSH) c. Security Operations Manual</td>
<td>As per standard requirement to be available at the DO’s office, agency offices, and each duty station, in addition: j. Mine area maps (provided by UNMAS); k. Maps/lists displaying permissible/non-permissible roads/areas; l. Maps displaying areas where armoured or vehicles with ballistic blankets fitted have to be used; m. Cell phone coverage map (maintained by FAO)</td>
<td>Requirements are mandatory</td>
</tr>
<tr>
<td>2.2</td>
<td>Warden System</td>
<td></td>
<td>a. Warden system for international staff to ensure emergency response coordination and staff concentration among UN (and NGO) compounds in a duty station - established and operational in all duty stations where more than one office and/or approved staff accommodation are located; b. Agency based warden system for national staff; c. Warden meetings monthly; exercise every 3 months, training every 6 months.</td>
<td>Requirement is mandatory</td>
</tr>
<tr>
<td>2.3</td>
<td>Staff Ceiling</td>
<td>Requirement for Security Phase IV areas.</td>
<td>a. Staff ceilings for international staff (assigned and on mission) to be established for all duty stations; b. Staff ceilings to be reviewed monthly (standing item on ASMT agenda).</td>
<td>ASMT recommends staff ceilings, SMT approves,</td>
</tr>
<tr>
<td>2.4</td>
<td>Building Emergency/Evacuation Plan</td>
<td>Established for all UN offices and facilities</td>
<td>a. Building emergency/evacuation plans exercised every 6 months</td>
<td>Requirement is mandatory</td>
</tr>
<tr>
<td>2.5</td>
<td>SMT and ASMT Meetings</td>
<td>To be conducted and documented as per UN Security Policy Handbook.</td>
<td>SMT and SMT Working Group Meetings alternate weekly (DO determines participation - attendance is mandatory) – ASMT meetings weekly</td>
<td>Requirement is mandatory</td>
</tr>
<tr>
<td>2.6</td>
<td>Security Clearance Procedures</td>
<td>System in place for approving security clearances into country, recording travel notifications, and tracking personnel movements inside the country.</td>
<td>a. Full ISECT implementation for external and internal travel, including Phase V areas b. ISECT profiles for all staff (agencies responsible that ISECT profiles are updated)</td>
<td>Requirement is mandatory</td>
</tr>
<tr>
<td>2.7</td>
<td>Incident Reporting</td>
<td>a. All security incidents are reported using “SIRS”</td>
<td>b. Other reports as per Field Security Handbook c. Agency FSAs report incidents simultaneously to parent agency and CSA</td>
<td>Requirement is mandatory</td>
</tr>
<tr>
<td>2.7</td>
<td>Crisis Coordination Centre (CCC)</td>
<td>a. Established for all UN offices and facilities;</td>
<td>b. CCCs established in [City] and all main operational hubs; c. Exercised every six months (or more frequently if SRA so indicates) - crisis management exercises only if no actual crisis occurred – otherwise prepare “lessons learned”.</td>
<td>Establishment of SIOC by [planned date].</td>
</tr>
</tbody>
</table>
### 3. MEDICAL SUPPORT

<table>
<thead>
<tr>
<th>No.</th>
<th>Item</th>
<th>Standard Requirement</th>
<th>Country Specific Requirements, Equipment &amp; Procedures</th>
<th>Remarks</th>
</tr>
</thead>
</table>
| 3.1 | Response to Medical Emergencies | g. Casualty Evacuation Plans: immediate medical attention, identification or procurement of appropriate means of transportation, and location of appropriate primary health care facilities (inside the country).  
|     |      | h. Medical Evacuation Plans: medical and administrative procedures necessary for evacuation of sick or injured personnel from the country, including the authority for authorization of evacuation and use of an air ambulance service where necessary.  
|     |      | i. Establish and maintain area–specific casualty and medical evacuation plans;  
|     |      | j. Establish and maintain Mass Casualty;  
|     |      | k. Register of locally available medical facilities, emergency response services, and contact numbers to be maintained up to date and made available in ECS (classified as per UN PKO medical standards;)  
|     |      | l. All staff to be trained in Basic First Aid;  
|     |      | m. Security staff and appropriate number of other staff trained and certified in trauma and mass casualty incident response;  
|     |      | n. Establish medical plan and PEP Protocol;  
|     |      | o. Adequate number of stress counsellors dedicated to [Country] based staff;  
|     |      | p. Adequate number of paramedics under supervision of a UN physician;  
|     |      | q. UN medical officer to supervise stabilisation centres trained and certified in Advanced Trauma Life Support (ATLS) and Pre-hospital Trauma Life Support (PHTLS) or equivalent;  
|     |      | r. Adequate air rescue capacity, minimum one pressurised aircraft with ALS on stand-by at all times;  
|     |      | | Response times to be reduced - objectives to be accomplished before end of 2009:  
|     |      | - CASEVAC - trauma stabilization by paramedic max. 1 hour after incident;  
|     |      | - Air MEDEVAC and admission to Level II hospital max. 3 hours after incident;  
|     |      | | Note: Quarterly report to DSS on progress |
| 3.2 | Medical Equipment | a. All vehicles to carry Vehicle First Aid kits (specifications as per Security Technical Standards Manual).  
|     |      | b. Emergency Trauma Bags (ETBs) distributed according to number of trained UN staff.  
|     |      | c. One Basic First Aid kit per building (or per floor in buildings with more than 50 personnel).  
|     |      | d. PEP Kits (which must be replaced by their due expiry dates) will be distributed through the country PEP Kit protocol (which is to be attached to the Country Security Plan as an annex, and available in all radio rooms and duty personnel folders)  
|     |      | e. Establish stabilization centres with ATLS and PHTLS capacity in all operational hubs (5 by September 2009 – all hubs by December 2009)  
|     |      | f. Ambulances (or ambulance type vehicles with ability to fit stretchers) in main operational hubs;  
|     |      | g. Establish UN dispensaries in selected locations (SMT decision);  
|     |      | h. Support local hospitals to increase MCI and response capacity (e.g. ambulances)  
|     |      | i. PEP kits stocked in UN dispensaries + 2 PEP kits per custodian (usually FSCO/FSA)  
|     |      | | Note: Quarterly report to DSS on progress |

CONTINUED FOR ALL MEASURES IN THE BASELINE