UNITED NATIONS SYSTEM CEB

Chief Executives Board for Coordination

CEB/2009/HLCM/3
16 February 2009

HIGH-LEVEL COMMITTEE ON MANAGEMENT (HLCM)
Seventeenth Session
WFP, Rome, 24-25 February 2009

REPORT OF THE INTER-AGENCY SECURITY MANAGEMENT NETWORK

PARIS, 26-28 JANUARY 2009

I. INTRODUCTION

1. The Inter-Agency Security Management Network (IASMN) met at the United Nations Educational, Scientific and Cultural Organization (UNESCO), Paris, France, from 26 to 28 January 2009. A list of participants from organizations, agencies, programmes and funds (hereafter referred to as the Organizations) as well as the agenda and list of documents are attached as Annex A. The IASMN wishes to express its gratitude to the UNESCO for hosting the meeting.

II. EXECUTIVE SUMMARY

2. As this entire report consists of recommendations of the IASMN, it would be duplicative to list individual recommendations in an Executive Summary.

III. RECOMMENDATIONS OF THE IASMN

A. Blast Assessment

3. The IASMN considered the Report of the Blast Assessment Working Group (BAWG), established as a result of the Report of the Independent Panel on Safety and Security of UN Staff and Premises. The BAWG report outlines a proposed policy as well as guidelines for the mitigation of blast at UN premises and operations.

4. Following extensive discussions, and recognizing that the vast majority of United Nations premises worldwide do not readily comply with the recommendations, the IASMN endorses the blast assessment as guidelines for a desirable standard to be implemented system-wide based on a credible SRA. The IASMN points out that implementation of these standards will be based on a determination of acceptable risk (utilizing the methodology of acceptable risk to be determined by the CEB) to be under-taken by each organization.

5. Recognizing that the implementation of blast mitigation measures will have significant cost and operational impact, the IASMN nonetheless recommends that lack of funding should not be an excuse not to implement appropriate measures.

6. The IASMN recommends that blast mitigation be considered as part of the Estate Policy for both existing as well as new premises and facilities and that suitable measures be adopted by organizations in line with existing security risk management policies. The representative of UNOCD, while supporting the normative intent of the policy, highlighted the need for detailed, actionable guidelines in respect of existing facilities as well as an analytical and operational differentiation between Headquarters, field representative or other field offices.

B. Minimum Operating Security Standards

7. The IASMN considered a revised MOSS document and requested DSS to make a number of amendments to the document which has been done and copies provided to all participants. The IASMN recommends that MOSS (Annex B) be approved by the HLCM. The representative of UNODC contended that MOSS does not apply to UN Headquarters and that the IASMN does not have the mandate to consider Headquarters issues. UNODC’s view was not shared by other participants.

C. Security Risk Management

8. The IASMN considered a revised version of the Security Risk Management (SRM) policy document, which provides the conceptual framework and policy for use of the Security Risk Management (SRM) model. The IASMN requested DSS to make a number of amendments to the document, which has been done and copies provided to all participants, and recommends that the policy (Annex C) be approved by the HLCM.

D. Conference Security

9. The IASMN considered proposed guidelines on the provision of security at conferences and events by the United Nations Organizations. The IASMN recommends that these guidelines be adopted for use as appropriate.

E. Provision of Guard Forces for UN Premises

10. The IASMN had previously discussed extensively the use of private security providers. In this context, the IASMN had requested the redrafting of Annex O to the Field Security Handbook to ensure a more detailed set of practical instructions is available for use by Security Advisers. The IASMN decides that it will reconvene in a small working group to discuss all issues related to this matter, taking into account also the work of the UN Working Group on Mercenaries and will make recommendations to the Summer session of the IASMN. The Working Group will be chaired by DSS and will consist of: UNHCR, FAO, WFP, UNICEF, UNDP, DPKO, DFS and WIPO.

F. Policy on Close Protection

11. The IASMN considered an amendment to the UN policy on Close Protection approved in October 2008 which would permit armed UN Close Protection officers to be allowed access to all UN premises and vehicles, when required, pursuant to their duties. The IASMN recommends approval of this amendment. In instances where this is not permitted, the host UN organization assumes full responsibility and accountability for the protection of the individual concerned.

12. The representative of the World Bank wished to record that the World Bank would not support this policy due to the special close protection needs of the World Bank.

G. Report of Medical Directors Working Group to the HLCM regarding Medical Recommendations in the IPSS and subsequent IASMN report

13. The IASMN considered a submission to the HLCM from the UN Medical Director on issues related to the support required by medical personnel and services deployed in the UN System. The IASMN endorses and supports the recommendations of the Medical Directors, especially with regard to the need to fund the United Nations Medical Emergency Response Team (UNMERT), which had already been endorsed by the CEB.

H. Policy for Appointment of Designated Officials ad interim

14. The IASMN considered a report regarding the appointment of Designated Officials ad interim and endorses the proposals included in the relevant Conference Room Paper which would require modifications of the Accountability Framework and the Field Security Handbook. The IASMN requests DSS to undertake the necessary action in this regard.

15. The representative of the World Bank wished to record that under no circumstance, the World Bank staff members should be appointed as Designated Officials or Designated Officials ad interim due to the fact that the World Bank has different policy for evacuation. The representative of UNODC noted his organization’s support of this policy for field locations, but not for Secretariat duty stations or Headquarters locations for which appropriate ad hoc solutions need to be found.

I. Information Management Issues

16. The IASMN considered a report from DSS on continuing information management issues, including the requirements for dedicated funding for a critical technical service required by the UN Security Management System. The IASMN recommends approval of the proposed course of action.

17. The IASMN welcomes the work undertaken by the DSS in developing and enhancing Information Management systems to support the UN Security Management System.

18. Taking note of past crises such as natural disasters, attacks of hotels and pandemic planning, the IASMN endorses expanding the use of ISECT to include not just countries/locations with a Security Phase in effect, but all countries/locations to which staff travel on official business, including official home leave or other entitlement travel where the cost of travel is absorbed by organizations of the UN System. The IASMN recommends that for personal travel, UN personnel be encouraged to use ISECT.

19. As requested by the IASMN Steering Group, a funding proposal was provided to establish an Information Management capacity. Recognizing that the HLCM addresses all budgetary matters, the IASMN notes the proposal and supports enhancing the Information Management capacity of the UN Security Management System.

20. The representative of the World Bank wished to record that the World Bank has its own special travel requirement and would not support the increase of funding for Information Management capacity of the UN Security Management System.

J. Human Resources

21. The IASMN considered a Conference Room paper regarding the implementation of a career path for security professionals. The IASMN reviewed the equivalency standards for security professionals and recommends that, in consultation with Human Resources Network, the profile of security advisors at all levels be developed to address the issue of education and professional experience that best respond to the requirements of the responsibilities of the positions.

22. The IASMN recommends that further work be done on addressing why it is difficult to attract and retain qualified candidates, especially women. The IASMN also recommends that in addition to qualifications related to education and experience, the potential of a candidate to have a career in the UN should be evaluated.

K. Local Cost Sharing of Field Activities

23. The IASMN considered a report from DSS regarding possible alternative funding mechanisms for locally cost-shared MOSS implementation. The IASMN recommends that the existing system remain in place until such time as the HLCM has decided on the overall funding strategy for the UN Security Management System.

24. The IASMN recommends that steps be taken to ensure that budgets for field activities are standardized in terms of content and format and that they are prepared in a timely manner to permit the organizations concerned to make appropriate budgetary arrangements.

25. The representative of the World Bank wished to record that the World Bank is incapable of sharing locally cost-shared budget because the World Bank does not have such budget structure.

L. Security Training

26. The IASMN recognizes the excellent work accomplished by DSS in the area of security training. Noting the importance of the training of Designated Officials, Security Management Teams and others, the IASMN endorses the Designated Official security training programme and the approach to SMT training.

27. Noting with concern the non-attendance of Heads of Agency at SMT training, the IASMN endorses DSS sending all SMT attendance reports to the Executive Directors of concerned Agencies, Funds, Programmes and Organizations bringing this to their attention for appropriate action. The IASMN encourages organizations to reflect attendance at SMT Training in the internal appraisal process for each relevant individual. The IASMN also recommends that no individual be permitted to serve as a Designated Official until such time as he/she has been trained.

28. The IASMN restated its continued support of the Secure and Safe Approaches in Field Environments programme (SSAFE) as well as its support to the increasing medical support training being undertaken by DSS.

29. The IASMN recommends that the Security Training Working Group be reconstituted to consider synergies and resources that can be harnessed to advance consistent security training across the UN Security Management System.

M. Critical Incident Stress

30. The IASMN welcomes the report on the improvements accomplished with the community of stress counselors and endorsed the report. The IASMN requests that the Critical Incident Stress Management Working Group, prepare and provide a plan of action with cost implications to implement the recommendations contained in the report at its next scheduled meeting. The IASMN recommends that DSS share the report of the Critical Incident Stress Counsellors with the Human Resources Network and the Medical Directors.

N. Terms of Reference of the IASMN

31. The HLCM at its sixteenth session (September 2008) requested the IASMN to take action on the following issues and to report thereon to it at its next session:

a) Draft the Terms of Reference of the Network, including mandate, responsibilities, composition, governance and working modalities;

b) Nominate a Vice Chair;

c) Propose a revised name for the Network.

32. Following extensive discussions, the IASMN recommends the following:

a) Terms of Reference
The IASMN will consider and make recommendations to the HLCM on:
i. all matters related to security and safety of staff, premises and assets of organizations participating in the UN Security Management System (UNSMS);
ii. any other matters referred to it by the HLCM.

b) Composition:
The membership of the IASMN will consist of the following:
i. all organizations which are members of the CEB;

ii. Organizations that have concluded a Memorandum of Understanding (MOU) with the UN for the purposes of participating in the UN Security Management System;

iii. Any organization or department which has a specific mandate for management of the safety and security of UN staff, personnel and premises or which are directly involved in the coordination, delivery and support of UN activities in the field especially during emergencies and in high risk environments;

iv. Any other organization as invited by the USG/DSS as Chair of the IASMN.

c) Chair and Vice-Chair of the IASMN:
i. It is recalled that at its video conference of 22 January 2002, the HLCM decided that the IASMN would be chaired by the UN Security Coordinator (now USG/DSS). The IASMN reaffirms that the USG DSS, as its representative at the HLCM and the CEB, should chair all IASMN meetings;

ii. The IASMN decides to nominate on an annual rotating basis a Vice-Chairperson, who will chair the meeting of the IASMN in the absence of its Chairperson. The IASMN recommends that the Vice Chair be fully involved in the organization of all IASMN meetings. The IASMN decides that Mr. Satoru Tabusa will serve as Vice-Chair for calendar year 2009.

d) Working Modalities of the IASMN

i. In order to facilitate the work of the IASMN, a Steering Group shall be appointed, the composition of which will be reviewed and confirmed by the IASMN.

ii. The Steering Group will consider and propose the agenda for the IASMN meetings as well as the draft documents;

Iii The IASMN will establish working groups on particular issues to assist its deliberations as necessary, drawing upon internal and external expertise. The terms of reference will be decided by the IASMN.

e) Name

The IASMN recommends that pending the approval of the HLCM and the CEB it should be known as UN Security Network (UNSN).

f) Secretariat

The IASMN points out that within DSS there is no established Secretariat for the IASMN nor is one envisaged at this time. The IASMN recommends that the HLCM immediately consider the approval of a Secretariat within DSS to be cost-shared by all members.

O. <u>The High Level Steering Committee Operational Working Group (OWG) on Safety and Security</u>

33. The IASMN met with the Chair of the High Level Steering Committee Operational Working Group (OWG) on Safety and Security to exchange views on matters of mutual interest. The Chair of the OWG also briefed the IASMN on the ongoing work of the Group. The IASMN assured the Chair of the OWG that it would support the work of the OWG and stressed that cooperation and consultation between the tow bodies should continue.

34. Various IASMN members provided the Chair of the OWG with their views on such critical issues as the security phase system, security risk management, host country responsibilities and other matters.

35. During these discussions, the representative of UNIDO advised the IASMN that UNIDO had recently appointed a full-time Security Focal Point to strengthen its security management team and encouraged other organizations to do the same.

P. <u>Other Matters</u>

36. With regard to the location of the next IASMN meeting in June or July 2009, participants were requested to propose venue. Proposals should be submitted to DSS by the end of February 2009.

Annex B

POLICY FOR 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)

Appendix 1 to MOSS Policy

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 in 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:

a. Security Risk Assessment.

b. UN Field Security Handbook (FSH).

c. Security Operations Manual.

d. Country/Area-specific Security Plan.

e. Country/Area-specific MOSS.

f. Security Standard Operating Procedures.

g. Relevant country maps.

h. Country PEP Protocol.

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.

5.2.2. 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.

Annex A

LIST OF PARTICIPANTS

CHAIRPERSON	**Ms. Diana Russler (DSS)**
SECRETARY	**Ms. Kathy Qi (DSS)**

AGENCIES, PROGRAMMES AND FUNDS AND OTHER ENTITIES OF THE UNITED NATIONS SECURITY MANAGEMENT SYSTEM

Asian Development Bank (ADB)	**Mr. Richard Jacobson**
Preparatory Commission for the Comprehensive Nuclear-Test-Ban Treaty Organization (CTBTO)	**Mr. Robert Erenstein**
European Bank for Reconstruction and Development (EBRD)	**Mr. Alan Drew**
Food and Agriculture Organization (FAO)	**Mr. Michael Hage**
International Atomic Energy Agency (IAEA)	**Mr. Steven E.S. Giwa** **Ms. Maria Bermudez-Samiei**
International Criminal Court (ICC)	**Mr. Jeff Kyle**
International Fund for Agricultural Development (IFAD)	**Mr. Antonio Kamil**
International Labour Organization (ILO)	**Mr. Satoru Tabusa** **Mr. Brian Wenk**
International Monetary Fund (IMF)	**Mr. Warren J. Young**
International Organization for Migration (IOM)	**Mr. John Shabatura**
Organization for the Prohibition of Chemical Weapons (OPCW)	**Mr. Robert Simpson**
Pan American Health Organization(PAHO)	**Mr. Michael A. Boorstein**
Joint United Nations Programme on HIV/AIDS (UNAIDS)	**Ms. Helena Eversole** **Mr. Fredric Claus**
United Nations Development Programme (UNDP)	**Mr. Andrew Lukach** **Mr. Adam Simonson**

United Nations Educational, Scientific and Cultural Organization (UNESCO)	**Ms. Lamia Salman-El Madini** **Ms. Magda Landry**
Chair of HR Network (UNESCO)	**Ms. D. Dufresne Klaus**
United Nations Population Fund (UNFPA)	**Ms. Janie McCusker**
United Nations High Commissioner for Refugees (UNHCR)	**Mr. Paul Stromberg**
United Nations Children's Fund (UNICEF)	**Mr. Bill Gent**
United Nations Industrial Development Organization (UNIDO)	**Mr. Andrei Lazykin**
United Nations Environment Programme (UNEP)	**Mr. Peter Marshall**
United Nations Relief and Works Agency for Palestine Refugees in the Near East (UNRWA)	**Ms. Laura Londen**
United Nations Volunteers (UNV)	**Ms. Michele Rogat**
Universal Postal Union (UPU)	**Mr. David Bowers**
World Food Programme (WFP)	**Mr. Mick Lorentzen**
Chair of OWG (WFP)	**Mr. Manuel Aranda Da Silva**
World Health Organization (WHO)	**Mr. Patrick Beaufour**
World Intellectual Property Organization (WIPO)	**Mr. Jan Van Hecke**
World Bank (WB)	**Ms. Autumn Hottle**

DEPARTMENTS OF THE UNITED NATIONS SECRETARIAT AND SUBSIDIARY ORGANIZATIONS OF THE SECURITY COUNCIL

Department of Field Support (DFS)	**Mr. Joel Cohen**
Department of Peace-keeping Operations (DPKO)	**Ms. Florence Poussin**
Department of Management Medical Services (DM)	**Dr. Brian Davey**

Department of Safety and Security (DSS)	**Mr. Gerard Martinez Mr. Mohammad Bani Faris Mr. Gerry Ganz Mr. Richard Floyer Acland**
DHSSS Chiefs	**Mr. Bruno Henn Mr. Marc Wood Mr. Kevin O. Hanlon Mr. Djiby Diop Mr. Elias Daoud Mr. Ousseini Ouedraogo Mr. Rodrigo Victor Mr. Gert Keulder**
International Criminal Tribunal for Rwanda (ICTR)	**Ms. Sarah Kilemi**
International Criminal Tribunal for the Former Yugoslavia (ICTY)	**Ms. Bonni Adkins**
Office for the Coordination of Humanitarian Affairs (OCHA)	**Mr. David Kaatrud**
Office of the High Commissioner for Human Rights (OHCHR)	**Mr. Stuart Groves**
United Nations Office on Drugs and Crime (UNODC)	**Mr. Franz Baumann**

OBSERVERS

Coordinating Committee for International Staff Unions and Associations of the United Nations System (CCISUA)	**Ms. Annie Rice**
Federation of International Civil Servants' Associations (FICSA)	**Mr. Steven Ackumey-Affizie**

Agenda

1. **Policy issues**

   a. MOSS (CRP 3 and Annex A)

   b. SRM (CRP 4)

   c. Policy for provision of guard forces (CRP 5, Annex A, B, C and D)

   d. Conference safety (CRP 6)

2. **Security training (CRP 8, Annex A, B, C, D and E)**

3. **Critical incident stress management (CRP 9)**

4. **Information management issues (CRP 10, Annex A and B)**

5. **The blast assessment working group (CRP 11, Annex A, B, C, D and E)**

6. **Implementation of career path for security professionals (CRP 12)**

7. **Local cost sharing issues (CRP 13)**

8. **Policy on close protection operations (CRP 14 and Annex A)**

9. **Selection of Designated Officials ad interim (CRP 15)**

10. **Submission from UN Medical Directors to the HLCM (CRP 16)**

11. **Terms of reference of the IASMN**

12. **Briefing on the High Level Steering Committee Operational Working Group on Safety and Security (CRP7, Annex A, B, and C)**

13. **Other matters**
    a. Location of the next IASMN meeting

List of Documents

CRP 1	Agenda
CRP 2	Report of the Steering Group, Geneva, November 2008
CRP 3 and Annex A	MOSS
CRP 4	SRM
CRP 5, Annex A, B, C and D	Policy for provision of guard forces
CRP 6	Conference safety
CRP 7, Annex A, B and C	Briefing on the High Level Steering Committee Operational Working Group on Safety and Security
CRP 8, Annex A, B, C, D and E	Security training
CRP 9	Critical incident stress management
CRP 10, Annex A and B	Information management issues
CRP 11, Annex A, B, C, D and E	The blast assessment working group
CRP 12	Implementation of career path for security professionals
CRP 13	Locally cost sharing issues
CRP 14 and Annex A	Policy on close protection operations
CRP 15	Selection of Designated Officials ad interim
CRP 16	Submission from UN Medical Directors to the HLCM

Annex C

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* <u>*risk level*</u> of undesirable events that may affect United Nations <u>personnel</u>, <u>assets</u>, and <u>operations</u>; providing guidance on the implementation of cost effective *solutions* in the form of specific prevention and <u>mitigation</u> strategies and measures with the aim of lowering the risk levels for the UN by reducing the <u>impact</u> and <u>likelihood</u> of an undesirable event.

6. The definition of *Security Risk Assessment* is:

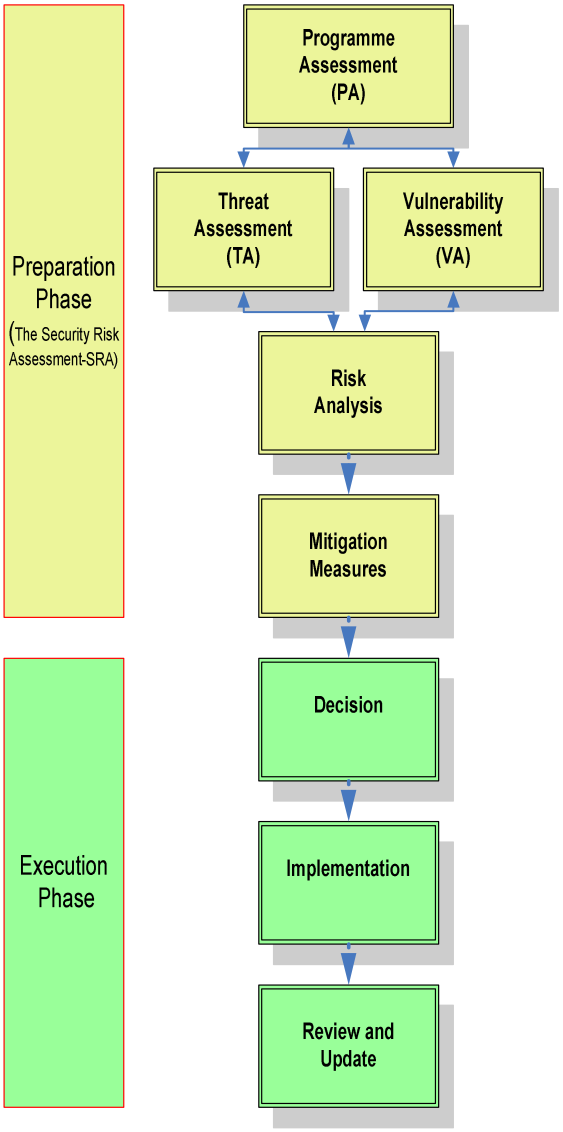
   The process of identifying those threats which could affect UN personnel, assets or operations and the UN's vulnerability to them, assessing risks to the UN in terms of likelihood and impact, prioritizing those risks and identifying prevention and mitigation strategies and measures.

7. *Threat* and *Risk* are defined as follows:

   <u>Threat</u>: 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.

   <u>Risk</u>: 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 determinate 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.

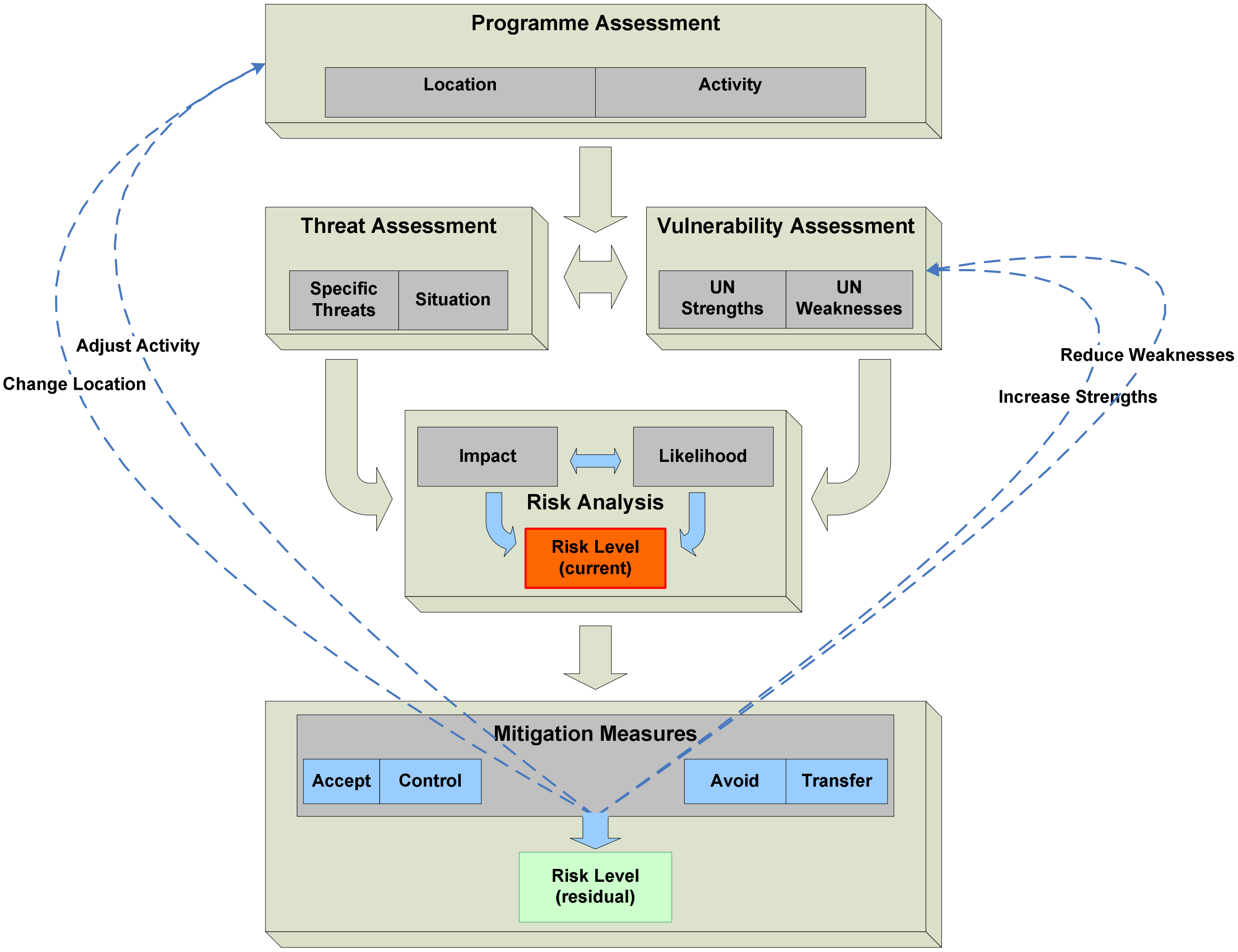
9. The Programme Assessment should identify all of the UN Agencies, Funds, Programmes and Organizations, that can be affected by the threats. It should assess how and why particular threats could affect programmes, and also identify those threats, which although present, are less likely to affect the 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:


Programme Assessment
Location
Activity
Threat Assessment
Specific Threats
Situation
Vulnerability Assessment
UN Strengths
UN Weaknesses
Adjust Activity
Change Location
Reduce Weaknesses
Increase Strengths
Impact
Likelihood
Risk Analysis
Risk Level (current)
Mitigation Measures
Accept
Control
Avoid
Transfer
Risk Level (residual)

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"

		IMPACT				
	RISK ANALYSIS TABLE	Negligible	Minor	Moderate	Severe	Critical
LIKELIHOOD	Very Likely/ Imminent	Low	Medium	High	Very High	Very High
	Likely	Low	Medium	High	High	Very High
	Moderately Likely	Very Low	Low	Medium	High	High
	Unlikely	Very Low	Low	Low	Medium	Medium
	Very Unlikely	Very Low	Very Low	Very Low	Low	Low

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.