UNITED NATIONS SYSTEM CEB

Chief Executives Board
for Coordination

CEB/2008/HLCM/5
5 March 2008

HIGH-LEVEL COMMITTEE ON MANAGEMENT (HLCM)
Fifteenth Session
FAO, Rome, 17-18 March 2008

Agenda item 3

REPORT OF THE INTER-AGENCY SECURITY MANAGEMENT NETWORK

Washington D.C., 26-28 February 2008

I. INTRODUCTION

1. The Inter-Agency Security Management Network (IASMN) met at the Headquarters of the World Bank, Washington, D.C., from 26 to 28 February 2008. A list of participants from organizations, agencies, programmes and funds (hereafter referred to as the Organizations) is attached as Annex A. The agenda and list of documents considered by IASMN members are attached in Annex B. The IASMN wishes to express its gratitude to the World Bank for hosting the meeting and welcomed the presence of Mr. Lakhdar Brahimi, Chairperson of the Independent Panel on Safety and Security of United Nations personnel and premises around the world, and his colleagues, who came to observe and listen to the first day of deliberations.

2. In the aftermath of the tragic incident in Algiers on 11 December 2007, on 19 February 2008, the Policy Committee, chaired by the Secretary-General and attended by a number of Executive Heads of United Nations agencies, programmes and funds (or their representatives), discussed the issue of how the United Nations system can operate in high risk/complex environments. The Policy Committee agreed that the matter should be considered by the IASMN, which was requested to make recommendations to the High Level Committee on Management (HLCM) and subsequently the Chief Executives Board (CEB), on what actions can be taken to address vulnerabilities of the United Nations security management system.

3. The Policy Committee specifically requested IASMN and the HLCM to develop recommendations for the CEB to consider during its session in late April on a number of urgent issues which are outlined in para. 26 below.

4. The IASMN wishes to reiterate at the outset that any recommendations contained in this report will have to be considered in conjunction with the report to be provided by the Independent Panel on Safety and Security of United Nations personnel and premises which will evaluate the strategic issues vital to the delivery and enhancement of the security of UN personnel and premises and the changing threats and risks faced by it.

5. The IASMN also wishes to point out that over the past years it has presented a large number of security recommendations which have been endorsed by the HLCM. Regrettably, a significant number of these recommendations, which directly impact on the safety and security of personnel of the United Nations

system, have yet to be implemented. The IASMN therefore believes that the time has come to turn these decisions into actions.

6. The IASMN points out that it had less than one week to consider this matter and develop substantial recommendations for the consideration of HLCM and CEB. Given these time constraints, in many instances the IASMN has been able only to identify a strategy or a framework that will require further inter-agency discussions before agreement can be reached on the way ahead. The IASMN intends to follow up on these matters and report to HLCM at its next meeting.

EXECUTIVE SUMMARY

7. As this entire report consists of recommendations in response to the Secretary-General's direction, it would be duplicative to list individual recommendations in an Executive Summary.

RECOMMENDATIONS OF THE IASMN

8. The unanimous view of the IASMN is that the United Nations security management system is very robust and, although there is always room for improvements and fine tuning, it is the failure to implement successfully the security policies, practices and procedures at all levels of the United Nations system that has resulted in deficiencies in a number of areas. At the same time the IASMN strongly reiterates that the essential responsibility of the UN security management system is "to enable the deliveries of UN programmes while maintaining the safety and security of staff as a high priority". The IASMN points out that there seems to be a tendency to forget this clause in the discussion regarding the enabling of UN programmes.

9. Following extensive discussions, the IASMN recommends that Executive Heads consider the following broad strategy with regard to the implementation of the UN security management system:

a) Decide on the level of acceptable risk that they are prepared to ask or allow their staff to take in the implementation of the mandates entrusted to them by Member States;

b) Agree a Risk Management Strategy that achieves a balance between the delivery of programmes and the maintenance of safety and security of staff and assets of the organizations of the UN system;

c) Ensure that security is an integral part of any programme, project or activity of the organization they represent and for which they are accountable;

d) Ensure that training programmes are implemented as critical steps in managing risk and crises;

e) Ensure that security is provided with appropriate and sustainable funding; and,

f) Ensure that the established governance mechanism for the UN security management system, i.e. the IASMN, HLCM, and CEB, is adhered to in order to avoid confusion, duplication and decision-making on security matters outside the framework for accountability for security.

10. To implement this strategy, the IASMN recommends a series of actions outlined below.

11. The Framework for Accountability for the United Nations security management system, which was adopted by both the CEB and the General Assembly (copy attached at Annex C), outlines the responsibilities

and accountabilities of all actors of the United Nations, including Executive Heads of UN system organizations. The IASMN strongly recommends the full and active implementation of this Framework.

12. In order to fulfil these responsibilities and accountabilities, it will be necessary for all Executive Heads and their senior managers to understand the concept of risk management and the steps that can be taken to implement mitigating strategies. In summary, the challenge will be to decide what level of risk is acceptable depending on the importance of a programme goal. Unacceptably high risks must be avoided or brought within acceptable levels with risk management strategies. These can be categorized in four groups, namely, a) the acceptance of risk (no further action required); b) controlling the risk (prevention and mitigation measures e.g. Minimum Operating Security Standards); c) avoidance of risk (temporarily distancing the potential target from the threat); d) transference of the risk (sub-contracting or insurance). This concept is outlined in a very useful guide prepared by UNICEF, the principles of which have been endorsed by the IASMN, which is attached as Annex D. The IASMN recommends that this guide be utilized to develop a common framework for risk management strategy that can be adopted across the United Nations system.

13. In this regard, the IASMN takes note that there are a number of emerging related risk management strategies in various organizations such as Early Warning/Emergency Preparedness and Response Planning, Enterprise Risk Management/Business Continuity Planning. The IASMN points out that, although there is some interaction between these mechanisms, they are operating in mainly independent silos. Whilst pointing out that security risk management is the clear remit of DSS, the IASMN nonetheless recommends that risk management be mainstreamed in the work of organizations and that common approaches, where possible, be developed to ensure greater coherence, inter-operability and inter-dependence. This matter will be taken up by the IASMN Steering Group.

14. The IASMN recommends that security must be considered as an integral part of every activity undertaken by the organizations of the UN system and must not be treated as an add-on either for programmatic or budgetary purposes. The IASMN recommends that the existing mechanism for security risk management must be integrated into programme planning and design, including in the development of individual project proposals and in planning frameworks such as CCA/UNDAF and CHAP/CAP. The IASMN also points out that future security challenges will not solely be linked to terrorism and criminality but also to the management of an increasing numbers of natural and manmade disasters including those resulting from climate change, and that security must also be considered in this context.

15. Noting the need for system-wide coherence and crisis response at Headquarters levels of the UN security management system, the IASMN recalls that the management and administration of security policies and procedures within each organization rests with the senior security managers/security focal points. The IASMN recommends that it is critical that such officials have immediate and unimpeded access to executive level management and to be provided with adequate resources, both human and financial, to enable them to discharge their responsibilities under the Accountability Framework.

16. The IASMN notes that there remains a lack of systematic information exchange between various entities of the United Nations security management system. The IASMN recommends that risk information and analysis, which is developed by a number of UN organizations, must be shared by all concerned to avoid duplication of time and effort and to ensure consistency and accuracy. In this connection, the IASMN has already adopted Information Sharing Protocols outlining how to share information without violating confidentiality.

17. The IASMN also points out that it will not be possible to manage risk and security- related issues in the absence of commercially available secure telecommunications and an information technology system

which is compatible across the UN system with full inter-connectivity and inter-operability at all levels. The IASMN recommends that the HLCM instruct the IT Network to address this issue as a matter of priority.

18. In order for any risk management strategy to be successful, it requires that information be provided on a timely and accurate basis at the country level. In this regard, the IASMN strongly recommends that a security analyst be employed as part of the DSS team to support Designated Officials and Security Management Teams in the gathering, analysis and dissemination of relevant information. The IASMN also recommends that where there are existing Joint Mission Analysis Centres (JMACs) and/or Security Information Operation Cell (SIOCs), the terms of reference and remits for these entities would need to be broadened to ensure that they are operating on an inter-organizational and inter-departmental basis and need.

19. The IASMN points out that the adoption and implementation of a Risk Management Strategy will require a significant education and training programme for Executive Heads and their Managers at the headquarters, regional and country levels. The IASMN notes that, more often than not, senior staff are selected and deployed with little or no training to be able to discharge the significant responsibilities placed upon them. IASMN recommends that DSS be given the resources to develop and implement a highly focused training programme in conjunction with resources and capacities of other training entities, to be provided to managers, prior to assuming their responsibilities, to include leadership, risk and crisis management skills. This training should further be complemented by a continuing, rolling programme involving table-top and practical exercises to further develop, maintain and enhance the skills of individual managers and management teams to deal with crises and emergencies that impact on the ability to maintain business continuity and the safety and security of staff and assets.

20. The IASMN points out that a risk management strategy involves the acceptance of a certain level of risk by both the employer and the employee. In this connection, the IASMN recommends that an urgent review, to be carried out by the Human Resources Network, is required of the contractual arrangements in place to ensure that personnel are compensated commensurate with the security risk they are being asked to take.

21. The question of adequate and sustainable funding for security continues to be a fundamental stumbling block. The IASMN recommends that this matter must be addressed through a shift in perception. The IASMN points out that in many organizations of the UN system, measures required for programme delivery are more often than not exclusively included under the security budget. Instead, the IASMN recommends that a system-wide determination must be made as to what measures belong under programme delivery costs, and what measures properly constitute security cost. For these strictly security costs, the IASMN recommends that the HLCM consider how best to ensure that each organization provide adequate sustainable funding for all its security activities. For example every organization of the UN system could have a dedicated budget line for the application of safety and security, including for every project (also comprising technical cooperation projects). Alternatively, security costs could be included as a percentage of common staff costs within each organization.

22. Further to the above, with regard to the issue of funding of security, at its meeting in October 2006 the HLCM, whilst agreeing that DSS was significantly under-resourced, decided that, due to zero growth budgets across the system, no further funding of security was possible. The impact of this decision is that many of the recommendations regarding security and safety of staff put forward by IASMN and approved by HLCM, have not been implemented because, out of necessity, they involve additional costs. The HLCM had requested that DSS demonstrate that the resources were being utilized effectively for the purposes for which they were provided and requested that a more results-based management approach be adopted. This has been achieved, as is reflected in the 2008-2009 strategic framework for DSS. Whilst the concept of providing value for money is fully accepted, the inescapable outcome from the Lessons Learned reports for Lebanon in 2006, DRC in 2007 and more recently the tragedy in Algiers has shown that a lack of resources (particularly

a lack of surge and crisis management capacity) has impacted the effectiveness of the UN security management system and, thus, the ability to enable UN programmes and keep staff and assets safe at the same time. The IASMN therefore recommends that the HLCM revisits the specific issues of ensuring that security is provided with the requisite funding.

23. The IASMN also considered possible alternative sources of funding to be considered by HLCM. The IASMN has already recommended (in its October 2007 report) that the unspent balance from the cost-shared budget should be retained in a contingency fund and utilized in accordance with inter-agency agreements. In order to enhance an unexpected crisis response capacity, the IASMN recommends that DSS be authorized to engage with Member States to enter into stand-by agreements for the provision of specialized expertise such as telecommunications surge capacity, blast engineers, etc. The IASMN also recommends that, for those organizations whose financial rules allow such actions, consideration should be given to raise funds from private and public channels, notably through the utilization of consultant firms.

24. The United Nations security management system cannot act in isolation of host governments, especially in light of the increase in threat and risk. It will therefore be necessary to engage more closely with host country authorities to explain the threats against the organizations of the UN system and to establish effective liaison with them to assist the UN in becoming more secure. In this connection the IASMN points out that it may be necessary to put in place supplementary agreements either between the organizations of the United Nations system and the Host Country, or on a system-wide basis at the duty station, outlining the latter's specific responsibilities of the safety and security of United Nations system personnel and their premises. To further this process, the IASMN requests the Office of Legal Affairs to circulate a model agreement so that members can finalize the content the Security Management Team in their discussions with host country authorities.

25. The IASMN wishes to point out that the existing governance mechanism for the UN security management system which was established by HLCM, endorsed by CEB and approved by the General Assembly provides an all-inclusive system which has successfully taken security forward over the past few years. The IASMN does not believe that creating any new mechanisms or structures would add any value to the existing mechanism. Instead, the IASMN believes that the inclusion on a systematic basis of those entities which have significant field presence and which do not at present fully participate in the work of IASMN (such as the Office for Drug Control, the Department of Political Affairs, the Department for Field Support and the Department for Peace-keeping Operations), would further strengthen and enhance the existing governance mechanism. The IASMN also wishes to point out that its membership consists not only of senior security professionals but also Directors of Administration and Operations, thus ensuring that discussions incorporate the perspective of a wide range of disciplines.

26. As outlined in paragraph 3 above, IASMN considered a letter from the Secretary-General to the Chairperson of the HLCM and the Under-Secretary-General of DSS transmitting specific requests from the Policy Committee. Following extensive discussions, the IASMN recommends the following with regard to the each request:

(a) "HLCM and IASMN should develop a proposed strategy to secure substantial additional resources for staff security, both technical and financial. This should include the significant investment that will be required to establish secure premises for the UN system in high-risk locations, as well as additional resources for the UN's crisis response capacity."

The IASMN considered the three parts of this request:

i. **The requirement for additional technical and financial resources**;

- The recommendations of the IASMN regarding financial resources are contained in paras. 9e, 21-23 above. With regard to technical resources, the IASMN points out that the number of professional security advisers, analysts, trainers, and critical incident stress counsellors is still far from sufficient, given the existing requirements. For example, there are still 58 countries of the 180 where the UN has a presence where there is no professional security adviser and others where the SRA identifies shortfalls. The IASMN recommends, subject to the outcome of the independent panel, that there be an urgent review of staffing levels across the UN security management system.

- The IASMN strongly reiterates that the implementation of Minimum Operating Security Standards is the cornerstone of the UN security management system and must be commensurate with the Security Risk Assessment. In this connection the IASMN recalls that providing for the safety and security of personnel of the United Nations system remains the responsibility of the employing organization irrespective of their physical location. In light of the step change which has occurred, the IASMN believes that further refinement of the MOSS is required and has established a working group to consider how the MOSS can be redesigned to make it more effective.

ii. **The establishment of secure premises**

- The IASMN recommends that the establishment of security premises must be based on a duty-station specific evaluation, using the security risk assessment process, which will determine whether common UN premises or single-agency premises are required to respond to the particular threat in that location. In this regard, in order to ensure a degree of consistency in consideration of this matter, the IASMN recommends that a project be established to consider the ideal design of UN common premises and compounds which will require the development of standards. This project will require expertise (architectural, engineering, etc.) which currently is not available within the UN system. Using this as a basis it will be necessary to consider a long term funding and business investment strategy requiring input from the Member States. The IASMN believes that this falls within the remit of the HLCM.

iii. **The additional requirements for crisis response capacity**.

- The recommendations of the IASMN regarding this matter are in paras 11 and 22 above.

(b) "The need to improve financial and psychosocial support for survivors and families in the event of a crisis, building on lessons learned from the attacks in Algiers and Baghdad"

The IASMN considered the two parts of this request:

i. **The requirement to improve the financial support for survivors and families of a crisis**

- The IASMN does not have the mandate to make recommendations on this matter and believes that this should be considered by the HLCM.

ii. **The requirement to improve psychosocial support for survivors and families.**

- The IASMN points out that, whilst there is some capacity within the UN system to provide psychosocial support to staff, there are not enough critical incident stress counsellors to respond to a major crisis. In addition, in the aftermath not only of Baghdad and Algiers but also of the dozens of other incidents involving the death and injury of staff, what has been lacking is the long-term follow-up and support. Noting that there are only 72 counsellors responsible for providing psycho-social support to 400,000 staff and dependents at 185 duty stations, the IASMN recommends that the number of such counsellors must be significantly increased across the UN system.

- With regard to long-term follow up and assistance, the IASMN also recommends that an urgent review be undertaken of the 269 families of victims who have lost their lives to malicious acts since 1992 to determine the lessons learned and to develop strategies for the future.

(c) "Sharing information and statistics on security casualties across the spectrum of UN entities and activities to support a more comprehensive analysis of the types of risks UN staff face."

- The IASMN points out that statistics are only indicators and that what must be assessed is the impact of the various incidents on the delivery of programmes. Although some data bases have been created to capture the statistics, the recording of the data is not consistent. The IASMN recommends that, in addition to capturing the incidents reported to security, there must be a link into insurance, medical and buildings managers to have a comprehensive indication of the number and type of incidents that are occurring.

- The recommendations of the IASMN with regard to information sharing and information analysis are contained in paras 16-18 above.

(d) "Promoting the full implementation of the accountability framework for the UN security management system and examining more closely the Designated Official system."

The IASMN considered the two parts of this request:

i. **Promoting the full implementation of the framework for accountability for the UN security management system**

- The IASMN recalls that the Framework for Accountability for the UN Security Management System has been approved by the CEB and mandated by the General Assembly and is a fundamental management tool to identify and correct deficiencies in the security management system. The IASMN recommends that the CEB direct each of its members to ensure that the accountability framework has been implemented as a policy within their own organization as a means of ensuring that comparable security policies are in place across the UN system.

- The IASMN recommends that Executive Heads thoroughly familiarize themselves with the accountability framework. Thereafter, IASMN recommends that Executive Heads direct that all personnel of their organization be trained at every level, in security and risk management. The recommendations of the IASMN with regard to training are contained in para. 19 above.

- The IASMN also points out that there appears to be a lack of understanding amongst the Department Heads of the United Nations Secretariat and Tribunals regarding their accountability with respect to security of staff and recommends that urgent action be taken to correct this lacuna.

- The IASMN recommends that internal oversight mechanisms within each organization incorporate compliance with the UN security management system in their assessment process, also utilizing information available in the DSS Compliance, Evaluation and Monitoring Unit. The IASMN also recommends that there be a greater exchange of information and coordination between DSS and the internal Audit departments of the organizations of the United Nations system.

ii. **Examining more closely the Designated Official system**

- With regard to the Designated Official system, the IASMN points out that, in accordance with the resolution of the General Assembly, the Designated Official function is entrusted to the senior most official in the country. However, the IASMN points out that this decision is not being applied consistently since in many cases there are representatives of agencies, programmes and funds who outrank the UN Resident Coordinator but who are not appointed as Designated Officials. In most instances the Designated Official is either a Special Representative of the Secretary-General or a Resident Coordinator. The IASMN recommends that, subject to the outcome of the Independent Panel, a review of the decision of the General Assembly should be undertaken to determine whether this approach is still appropriate, given the step change in security.

- The IASMN also points out that the function of Designated Official is often the third or fourth hat of an individual who is already tasked to be the Resident Coordinator, Humanitarian Coordinator, etc. These individuals are being asked to be superhuman in carrying out these functions where there will necessarily be tension, if not conflict of interest, between the deliveries of the various functions. The IASMN therefore recommends that this issue be urgently considered by the UN Development Group as well as the HLCM and CEB.

- In order to strengthen the position of the Designated Official vis-à-vis the host country authorities, the IASMN recommends that the functions of Designated Official be included in the letter of accreditation which is sent to the Government. This is particularly critical for Resident Coordinators and SRSGs. In addition, the IASMN recommends that consideration be given to including the functions of Designated Official in the country level agreements signed between the United Nations and the host country.

- The IASMN recommends that Designated Officials be empowered by the CEB to ensure compliance with security policies, practices and procedures by all organizations of the UN system present at the duty station. In this regard, Designated Officials should be supported by all organizations in implementing appropriate sanctions under the applicable rules, as required. For example, this could include the withdrawal of security clearance for any individuals and/or organizations who act in violation of security policies, practices and procedures. In addition, the IASMN recommends that the Secretary-General urge CEB members to take appropriate measures against those individuals who are in breach of policies, procedures and practices of the UN security management system and to provide a yearly report on such actions taken.

- The IASMN also considered the concerns expressed by the small group of Designated Officials who met in Cairo regarding the support provided to them. Whilst fully cognizant of the need to support Designated Officials, the IASMN notes that these Designated Officials have made a number of suggestions which would fundamentally change the UN security management system and its system of checks and balances. The IASMN cannot endorse proposals related to the reporting lines of security advisers or security budgets; the IASMN also does not believe that the creation of yet another consultative group as suggested by some Designated Officials is desirable as this would unnecessarily complicate and add another tier to the security management process. Instead the

IASMN decides that it would be more practical and beneficial to invite one Designated Official from each region on a rotating basis, to attend an IASMN meeting each year in order to exchange views on matters and resolve issues which are of concern to them with the entire UN security system instead of piecemeal.

- The IASMN points out that at present, DSS is only given a very limited amount of time to provide Designated Officials and Designated Officials, a.i. with training prior to their deployment. The situation is even more serious for Special Representatives of the Secretary-General, few if any of whom come for security training. The IASMN recommends that urgent action is required to ensure that the appropriate level and amount of training is provided to all Designated Officials prior to their deployment. Other recommendations of the IASMN in connection with training are located in paras 9d and 21 above.

e) "Considering how staff security aspects may be included in the earliest stages of planning at the country level, particularly in high-risk/complex environments;"

- The IASMN recommends that references to high-risk/complex environments should be discontinued. In the view of the IASMN such definition is unnecessarily restrictive since situations can change rapidly. Given the global terrorist threat against the UN, whilst it may be possible to identify locations which today meet the criteria for high risk, it would be irresponsible not to implement identified strategies across the board for each duty station and area of operation. Instead, the IASMN recommends that, whilst taking into account the need to prioritize resources, a security risk assessment must be conducted on a regular basis at all duty stations at country, capital and sub-regional level to ensure that the requisite mitigating measures have been identified and implemented.

f) "Establishing a comprehensive mechanism for information management as it relates to the security of UN staff and operations, i.e. how this information is processed, analyzed and disseminated."

- The recommendations of the IASMN are contained in paras. 16-18 above.

g) "Consolidating all previous recommendations arising out of the reviews, investigations, lessons learned and studies conducted on the UN security management system."

- The IASMN has considered a consolidated matrix of recommendations prepared by DSS and is in the process of prioritizing those which have not been implemented. These will be forwarded to the Independent Panel, at the request of its Chairman.

27. In conclusion to this part of the report of the IASMN which has addressed the direct request of the Secretary-General, the discussions of the IASMN were very full and frank and focused primarily on furthering the agenda of security management. The IASMN wishes to reiterate yet again that the purpose of security is not only to enable the effective delivery of UN activities but also to maintain the safety, security and well-being of staff as a high priority. By ensuring that the concepts of security management are mainstreamed into every day activities, and given the necessary level of importance within each organization, the goals of the organizations that make up the UN security management system can be achieved without unnecessarily sacrificing the lives of staff.

==========

OTHER ISSUES

28. The IASMN also considered a number of items which had been on its agenda prior to the meeting of the Policy Committee and has made the following recommendations:

HUMAN RESOURCES STRATEGY

29. The IASMN considered and recommends approval of the report prepared by DSS on a human resources strategy with the following specific recommendations:

i) Noting the dearth of women applicants for security positions, the IASMN requests its members to develop additional strategies to identify and recruit women security officers, including identifying women who could be trained to be security advisers;

ii) With regard to language training, the IASMN encourages security staff to improve their language skills in the official languages and, subject to criteria to be developed by DSS, recommends that these staff be provided support and, if possible, financial assistance to defray part of the costs.

iii) Noting the concerns expressed regarding the UNDP Results and Competency Assessment (RCA) in the assessment of security advisers, the IASMN requests DSS to consider the use of 180 or 360 degree assessments; The IASMN also requests that the role of DSS in the assessment process be clarified. On a related matter, the IASMN requests that for short-term staff on mission, appraisals be prepared to reflect the performance of the officer

iv) The IASMN requests DSS to develop a strategy to identify and mentor qualified officers in the Safety and Security Services who have the potential to become security advisers.

v) Given the specialized technical nature of the professional security field, the IASMN requests DSS to raise with OHRM the possibility of obtaining exemptions from Human Resources requirements for security personnel that inhibits the movement of personnel across categories of staff.

vi) With regard to the exchange of security personnel amongst organizations of the UN system, the IASMN requests DSS to prepare a framework agreement for this purpose, to include SSS officers.

vii) With regard to background checks for security personnel, the IASMN requests DSS, in conjunction with OHRM and OLA, to consider establishing a mechanisms to identify officers who have been removed from their functions for non-performance of their responsibilities or for disciplinary reasons.

vix) With regard to entry level screening, the IASMN requests DSS to discuss with the medical directors to consider the possibility of establishing specific entry level screening requirements for security personnel

COMPLIANCE ISSUES

30. The IASMN considered a report by DSS regarding the activities of the Compliance, Evaluation and Monitoring Unit. The IASMN reiterates that the role of the Compliance Unit is primarily to help Designated Officials and members of Security Management Teams to identify gaps in the system and to recommend

remedial action. This provides a very positive support mechanism. The only time a more adversarial approach is required is when there is a persistent failure to act upon and correct identified deficiencies which impact on the safety and security of staff. The IASMN recommends the following :

i) In the first instance, cases of non-compliance should be reported to the relevant security focal point. In cases where there is no improvement in the situation, then the matter should be brought to the attention of the Executive Heads by the USG/DSS for action.

ii) In the event that an organization at a particular duty station does not implement the recommendations of a compliance mission, the IASMN recommends that consideration should be given to denying security clearance to staff from that organization in the country.

iii) The IASMN requests DSS Compliance Unit to carry out spot checks of responses provided to it during compliance missions.

vi) The IASMN approves the overall MOSS country appraisal compliance rating system proposed by DSS.

MORSS

31. The IASMN considered a conference room paper prepared by WHO regarding the implementation of Minimum Operating Residential Security Standards (MORSS). The IASMN notes with concern that MORSS, which is designed to reimburse residential security measures at the home of internationally-recruited staff members, is being used for other purposes. In this connection IASMN recalls that the original intent of residential security measures was to provide reimbursement for bars, alarms and guards. The IASMN reiterates that all proposed MORSS measures must be justified by the Security Risk Assessment.

32. The IASMN recommends that reimbursement or payment for residential guards normally will be provided for guards who are security professionals hired through private guard companies which have been vetted by the Security Adviser.

33. In light of the concerns expressed in para. 31 above, the IASMN recommends that the Human Resources Network review MORSS arrangements with a view to clarifying the domain of its application.

CRITICAL INCIDENT STESS MANAGEMENT

34. The IASMN was briefed by DSS regarding efforts to resolve the continuing disagreements amongst some stress counsellors of the UN system. The IASMN welcomes the positive steps being taken in this regard and looks forward to the outcome of the forthcoming critical incident stress counselling working group.

35. The IASMN commends the DSS Critical Incident Stress Unit (CISMU) for its decisive and positive response to the needs of staff in the aftermath of the incidents in Algiers, Chad and Kenya and recommends that the staffing of CISMU be increased to ensure that DSS is in a position to fulfil the mandate given to it by the General Assembly.

36. The IASMN recommends that the field coordination pilot project for hiring of stress counsellors be extended for one year and a detailed report provided to the IASMN at its February 2009 meeting.

MEDICAL SUPPORT IN THE FIELD

37. The IASMN considered a recommendation that the United Nations Medical Director participate in the IASMN. The IASMN welcomes this proposal which will help ensure that medical issues related to the safety and security of staff are included in its deliberations.

38. The IASMN notes with concern the variety of different contracts between organizations of the United Nations and a private emergency medical service provider. The IASMN wishes to bring this matter to the attention of the HLCM so that the appropriate entities within the UN system could be requested to review this matter.

AVIATION SAFETY

39. The IASMN expresses grave concern regarding the lack of any significant progress on the critical issue of aviation safety. The IASMN points out that each of its members is required on a daily basis to address issues of aviation safety for which they do not have expertise. The IASMN also points out that there is no centralized expertise within the UN system to address this issue. The IASMN recalls that it has already recommended that a centralized Aviation Safety Unit must be established within DSS to provide the system-wide guidance which is required. The IASMN has made a number of recommendations regarding the issue of Aviation Safety which have been adopted by the HLCM but which have not been implemented. In light of the above, the IASMN decides that there is no value in developing further policy initiatives unless there is an Aviation Safety Unit in place to foster implementation.

40. Given the need for specific expertise authoritatively to handle the issues related to aviation safety, the IASMN therefore has no choice but to suspend all activities of the Aviation Safety Working Group until a centralized Aviation Safety Unit has been established and resourced.

POLICY ISSUES

41. The IASMN considered how best to systematize the means by which security policy is developed. Given the scope and breadth of this issue, the IASMN requests a Working Group, consisting of IASMN principals to consider this matter and report back to the full IASMN.

DSS LIAISON PROJECT DARFUR

42. The IASMN was provided with a progress report on the implementation of the NGO Liaison project in the Darfurs. The IASMN requests that DSS continue its evaluation of this project, to include full lessons learned, before expanding this project to other locations. In particular the IASMN expressed concern that, at a time when efforts were being undertaken to correct deficiencies in the UN security management system, the extension of this project to other locations needed to be carefully considered.

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

ADB	**Mr. Ken Chee**
CBD	**Mr. Victor Ogbuneke**
CTBTO	**Mr. Robert Erenstein**
EBRD	**Mr. Alan Drew**
FAO	**Mr. Michael Hage**
IAEA	**Ms. Maria E. Bermudez-Samiei**
	Ms. Lodi Wazir
IFAD	**Mr. Antonio Kamil**
ILO	**Mr. Brian Wenk**
IMF	**Mr. David Androff**
	Mr. Warren J. Young
	Mr. Charles Gleichenhaus
ITU	**Mr. Claude Vadeboncoeur**
OPCW	**Mr. Robert Simpson**
PAHO	**Mr. Edward Harkness**
	Ms. Sofia Benegas
UNAIDS	**Ms. Susie Bolvenkel-Prior**
UNDP	**Mr. Andrew Lukach (first day)**
	Mr. Jab Swart
UNESCO	**Ms. Magda Landry**
UNFPA	**Ms. Janie McCusker**
UNHCR	**Mr. Daniel Endres**
	Mr. Svante Yngrot
UNICEF	**Mr. Bill Gent**
UNIDO	**Mr. Ranko Vujacic**
	Mr. Paul Maseli
UNOPS	**Mr. Richard Nasereddin**
UNRWA	**Ms. Laura Londen**
UNU	**Mr. Anthony Powers**
UNV	**Ms. Michele Rogat**
UPU	**Mr. David Bower**
WFP	**Mr. Mick Lorentzen**
WHO	**Mr. Patrick Beaufour**
WIPO	**Mr. Drew Donovan**
WMO	**Mr. Michel Nicolas**
World Bank	**Mr. Van Pulley**
	Mr. Chris Shorter
	Ms. Autumn Hottle

DEPARTMENTS OF THE UNITED NATIONS SECRETARIAT

DEPARTMENT OF PEACE-KEEPING OPERATIONS	**Mr. Tom Hojbjerg (first day)**
DEPARTMENT OF SAFETY AND SECURITY	**Mr. David Veness (first day)** **Mr. Gerard Martinez** **Mr. Gerry Ganz** **Mr. Bruno Henn** **Ms. Neeta Tolani** **Mr. Igor Mitrokhin** **Mr. John Logan**
INTERNATIONAL CRIMINAL TRIBUNAL FOR RWANDA	**Ms. Sarah Kilemi**
OFFICE FOR THE COORDINATION OF HUMANITARIAN AFFAIRS	**Mr. David Kaatrud**
OFFICE OF THE HIGH COMMISSIONER FOR HUMAN RIGHTS	**Mr. Stuart Groves**
OFFICE OF LEGAL AFFAIRS	**Mr. Antonio Menendez-Zubillaga**

OBSERVER

CCISUA	**Mr. George Odoom**

ANNEX B

AGENDA OF THE IASMN

1. Consideration of the Report of the Policy Committee and Letter from the Secretary-General

2. Briefing on Heightened Threat to United Nations (Step Change) by Under-Secretary General for Safety and Security

3. Lessons Learned – Algiers

4. Global Threat Assessment

5. Information Sharing Protocols

6. Compliance

7. Minimum Operating Security Standards

8. Policy Issues

9. Human Resources Management for Security Professionals

10. Host Country Agreements

11. Minimum Operating Residential Security Standards

12. Critical Incident Stress Management

13. Aviation Safety

14. Lessons Learned – NGO Project

15. Other Matters
    Medical Support in the Field

ANNEX C

INTER-ORGANIZATIONAL SECURITY MEASURES; FRAMEWORK FOR ACCOUNTABILITY FOR THE UNITED NATIONS SECURITY MANAGEMENT SYSTEM

I. INTRODUCTION

1. The primary responsibility for the security and protection of personnel employed by the United Nations system organizations, their spouse and other recognized dependants and property and of the organizations' property rests with the Host Government. This responsibility flows from every government's normal and inherent function of maintaining order and protecting persons and property within its jurisdiction. In the case of international organizations and their officials, the government is considered to have a special responsibility under the Charter of the United Nations or the government's agreements with the individual organizations.

II. MISSION STATEMENT OF THE UNITED NATIONS SECURITY MANAGEMENT SYSTEM

2. The goal of the United Nations security management system is to enable the effective and efficient conduct of United Nations activities while ensuring the security, safety and well-being of staff as a high priority.

III. ACTORS WITHIN THE UNITED NATIONS SECURITY MANAGEMENT SYSTEM

A. The Secretary-General

3. Under Article 97 of the Charter of the United Nations, the Secretary-General is the chief administrative officer of the Organization; the mandates promulgated by the principal organs are entrusted to him for their implementation under Article 98. The Secretary-General is thus accountable to the Member States for the proper running and administration of the Organization and implementation of its programmes to include, in the context of this framework, ensuring the overall safety and security of United Nations personnel at headquarters locations and in the field, as well as United Nations premises and assets at headquarters and field locations. The Secretary-General can delegate authority to the various Under-Secretaries-General who are in turn, individually or collectively, accountable to him, as appropriate.

B. The Under-Secretary-General for Safety and Security

4. The Under-Secretary-General for Safety and Security is directly accountable and reports to the Secretary-General. He/she is responsible for the executive direction and control of the United Nations security management system and the overall safety and security of United Nations civilian personnel and their recognized dependants at both headquarters locations and in the field, as well as United Nations premises and assets at field and headquarters locations. He/she represents the Secretary-General on all security-related matters. He/she is responsible for developing security policies, practices and procedures for United Nations system personnel worldwide, and coordinating with the organizations of the United Nations system to ensure implementation, compliance and support for security aspects of their activities; preparing

reports of the Secretary-General on all security related matters; and advising the Secretary-General on all matters related to security and safety of civilian personnel of the United Nations system.

C. Executive Heads of United Nations systems organizations[1]

5. Executive Heads of the United Nations funds and programmes are responsible and accountable to the Secretary-General for ensuring that the goal of the United Nations security management system is met within their respective organizations. Without prejudice to their accountability to their own governing and legislative bodies, Executive Heads of the United Nations specialized agencies and of other organizations participating in the UN security management system recognize the coordinating role and authority of the Secretary-General in matters related to safety and security of United Nations personnel and commit themselves to ensuring that the goal of the United Nations security management system is met.

D. Senior Security Managers and/or headquarters Security Focal Points

6. The executive heads will appoint a Senior Security Manager and/or headquarters Security Focal Point to be responsible for coordinating the organization's day-to-day response to safety and security and providing all the relevant actors with advice, guidance and technical assistance.

E. Designated Officials

7. In each country or designated area where the United Nations is present, the senior most official is normally appointed as the Designated Official for Security. The Designated Official is accountable to the Secretary-General, through the Under-Secretary-General for Safety and Security, for the security of personnel employed by the organizations of the Untied Nations system and their recognized dependants throughout the country or designated area. The Designated Official is responsible and accountable for ensuring that the goal of the United Nations security management system is met at the duty station.

F. Representatives of organizations participating in the United Nations security management system

8. Representatives of organizations (the "country representative", "agency head" or "head of mission") of the United Nations system participating in the United Nations security management system are accountable to the Secretary-General through their respective executive heads, under the overall guidance of the Under-Secretary-General for Safety and Security, for all matters related to the security of their personnel at the duty station.

G. Security Management Team

9. The Security Management Team shall normally consist of the Designated Official, who acts as chair, the head of each United Nations organization present at the duty station, and the Chief Security Advisor. The Security Management Team advises the Designated Official on all security related matters. In peacekeeping missions, where the Head of Mission serves as the Designated Official, the Security Management Team may also include Heads of Offices or Sections, as specified by the Designated Official. Members of the Security Management Team have a collective responsibility to support the Designated Official in the discharge of

[1] The term 'organizations' includes: the major organizational units of the Secretariat that have heads officially accountable to the Secretary-General; other bodies subsidiary or related to the United Nations such as the United Nations funds, agencies, and programmes; and organizations participating in the United Nations security management system.

his/her mandate related to the safety and security of all personnel employed by the organizations of the United Nations system and their recognized dependants.

H. Area Security Coordinators

10. Area Security Coordinators are staff members appointed in writing by the Designated Official, in consultation with the Security Management Team, in areas of larger countries that are separated from the capital in terms of both distance and exposure, in order to coordinate and control security arrangements applicable to all personnel employed by organizations of the United Nations system and their recognized dependants in their area of responsibility. Area Security Coordinators are accountable to the Designated Official for their security-related responsibilities, in accordance with their respective Letters of Appointment.

I. Chief Security Adviser/Security Adviser

11. The Chief Security Adviser/Security Adviser is a security professional appointed by the Under-Secretary-General for Safety and Security to advise the Designated Official and the Security Management Team in their security functions. The Chief Security Adviser/Security Adviser reports to the Designated Official and maintains a technical line of communication to the Department of Safety and Security. In the absence of a Chief Security Adviser/Security Adviser, the Designated Official, in consultation with the Department of Safety and Security, should appoint a Country Security Focal Point for the Security Management Team.

J. Country Security Focal Point (if applicable)

12. In the absence of a Chief Security Adviser/Security Adviser, the Designated Official, in consultation with the DSS and the staff member's employing organization will appoint an international staff member to act as Country Security Focal Point for the Security Management Team. CSFPs are accountable to the Designated Official for the security-related responsibilities, in accordance with their respective letters of appointment.

K. Other Security Personnel of the Department of Safety and Security

13. Security personnel of the Department of Safety and Security are responsible for assisting the Chief Security Adviser and the Designated Official, and are accountable to their respective heads of office.

L. Single-Agency Security Officers

14. Single-Agency Security Officers are security professionals hired by organizations of the United Nations security management system to advise their respective organizations and to be responsible for the security aspects of activities that are specific to their organizations. Single-Agency Security Officers report to their agency's Head of Office, while at the same time supporting the Designated Official under the coordination of the Chief Security Advisor.

15. When required to act as the Chief Security Adviser ad interim for a specified period, in the absence of the Chief Security Adviser for a given duty station, this will be confirmed in writing by the Designated Official and include the terms of reference of the Chief Security Adviser for accountability purposes.

M. Wardens

16. Wardens are appointed in writing by the Designated Official, in consultation with the Security Management Team, to ensure proper implementation of the security plan in a predetermined zone of a large

city. Wardens are accountable to the Designated Official/Area Security Coordinator for their security-related functions, irrespective of their employing organization.

N. Personnel employed by organizations of the United Nations system

17. Personnel employed by the organizations of the United Nations system are accountable to their respective organizations. All such personnel have the responsibility to abide by security policies, guidelines, directives, plans and procedures of the United Nations security management system and their organizations.

IV. CONCLUSION

18. This framework for accountability provides clear guidance as how to enable "the effective and efficient conduct of United Nations activities, while ensuring the safety, security and well-being of staff as a high priority". This goal may be attained by ensuring that all actors of the United Nations security management system are empowered by providing them with the necessary resources, training and a clear understanding of their roles and responsibilities.

19. The roles and responsibilities of all actors of the United Nations security management system for which they will be held accountable are attached at Annex.

ANNEX

ROLES AND RESPONSIBILITIES OF ACTORS WITHIN THE UNITED NATIONS SECURITY MANAGEMENT SYSTEM

A. The Secretary-General

The Secretary-General ensures the overall safety and security of United Nations personnel at headquarters locations and in the field, as well as that of United Nations premises and assets at headquarters and field locations.

B. Under-Secretary-General for Safety and Security

The Under-Secretary-General for Safety and Security:

a) Advises the Secretary-General on all matters related to security and safety of civilian personnel of the United Nations system;
b) Represents the Secretary-General on all security-related matters;
c) Manages the Department of Safety and Security;
d) Manages the development of security policies, practices and procedures for personnel employed by the United Nations system worldwide;
e) Coordinates with the organizations of the United Nations system to ensure implementation, compliance and support for security aspects of their activities;
f) Prepares reports of the Secretary-General on all security related matters; and
g) Directs the organizational response to crisis management as required.

C. Executive Heads of United Nations organizations[2]

The Executive Heads:

a) Ensure that safety and security are core components of all programmes and activities;
b) Ensure that all managers and personnel working for them not only support the Secretary-General but also discharge their responsibilities in ensuring compliance with the United Nations security management system;
c) Ensure the resources necessary to achieve the goal of the United Nations security management system are provided;
d) Liaise closely with the Under-Secretary-General for Safety and Security to ensure a coherent system-wide approach to security;
e) Have a collective responsibility to work together to implement and contribute to the development of the United Nations security management system and to support the Secretary-General in ensuring that the legislative mandates given to him by the General Assembly are discharged;
f) Have an obligation to advocate in all available forums to ensure that Member States provide for the safety and security of all personnel employed by the organizations of the

[2] The term 'organizations' includes: the major organizational units of the Secretariat that have heads officially accountable to the Secretary-General; other bodies subsidiary or related to the United Nations such as the United Nations funds, agencies and programmes; and organizations participating in the United Nations security management system.

United Nations system and their recognized dependants and that crimes against such personnel will not be tolerated and the perpetrators brought to justice;
g) Have a "duty of care" to ensure that personnel employed by the organizations of the United Nations system and their recognized dependants are not exposed to exceptional risk and that all measures are taken to mitigate risks;
h) Appoint one individual as the senior security manger and/or headquarters security focal point;
i) Recognize and reward good performance in security management; and
j) Ensure that provision is made to address specific security concerns for women as required.

D. Senior Security Managers and/or headquarters Security Focal Points

The Senior Security Manager and/or headquarters Security Focal Point is responsible for:

a) Advising the Executive Head or Senior Programme Manager on security matters and keeping him/her updated on security management issues;
b) Ensuring that Country Representatives or Heads of Mission of the organization are aware that they must participate fully in the Security Management Team, as applicable;
c) Assisting/supporting in the mobilization of resources to assist field offices in the implementation of security requirements;
d) Serving as a member of the Inter-Agency Security Management Network;
e) Working in close association with the Department of Safety and Security and other members of the Inter-Agency Security Management Network, as well as supporting the Under-Secretary-General for Safety and Security in the discharge of his/her responsibilities;
f) Providing advice to field representatives for the implementation of minimum operating security standards and minimum residential security standards, as applicable;
g) Ensuring that all personnel employed by the organizations of the United Nations system and their recognized dependants of the agency are aware of the training requirements and facilitating the provision of security training and briefings to all personnel of the organization and their dependents;
h) Disseminating information and education regarding security matters; and
i) Monitoring and reporting on compliance with security policies, practices and procedures.

E. Designated Officials

The Designated Official is responsible for:

a) Ensuring the observance of the arrangements detailed in the United Nations Field Security Handbook and subsequent security policies and directives, as well as developing and implementing the required plans for the duty station with the aim of maintaining the security and safety of personnel employed by the United Nations system and their property, or that of the organizations.
b) Supervising and enabling the security personnel at the duty station to effectively discharge their functions;
c) Recommending to the Under-Secretary-General for Safety and Security a suitable nomination to act as Designated Official ad interim. Such appointees normally will be the head of an organization. At those locations where there is a peace-keeping mission the Designated Official ad interim is normally the Resident Coordinator;
d) Keeping the Secretary-General informed, through the Under-Secretary-General for Safety and Security, of all developments in the country that have a bearing on the security and

protection of the civilian personnel employed by the organizations of the United Nations system and their recognized dependants and their property, or that of the organizations. In the event that operational matters affect security or inter-agency security issues, this information must be communicated to the Under-Secretary-General for Safety and Security;

e) Implementing any arrangements decided by the Secretary-General in support of the Host Government's measures for the security and protection of personnel employed by the organizations of the United Nations system, their recognized dependants and their property and of the organizations' property, as well as maintaining liaison with the Government of the host country on matters concerning the security and protection of these individuals;
f) Ensuring collaboration on security with intergovernmental and non-governmental organizations working as operational partners of the United Nations system in accordance with established guidelines;
g) Ensuring the regular functioning of the Security Management Team and identifying staff members who will have special responsibilities in this regard;
h) Keeping the members of the Security Management Team, as well as the senior officials of each organization at the duty stations (as applicable) fully apprised of all security-related information and measures being taken in the country;
i) Ensuring that all personnel employed by the organizations of the United Nations system are appropriately equipped with required safety and security equipment as specified in minimum operating security standards and trained in its use;
j) Including staff members and the recognized dependants of intergovernmental and non-governmental organizations that have signed the Memorandum of Understanding in security arrangements at the duty station;
k) Ensuring that there is a fully integrated functioning and operational communications system for security management;
l) Appointing, together with the Security Management Team, Area Security Coordinators and Wardens and verifying that the team has adequately trained and equipped them; as well as providing their parent agency with input for the individual's performance appraisal;
m) Ensuring that the special arrangements, agreed on an inter-agency basis to be implemented when internationally-recruited personnel are evacuated, are in place for locally-recruited personnel to include options for relocation within the country, as required;
n) In an emergency where it has not been possible to communicate with the Under-Secretary-General for Safety and Security, the Designated Official uses his/her best judgment in carrying out relocations/evacuations and reporting to the Secretary-General, through the Under-Secretary-General for Safety and Security, immediately thereafter;
o) Establishing a briefing system that will ensure that all personnel employed by the organizations of the United Nations system and their recognized dependants are advised of specific precautionary measures that they should take in relation to the security plan, and ensuring that all such personnel receive adequate and appropriate security training;
p) Submitting all requested reports to the Department of Safety and Security, as outlined in the United Nations Field Security Handbook or other directives from the Under-Secretary-General for Safety and Security;
q) Upon being advised of instances of non-compliance with United Nations security policies, practices and procedures, the Designated Official takes appropriate actions, including referral to the organization concerned, as well as reporting serious instances of non-compliance to the Under-Secretary-General for Safety and Security; and

r) Ensuring that provision is made to address specific security concerns for women as required.
s) If applicable, appointing, in consultation with the employing organization, a Country Security Focal Point and ensuring that the Country Security Focal Point receives appropriate training to fulfil his/her responsibilities.

F. Representatives of organizations participating in the United Nations security management system

The representatives of organizations participating in the United Nations security management system are responsible for:

a) Being responsible for the safety and security of personnel of their organizations at the duty station and their recognized dependants and for the implementation of the security plan;
b) Ensuring that safety and security is a core component of all programmes in the country and that appropriate funding is provided based on need;
c) Consulting with and assisting the Designated Official on all matters concerning security and the implementation and maintenance of both the security plan and minimum operating security standards and compliance with both;
d) Serving as members of the Security Management Team;
e) Advising the Designated Official, Chief Security Advisor and agency Security Focal Point on the particular concerns of his/her organization regarding security;
f) Ensuring full and complete compliance by his/her personnel and their recognized dependants with all security-related instructions;
g) Taking action on instances of non-compliance of security policies, practices and procedures and advising the Designated Official on actions taken;
h) Ensuring that specialized activities of the organization are conducted in a way that manages the risks to personnel;
i) Ensuring that the Designated Official is provided, on a regular basis, with updated lists of all personnel of the agency and their recognized dependants in the area;
j) Ensuring that the Designated Official is at all times informed of the whereabouts and the movement of agency personnel and their recognized dependants in the area, in accordance with procedures established at the duty station;
k) Reporting to the Designated Official and agency Security Focal Point all security-related incidents;
l) Ensuring that recognized dependants left in the duty station by internationally-recruited staff who are serving elsewhere, are accorded the same provision for security as dependants of international staff serving at the duty station;
m) Ensuring that arrangements are in place for intergovernmental and non-governmental organizations working as operational partners with the concerned United Nations agencies;
n) Ensuring that movement of all personnel is undertaken in accordance with United Nations system rules and procedures;
o) Ensuring that personnel have adequate and operating communications equipment in line with the minimum operating security standards;
p) Ensuring that all his/her personnel attend appropriate security awareness training and briefing; and
q) Personally attending all training programmes.

G. Security Management Team

Under the overall authority of the Secretary-General, through the Under-Secretary-General for Safety and Security and the Designated Official in the country, the Security Management Team has a collective responsibility for:

a) Working in close collaboration with the Designated Official;
b) Meeting on a regular basis to review the prevailing situation and ensuring that security is being managed effectively at all locations throughout the country where personnel employed by the United Nations system are present;
c) Ensuring that there are functioning and effective security and contingency plans that are maintained and implemented for all locations throughout the country where personnel employed by the United Nations system and their recognized dependants are present;
d) Ensuring that lists of personnel and their recognized dependants are up-to-date;
e) Ensuring that each Area Security Coordinator and Warden is trained and equipped to carry out his/her functions and ensuring that they understand fully and implement the complete range of these responsibilities;
f) Establishing minimum operating security standards and minimum residential security standards, based on a credible threat and risk assessment, at all locations throughout the country where personnel employed by the United Nations system and their eligible dependants are present, including the monitoring of its implementation, and ensuring compliance;
g) Ensuring that resources are available to implement all measures that are approved;
h) Providing input, as appropriate, on the performance appraisal of all security officers employed in the country by the United Nations system, where they have personnel operating; and
i) Ensuring that provision is made to address specific security concerns for women as required.

H. Area Security Coordinators

The Area Coordinator is responsible for:

a) Acting on behalf of the Designated Official from whom they have delegated responsibility to coordinate and control the security arrangements for sub-office operations outside the capital;
b) Appointing wardens for their area of responsibility;
c) Developing and maintaining area-specific security plans;
d) Maintaining lists of personnel employed by the organizations of the United Nations system and their recognized dependants at their location;
e) Implementing minimum operating security standards, based on an up-to-date threat and risk assessment;
f) Keeping the Designated Official systematically informed regarding incidents or developments in their area of responsibility that have a bearing on the security and safety of personnel employed by organizations of the United Nations system and their recognized dependants;
g) Convening meetings of the Area Security Management Team; and
h) Managing the security clearance system for their area.

I. Chief Security Adviser/Security Adviser[3]

The Chief Security Adviser/Security Adviser is responsible for:

a) Serving as principal adviser to the Designated Official and the Security Management Team on all aspects of security management, crisis readiness and preparedness at their respective duty stations and in the execution of responsibilities with regard to the security of personnel employed by the organizations of the United Nations system and their eligible dependents, and their property;
b) Participating in and providing security inputs to operational planning;
c) Cooperating closely on security matters with Security Focal Points of the organizations of the United Nations system;
d) Managing the security unit to include personnel, finance, budget and logistics.
e) Cooperating closely on security matters with all other officers of the United Nations system at the duty station to ensure the best possible security management;
f) Assisting security operations conducted by agencies as requested;
g) Establishing and chairing a security coordination cell for duty stations where there are also Single-agency Security Officers, in order to ensure that all security officers at the duty station are working together to further security management;
h) Ensuring an appropriate record of meetings undertaken by the security coordination cell is undertaken.
i) Developing good contacts with national security agencies, with a view to obtaining the best possible protection for personnel employed by the organizations of the United Nations system and their recognized dependants, and their property;
j) Serving as a member of the Security Management Team at the country level;
k) Undertaking security risk assessments for all locations in the country where personnel of the organizations of the United Nations system and their recognized dependants are present and facilitating the implementation of recommended mitigating measures;
l) Preparing, maintaining and updating the country-specific security plan, contingency plans and security listings of personnel employed by the organizations of the United Nations system and their recognized dependants;
m) Ensuring that plans for relocation/evacuation to a safe area are current, feasible and implementable;
n) Ensuring that an effective and functioning security and emergency communications system is in place;
o) Ensuring that all personnel employed by the organizations of the United Nations system and their recognized dependants receive briefings upon initial arrival, local security training as necessitated by changes in the security environment, and are kept informed of matters affecting their security;
p) Maintaining up-to-date instructions for personnel employed by the organizations of the United Nations system and their eligible dependents on precautions they should take in relation to the implementation of the security plan, including comprehensive listing of emergency supplies they should have on hand and guidance on their behaviour during a variety of emergencies, including natural disasters and political crises;

[3] The term 'Chief Security Advisor' will apply to the senior security professional within a Designated Official's area of responsibility. This term replaces previous titles such as Chief Security Officer, Chief of Safety and Security Services, Field Security Coordination Officer and Regional Security Coordination Officer, as appropriate.

q) Reporting all cases in which personnel employed by the organizations of the United Nations system and/or their recognized dependants have been victims of crime and submitting required reports on such cases;
r) Conducting security surveys of residential areas and premises;
s) Ensuring that the appropriate level of confidentiality is maintained with regard to security matters;
t) Advising the Designated Official and the Security Management Team on operational security requirements consistent with the minimum operating security standards; and
u) Reporting to the Designated Official all instances of failure or non-compliance with security policies, practices and procedures.

J. Country Security Focal Point (if applicable)

The Country Security Focal Point is responsible for:

a) Managing the day-to-day security related matters;
b) Ensuring that lists of personnel and their recognized dependants are up to date.
c) Preparing, maintaining and updating the country-specific security plan
d) Ensuring that all mandatory reports are provided in a timely manner to DSS;
e) Immediately reporting all security related incidents involving UN staff and their recognized dependants to the Designated Official and DSS;
f) Assisting the Designated Official and Security Management Team in the development and implementation of MOSS and MORSS;
g) Serving as a member of the Security Management Team;
h) Conducting residential security surveys for UN internationally-recruited staff.

K. Other Personnel of the Department of Safety and Security Personnel

Chief of Security and Safety Services/Sections

The Chief of Security and Safety Service/Section is responsible for:

a) Providing for the security and safety of delegates, staff, visiting dignitaries and other visitors within a United Nations complex at Headquarters and Offices away from Headquarters;
b) Assisting the Chief Security Adviser and participating in the work of the security cell for the development of security policies and procedures;
c) Providing strategic and executive direction on managing and optimizing its resources, determining priorities and allocation of resources to carry out the security and safety programme;
d) Providing strategic and executive direction on executing, monitoring and maintaining safety and security standard operation procedures and systems, emergency preparedness and crisis management, as well as conducting threat and risk assessments;
e) Providing strategic and executive direction on human resources, finance, budget and logistical matters for his/her Service/Section;
f) Providing strategic and executive direction on standardized and specialized training for staff and security personnel;

g) Providing the ultimate responsibility for personal protection of United Nations senior officials and dignitaries present and/or visiting his/her area of responsibility as and when needed;
h) Providing strategic and executive direction on the implementation of relevant minimum operational security standards;
i) Coordinating and liaising with local authorities and local law enforcement agencies;
j) Cooperating closely on security and safety matters with all other offices of the United Nations system at the duty station to ensure the best possible security management; and
k) Retaining day-to-day operational responsibility and reporting to their respective Directors-General or Executive Secretaries, who will serve as designated officials, working in close cooperation with their Chiefs of Administration, if located at an Office away from Headquarters[4].

Chief Security Officer for Peacekeeping Missions

The Chief Security Officer is responsible for:

a) Heading the security section and serving as the mission Security Adviser to the Head of Mission on all security-related matters;
b) Assisting the Chief Security Adviser and participating in the work of the security cell for the development of security policies and procedures;
c) Contributing to threat and risk assessments for all locations in the mission area where personnel are present and actively participating in the planning, evaluation of effectiveness of the country security plans and other aspects of security operations;
d) Reviewing and monitoring activities related to the mission Security Programme and mission security plans. Identifying air and land evacuation requirements to be used in emergencies;
e) Ensuring availability of emergency communications by making periodic checks to determine if the system is adapted and functioning properly;
f) Establishing a 24-hour emergency response system;
g) Maintaining continuing awareness of prevailing local security conditions, identifying probable threats and advising mission and project personnel to follow appropriate preventative steps;
h) Arranging protection detail for senior personnel or visiting VIP's as necessary;
i) Compiling and maintaining an updated staff list that includes all mission personnel, including visiting missions and consultants;
j) Monitoring and evaluating office physical security measures, and conducting security surveys of installations and facilities;
k) Determining the need for, and providing training and advice to mission personnel on residential security measures;
l) Establishing procedures for and conducting investigations on all deaths and all accidents and incidents in which mission personnel have been victims of crime, and following up on all arrests of mission personnel; and
m) Assuming responsibility for guard force management and issuance of identity cards.

[4] The Chief of the Security and Safety Service, United Nations Headquarters in New York reports to the Director, Division of Security and Safety Services, Department of Safety and Security.

Field Security Officers

The Field Security Officer is responsible and accountable to the Chief Security Adviser/Security Adviser for the following:

a) Implementing all aspects of security management, crisis readiness and preparedness at the duty station;
b) Preparing, maintaining and updating country-specific security plans, contingency plans and security listings of personnel employed by organizations of the United Nations system and their recognized dependants;
c) Undertaking threat and risk assessments for all locations in the country where personnel employed by organizations of the United Nations system and their recognized dependants are present;
d) Developing good contacts with national law enforcement agencies, with a view to obtaining the best possible protection for personnel employed by the organizations of the United Nations system and their recognized dependants; and
e) Conducting security surveys of residential areas and premises.

L. Single-agency Security Officers

The Single-agency Security Officer, in addition to agency-specific responsibilities, is responsible for:

a) Advising and assisting the agency country representative, situation or operations manager, on his/her security responsibilities, including participation in operational planning, and providing security inputs, as well as compliance with United Nations security policies, practices and procedures;
b) Advising and assisting the area security coordinator or Designated Official in the discharge of his/her responsibilities, when requested to do so;
c) Participating as a member of the security cell established by the Chief Security Advisor;
d) Advising the security cell on particular concerns of his/her organization regarding security;
e) Acting as the Chief Security Advisor ad interim, during the absence of the Chief Security Advisor for a given duty station, as appropriate and when required.

M. Wardens

The Warden is responsible for:

a) Functioning as a channel of communication between the Designated Official and personnel employed by the organizations of the United Nations system and their recognized dependants in his/her zone;
b) Ensuring that such personnel are regularly informed with regard to security arrangements and the emergency phases in effect;
c) Ensuring that one person is designated to maintain contact with United Nations system visitors residing temporarily at residences or hotels within the warden’s zone;
d) Carrying out other security-related duties as assigned by the Designated Official or the Chief Security Advisor;

e) Ensuring that recognized dependants left in the duty station by internationally-recruited staff who are serving elsewhere, are accorded the same provision for security as dependants of international staff serving at the duty station; and
f) Visiting every family living in their area to ensure that they are aware of the security arrangements.

N. Personnel employed by the organizations of the United Nations system

The personnel employed by the organizations of the United Nations system are responsible for:

a) Familiarizing themselves with information provided to them regarding the United Nations security management system at their location;
b) Receiving security clearance prior to travelling;
c) Attending security briefings and signing a document certifying that they have been briefed;
d) Knowing who their Warden and Chief Security Advisor or Country Security Focal Point is;
e) Being appropriately equipped for service at all duty stations;
f) Applying and complying with all United Nations system security regulations and procedures at the duty station, whether on or off duty;
g) Comporting themselves in a manner which will not endanger their safety and security or that of others;
h) Reporting all security incidents in a timely manner; and
i) Attending and completing security training relevant to their level and role; and
j) Completing the Basic Security in the Field CD-ROM.

ANNEX D

Security and Risk Management: A Guide for UN Managers

Introduction

The terms *risk* and *risk management* have evolved into more common use in the UN, often in the context of security, business continuity, emergency preparedness, and audit. Despite their increased use, the terms are not clearly or commonly understood. This paper sets out to explain *what* risk management means, *why* it is important to UN managers, and *how* to use a simple but structured decision-making model to help us better achieve our goals. This paper aims to help you better understand and use risk management tools in the UN, including the *Security Risk Assessment* (SRA) and *Security Risk Management* (SRM) processes.

What is Risk Management?

Any UN objective, from global strategic goals to local program plans, may fail because of various obstacles. In the security context, obstacles are called *threats*. Think of threats as "disenablers." All managers must identify threats and evaluate how these threats may affect their objectives. In many of the places where we work, the effect of threats, if not managed, can be fatal.

An organization's vulnerability to threats is called "risk." The process whereby a manager identifies and systematically deals with obstacles to success is called risk management. Risk management is the systematic selection of cost-effective approaches for minimizing the effect of threat realization to the organization. Risk management *enables* success by managing "*disenablers*".

*Risk Management is the **systematic** selection of **cost-effective** approaches for **minimizing the effect** of threat realization to the organization.*

Why is it Important?

Risk management is an essential management tool. It is key to achieving the best possible results in complex and dangerous environments. It increases our chances of success by decreasing the effect of threats. Risk management offers a structured approach to help make good decisions and allows for clear accountability. Proper risk management allows managers to maximize opportunities. Risk management is "good for business."

*Risk Management is key to achieving the **best possible results** in complex and dangerous environments.*

A Simple and Structured Approach

The risk-management process is a structured, problem-solving mechanism. It is a six-step process:

Step 1:	**Goals**	*(What are my program priorities?)*
Step 2:	**Threat** Identification & Assessment	*(What are the obstacles to achieving goals?)*
Step 3:	**Risk** Assessment & Prioritization	*(How will they affect us and which require the most attention?)*
Step 4:	Risk Management **Decisions**	*(What can we actually do about it?)*
Step 5:	**Implementation** & Review	
Step 6:	Goals are **achieved**!	

The following explains this process in more detail:

Step 1: Goals

Managers set goals and they manage people, resources and risk in order to achieve those goals. Managers also establish priorities among these goals.

Step 2: Threat Identification & Assessment

Threat identification is a process whereby you decide what you are up against. In the security context, a manager should sit down with security and other advisors to list people and events that may block success (i.e., threats). The next step is to assess the threats. In the UN security context, a professional security officer is the key player in the threat assessment process to guarantee that senior managers get the best information for their decisions. When human beings are the potential cause of harm, the threat they pose can be assessment by looking at three components:

1. **Mind-Set** (mental orientation toward harming the target)
2. **Capability** (to harm the target)
3. **Context** (that permits the harm to happen)

Having carried out the threat assessment, the next step is to carry out a risk assessment. Not all threats carry the same risk to the UN's staff, assets and programmes.

Step 3: Risk Assessment & Prioritization

Human beings make subjective risk evaluations daily, but research shows that these evaluations are often inaccurate. The most common error is the "optimistic bias", whereby people believe that they will not be the victim of an undesirable incident because it has never happened to them before. Most people find it impossible to imagine themselves as the victim of a dangerous event and say "it can't happen to me." A common error among humanitarian workers is "danger habituation." As the

*Most people find it impossible to imagine themselves as the victim of a dangerous event and say "**it can't happen to me**."*

dangers increase, people get used to them, become complacent and neglect to take the necessary security precautions. These errors can lead to programme cancellation, or worse, the death or serious injury of staff.

Here's an example of the dangers of subjective risk evaluations. In the US in 2005, there were more than 6 million vehicles accidents that injured 2.9 million people and killed more than 43,000. Of those who died, more than half were not wearing seatbelts. It is a safe assumption that none of those who died thought that they were acting irresponsibly or that they were going to die.

To avoid the problems that come with subjective risk evaluations, you need to assess risk in a structured way. To do so, you must first understand that risk is a product of:

1. The **Likelihood** of being affected by a threat, and

2. The **Impact** that such an event would have on the organization (impact is evaluated in both financial and other types of costs like human resources, lost productivity, public image, loss of life, etc.).

Risk = Likelihood x Impact

The easiest way to assess likelihood and impact is to evaluate a potential threat on a five-point scale for each category. Combining the two scales on the matrix below gives the risk.

Risk Matrix

		Impact				
		Negligible	Minor	Moderate	Severe	Critical
Likelihood		1	2	3	4	5
Very Unlikely	1	Negligible (1)	Low (2)	Low (3)	Low (4)	Low (5)
Unlikely	2	Low (2)	Low (4)	Medium (6)	Medium (8)	Medium (10)
Moderately Likely	3	Low (3)	Medium (6)	Medium (9)	High (12)	High (15)
Likely	4	Low (4)	Medium (8)	High (12)	High (16)	Critical (20)
Very Likely /Imminent	5	Low (5)	Medium (10)	High (12)	Critical (20)	Critical (25)

Two examples help illustrate how to undertake a risk assessment using this matrix. **Example 1**: Based on a threat assessment, you assess that the likelihood of staff members stealing office supplies as "very likely". You also note that, if this occurs, the impact would be "not serious." Therefore, the risk is "low." **Example 2**: If you assess that it would be "moderately likely" that a certain group would bomb your building, but that the impact would be "Critical," then the risk from a bomb is "High."

The higher the risk, the more attention we must pay to lowering that risk. Managers must prioritize critical and high risks and then work downwards. Low risks that nonetheless have critical impacts must not, however, be forgotten.

Various aspects of the threat assessment will influence your judgment about both the likelihood and impact of a certain threat. To illustrate, we can use an example about armed crime. If the threat assessment identifies a threat from large, well-armed criminal groups working in a city with poor lighting at night and a weak police force, then the likelihood of a successful attack will be high. If a criminal group is known to use automatic weapons during armed robberies, then the potential impact would be loss of life, so the risk associated with this group would be greater than if they did not have such weapons.

As well, your present vulnerability to an attack also affects the risk assessment. The risk associated with an attack by even a small, unarmed criminal group will be higher if the target is not properly protected. A lack of ability to control the after-effects of a serious incident is also a form of vulnerability and needs to be examined. The risk of someone dying after being shot in an armed robbery, for example, will increase if proper medical attention is not given to the victim.

*A lack of ability to **control** the **after-effects** of a serious incident is also a form of vulnerability and **needs to be examined**.*

Once you have identified all the major threats and established their corresponding risks, you are ready to make sound decisions on how to lower risks.

Step 4: Risk Management Decisions

Risk management is the process where by an organization attempts to lower risk by influencing likelihood and/or impact. Because we have little influence over the cause of a threat, it is best to concentrate on lowering risk.

There are 4 main strategies for managing risk (**ACAT**):

1. **A**ccept the risk (no further action)
2. **C**ontrol the risk (using prevention and/or mitigation measures, e.g. MOSS)
3. **A**void the risk (temporarily distance the target from the threat)
4. **T**ransfer the risk (insurance, sub-contract, etc.)

The risk management strategy you choose will depend on the level of risk. Below are some suggested risk management strategies you may consider based on the level of risk:

		Impact				
		Negligible	Minor	Moderate	Severe	Critical
Likelihood		1	2	3	4	5
Very Unlikely	1	Accept	Transfer & Accept	Transfer	Transfer	Transfer & Control
Unlikely	2	Control & Accept	Control & Transfer	Transfer & Control	Transfer & Control	Transfer & Control
Moderately Likely	3	Control	Control & Transfer	Control & Transfer	Control & Avoid	Avoid & Control
Likely	4	Control	Control & Transfer	Control & Avoid	Control & Avoid	Avoid & Control
Very Likely /Immanent	5	Control	Control & Transfer	Control & Avoid	Control & Avoid	Avoid

Senior management must decide what level of risk is acceptable depending on the relative importance of a program goal. Unacceptably high risks must be avoided or brought within acceptable levels with risk-management strategies.

The risk strategy for highly-likely events is to try to lower their likelihood. Security measures and procedures lower the likelihood of a successful attack on your organization. A professional security officer can provide advice on security strategies.

The strategy for high impact events is to attempt to lower the impact. Contingency planning, communication and response strategies (police/medical) lower the impact once an event has occurred.

Ideally, you should try strategies that will lower both likelihood and impact. You are encouraged to be creative in the ways you can lower likelihood and impact. The best risk management strategies available in the UN to lower both likelihood and impact of security threats are *Minimum Operating Security Standards* (MOSS).

Step 5: Implementation & Review

Once the risk-management decisions are made, you must then implement the risk-management strategy and then continually monitor the threat and risk environments to ensure that your strategy is providing best protection in the most effective and efficient way. Once again, the objective is to achieve our goals.

Conclusion

For managers to achieve their goals, they must approach risk in a structured way. The risk-management approach laid out in this paper is the easiest and most effective way of managing risk. The UN would be seriously inhibiting its ability to achieve it humanitarian objectives if it did not effectively manage the risks to its staff and asset. Safe staff and assets are keys to achieving goals.

Because risk-management decisions include concerns of cost and benefit, as a manager, you are best placed to evaluate such issues. Although managers may worry about the costs of risk management, it is also important to consider the costs of not managing risks. Not managing risk can be unacceptably expensive because undesirable events have more than just a primary impact on the organization. Risk events will always have secondary and tertiary costs. Therefore, risk management saves money by lowering loss.

*Undesirable events have **more than just the primary impact** on the organization. Risk events will always have **secondary** and **tertiary** costs.*

We hope that this guide will help you undertake the difficult task of identifying and managing the risks you face, especially security risks.

Prepared by: **Paul J. Farrell**, UNICEF Deputy Security Coordinator.
To discuss Security and Risk Management in more detail or in relation to your specific context, please contact the UNICEF Security Team the Office of Emergency Programmes (EMOPS).