United Nations
Department of Peacekeeping Operations
Department of Field Support

Ref. 2010.29

Policy

SECURITY RISK MANAGEMENT PROCESS

Approved by: Alain Le Roy, USG/DPKO and Susana Malcorra, USG/DFS
Effective date: 1 November 2010
Contact: OUSG/Focal Point For Security
Review date: 1 November 2012

DPKO/DFS POLICY ON THE SECURITY RISK MANAGEMENT PROCESS

Contents:

ANNEXURES:

A. PURPOSE

1. This policy establishes the Security Risk Management (SRM) process as the methodology for security threat and risk assessment and the management of security risk in DPKO field missions. The intent of this policy is to extend the SRM process used in the UN Security Management System to include mission military and police components.

2. SRM is a Chief Executives' Board-approved analytical procedure that assists in assessing the operational context of the UN; identifies existing and potential security threats; identifies the risk level of undesirable events that may affect UN personnel, assets and operations; and provides guidance on the implementation of cost-effective solutions in the form of specific prevention and mitigation strategies and measures with the aim of lowering the risk levels for the UN by reducing the likelihood and impact of an undesirable event.[1]

B. SCOPE

3. This policy applies to all DPKO-directed missions. The policy is also applicable to any DFS-directed support centre where formed military and/or police units are located.

C. RATIONALE

[1] Political, economic, social and other factors influence security threats. Analyses of these factors and their relation to mission mandates are normally conducted by a mission's Joint Mission Analysis Centre (JMAC) or, where JMACs are not present by other analytical capacities. These 'strategic studies' provide short, medium and long term forecasts within which the Security Risk Management process occurs and Security Risk Assessments are produced.

4. Multiple, dissimilar security threat and risk methodologies employed by field mission civilian, military and police components or a lack of effective methodology may result in uncoordinated, incomplete and competing assessments of security threats and risks and may hamper senior mission leader decision-making on required risk management measures and their implementation. This circumstance can also result in the lack of a common view of security threats and risks between the mission and headquarters. In particular, a shared view of security threats and risks between a mission and headquarters is vital to support effective dialogue with troop and police contributing countries.

5. Adoption of the SRM process harmonizes security threat and risk assessment among mission components and provides a complete mission depiction of its security threats and risks with a common Security Risk Assessment format. The single format provides information on each step of the Security Risk Assessment process and, if required, on required risk management measures. The use of the SRM enhances understanding of the security environment and associated security threats and risks both in the mission and at headquarters. This, in turn, supports decision-making on required risk management measures and facilitates the mobilization of necessary resources.

6. As a precursor to defining the specific security threats and associated risks throughout the SRA process, generic threats can be identified using the Structured Threat Assessment of the Security Level System (Annex C). The Structured Threat Assessment in the Security Level System can be used as a foundation for DPKO threat updates to meetings of Troop and Police Contributing Countries while ensuring coherence in view between headquarters and the field mission.

D. PROCEDURES

D.1 SRM Process, SRA Format and the Security Level System.

7. The SRM process is found at Annex A. The Chief Executives Board approved the SRM process on 4 April 2009. The SRM is presented in its original approved text. In blue comments along each page's right side margin are DPKO comments that extend the SRM to encompass military and police components.[2] Joint Mission Analysis Centres (JMACs), by separate policy, are already tasked to input to mission threat assessments. Missions will develop internal coordination modalities to implement the SRM process to encompass inputs from civilian security, JMAC, military and police components and other mission offices, as required. Coordination modalities will not replace any aspect of the UN Security Management System, including the Security Management Team. The approved Framework for Accountability also remains unaltered.

8. The format template for the Security Risk Assessment is found at Annex B. Missions will prepare their Security Risk Assessment in three parts

[2] Annexes should be read taking into consideration that not every term has been redefined for military and police purposes, but that the existing processes of the Annexes should be understood not in terms of the exact wording of the Annexes but rather in terms of the intent of this policy.

using the format for each part: Part A will address organizations and personnel who are under the UN Security Management System including the Minimum Operating Security Standards as specified in the original text of the SRM process found in Annex A to this policy; Part B will address the military component where formed units are present and related personnel and activities; and Part C will address the police component where formed units are present and related personnel and activities.

9. The Security Level System Guide is at Annex C. As a precursor to the SRA, this will be used by the mission to determine the Security Level with input and coordination from civilian security, military and police components, JMAC and others, as needed.[3]

D.2 Approval Authorities

10. Part A (UNSMS) of the Mission SRA will follow the SMT consultation; DO approval and DSS endorsement procedure specified in the original SRM.[4] In missions where the Director/Chief of Mission Support is not an SMT member, he/she will be consulted on security risk management resource requirements.

11. Parts B (Military) and C (Police) of the Mission SRA will be discussed within the mission Senior Management, approved by the respective Heads of military (Part B) and police components (Part C) and final approved by the Head of Mission.

D.3 Information Flow Relevant to the Mission SRA

12. The Mission SRA (Parts A, B and C), as a single document in three parts, will be communicated to the relevant DPKO Integrated Operational Team (IOT) at headquarters and to the DSS Peacekeeping Operations Support Section (POSS) or relevant DSS Regional Desk where that Desk has responsibility for the DPKO-directed mission or DFS-directed support centre.

13. DPKO IOTs will establish a SRA Review Group comprising members of the IOT, DFS, the Office of Military Affairs and Police Division and supported by DSS POSS or the relevant DSS Regional Desk to review the SRA, understand its risk and risk mitigation implications, seek clarifications from and input any concerns to the mission submitting the SRA, assess the resource implications of risk mitigation measures and support the out-of-mission area processes for obtaining risk management resources, in particular during budget development and approval processes.

14. Due to its sensitivity, in particular as regards security vulnerabilities, persons handling SRA materials need to be cognizant of information

[3] This policy does not add new responsibilities to the mission Chief Security Adviser/Chief Security Officer/Security Adviser regarding security of military and police components.

[4] In those missions where the Head of Mission is not a Designated Official for security but is an SMT member, Part A will also be part of a larger UN SRA for a country or area.

security both in the mission and at headquarters.[5] The transmission media for communication of the SRA will be via Groove to the relevant IOT, OMA Assessment Team, Police Division and DSS POSS or relevant Regional Desk. If deemed necessary by the mission, locked PDF format may be used.

D.4 Use of the SRA in Intergovernmental Groups, TCC and PCC Meetings

15. The Structured Threat Assessment in the Security Level System should be used as the foundation for security threat presentations to Intergovernmental Groups (e.g. Special Committee on Peacekeeping) and TCC/PCC meetings.

16. The SRA depicts risk management measures. These measures may be used to inform TCC/PCCs in order to better prepare their military or police units.

17. The Mission SRA will not be released outside the UN without the approval of the USGs of DPKO, DSS and, in the case of DFS-directed support centres the USG DFS.

E. TERMS AND DEFINITIONS

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

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

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

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

22. *Structured Threat Assessment:* A methodology that complements and strengthens the SRA process by improving the situational threat analysis step. The Structured Threat Assessment consists of five general threat categories of which each is assessed using three standard component parts of any threat – Intent, Capability and Inhibiting Context. Evaluating

[5] Reference ST/SGB/2007/6, paragraphs: 1.2 (b) and (c); and sections 2 - 5.

these five categories of threat in the STA methodology allows the determination of a Security Level.

F. REFERENCES

23. **Related Guidance Materials**

- CEB/2009/1, 5 May 2009.
- CEB/2009/HLCM/INF.1, 9 April 2009, United Nations System Staff Security and Safety.
- Inter-Organizational Security Measures: Framework for Accountability for the United Nations Security Management System.
- ST/SGB/2007/6, Information sensitivity, classification and handling, 12 February 2007.
- DPKO/DFS Policy, Joint Operations Centres (JOC), 1 February 2010.
- DPKO/DFS Policy, Joint Analysis Centres (JMAC), 1 February 2010.
- DPKO/DFS Policy, Applicability of the Arrangements of the United Nations Security Management System to Individually Deployed Military and Police Personnel in DPKO- or DPA-led Missions, 1 May 2008.

G. CONTACT

24. The contact officer for this policy is the DPKO-DFS Focal Point for Security, William Phillips, Building DC-1, 9th Floor, Room 0944, Telephone: +1 917 367 5237, Fax: 1 212 963 9053, e-mail: phillipsw@un.org.

H. HISTORY

25. This policy is based upon the DSS issued-memorandum, subject: Entry into effect of new policies on Security Risk Management (SRM) and Minimum Operating Security Standards (MOSS), and Guidelines for Determining Acceptable Risk signed on 20 April 2009 with associated annexes.

SIGNED: A- L ~~

DATE: 7 October 2010

SIGNED:

DATE: 07/10/10

Annex A

The following exact text is the original document approved by the Chief Executives Board on 4 April 2009. The right side margin boxed text, linked by superscript, provide notes applicable to the extension of the SRM process to mission military and police components. The Policy for United Nations Minimum Operating Security Standards does not apply to formed units of the military and police components.

POLICY AND CONCEPTUAL OVERVIEW OF THE SECURITY RISK MANAGEMENT PROCESS

Introduction

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

2. The UNSMS Security Risk Management model is the managerial tool of the UN for the analysis of safety and security threats that may affect its personnel, assets and operations.[1]

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

4. Overall responsibility for the safety and security of UN staff rests with the Host Government; however, accountability also rests with managers at all levels, and not with their security advisers. Security advisers must provide the technical security inputs and advice which allow UN managers to make informed decisions for managing security risks. Security Risk Management therefore requires good teamwork between those who plan and direct UN operations and those who advise on the security measures which enable them.[2]

Key terminology

5. The definition of *Security Risk Management* is:

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

[1] The SRM was originally designed for the UNSMS (Security Management System). With the issue of this policy, the applicability of the SRM will expand to include military and police components.

[2] Heads of military and police components in peacekeeping missions are mandatory members of the mission/country Security Management Team. Within their military and police competencies, Heads of military and police components will provide military and police-based security inputs and advice. As leaders, Heads of military and police components are accountable to the Head of Mission for the safety and security of their respective components.

the risk levels for the UN by reducing the impact and likelihood of an undesirable event.

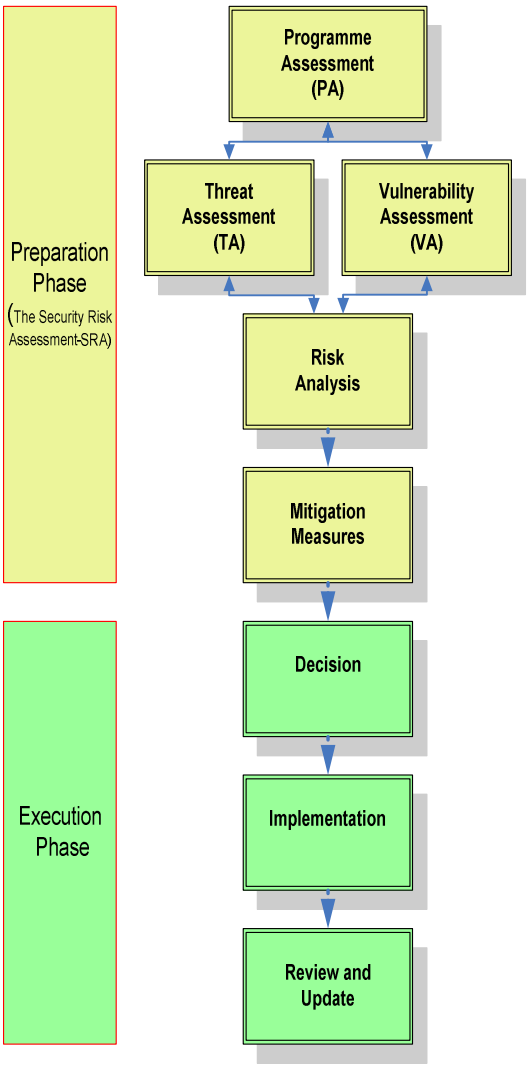
6. The definition of *Security Risk Assessment* is:

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

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

> Threat: Any factors (actions, circumstances or events) which have the potential or possibility to cause harm, loss or damage to the United Nations system, including its personnel, assets and operations.
>
> Risk: The combination of the *impact* and *likelihood* for harm, loss or damage to the United Nations system from the exposure to threats. Risks are categorized in levels from Very Low to Very High for their prioritization.

The Security Risk Management Model:



The model is organized in two distinctive phases:

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

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

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

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

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

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

The **Execution** Phase includes:

Decision, the DO and SMT will select and approve the risk management measures to reduce the current risk levels associated to each threat to the UN. An Implementation Plan is also decided and approved.[3]

Implementation of the selected risk management measures. Often overlooked, this step is a critical element of the SRM process. The DO and the SMT members must ensure that the risk management measures are budgeted and implemented in accordance with the plan. Accountability does not end with the analyses; it ends with full implementation of the required measures.[4]

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

[3] Decision While the Heads of military and police components are members of the SMT and participate in SMT discussions, the Head of Mission and the Heads of military and police components will select and approve risk management measures applicable to military and police components.

[4] Implementation The Head of Mission must ensure that risk management measures applicable to military and police components are budgeted. The Head of Mission and the Heads of military and police components will ensure implementation of required measures. The Director/Chief of Mission Support will be consulted on all risk management resource requirements prior to approval of the SRA.

Programme Assessment

8. The Programme Assessment is essential to the SRA, and it is a distinct and separate part of the process, which is a fundamental part of the Country/Area Operations Planning process. The Programme Assessment must be developed as a collaborative effort between the responsible officers of the AFPs and organizations (usually the programme officers) who will conduct the programmes and security advisers (including agency security officers where present) in order to ensure "mainstreaming" of security at the earliest stage of Country/Area Programme Operations Planning. It is critical that security officers are consulted early in all programme development to ensure that security is included to avoid delays when programmes are implemented.[5]

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

[5] Military and police mission and task analysis based upon the mission mandate constitute their parts of the 'Programme Assessment' of the SRA.

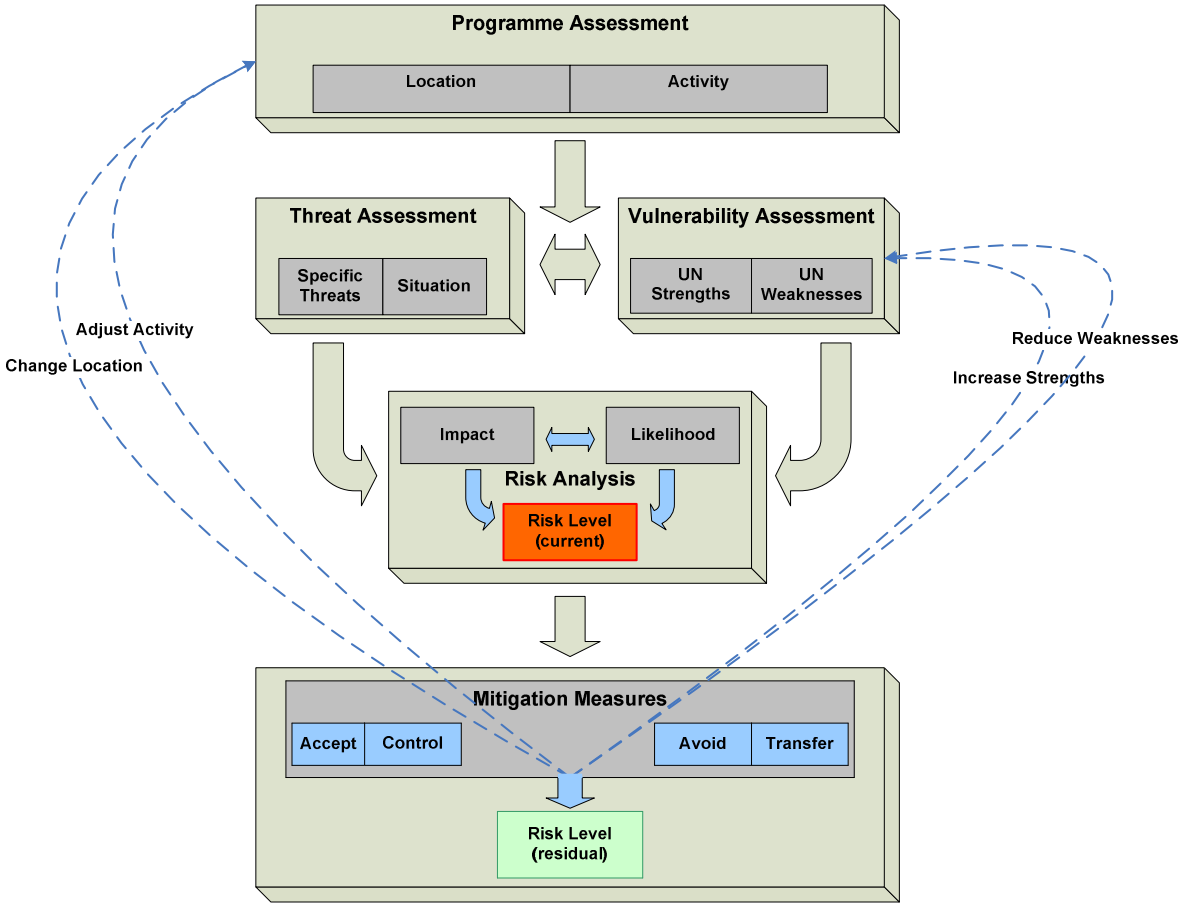
likely to affect the UN or may even be irrelevant to UN operations. A comprehensive picture of programme activities should be constructed to allow integration with security information.

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

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

The Security Risk Assessment (SRA)

11. The functioning of the SRA within the overall SRM process is illustrated in the diagram below:



12. A credible SRA is an essential pre-requisite to the effective management of risk; the objective of an SRA is to identify and assess the nature of the risks to a UN operation or activity so that those risks can be effectively *managed* through the application of mitigating measures.

13. The main risk management measures are prevention (lowering likelihood) and mitigation (lowering impact). Risk management strategies can also be categorized as follows:

    a. Accept. The unmitigated risk is accepted without the need for any further mitigating measures.

    b. Control. Implement prevention and/or mitigation measures to reduce the risk to an acceptable level.

    c. Avoid. Temporarily distance the potential target (e.g. UN staff, vehicles etc) from the risk.

    d. Transfer. Insurance, or sub-contracting implementation to other parties who can operate safely.

Frequency of Completing and Updating Security Risk Assessments

14. The Security Risk Assessment is a tool which is a living document and must be under constant review by the CSA, DO and SMT.[6] In particular, a validation should be carried out at each SMT meeting when there is a change or development in the "UN Security Situation" (the PA, TA or VA) which could affect UN operations or activities, for example:

    a. There is a change in the political situation or an upcoming event of political significance (e.g. an election) that may impact on UN security.

    b. There is a change in operations (i.e. new role for the UN or elements of the UN in country or region).

    c. Or when planning for:
        i. A new mission to be deployed.
        ii. The consideration and selection of new offices or facilities.
        iii. An expansion of programmes into new areas of a country.
        iv. Operations resuming after a programme suspension, relocation or evacuation for security reasons.
        v. Special events or conferences.
        vi. New spending on security measures.

15. Validating the SRA must be a standing item on the agenda of every SMT meeting. If new information is reported that changes the SRA, it should be noted in the SMT minutes and the SRA matrix updated to contain the relevant changes, conclusions and new recommendations which were decided in the SMT.[7]

[6] Parts of the SRA applicable to the military and police components must be under constant review by the Heads of those components and the Head of Mission.

[7] The SRA applicable to the military and police components is validated by the Heads of those components and the Head of Mission.

Security Risk Analysis Table

16. The UN Security Management System has established the following table for the evaluation of "Risks Levels"

Risk Analysis / Likelihood	Impact: Negligible	Minor	Moderate	Severe	Critical
Very likely	Low	Medium	High	Very High	Unacceptable
Likely	Low	Medium	High	High	Very High
Moderately Likely	Very Low	Low	Medium	High	High
Unlikely	Very Low	Low	Low	Medium	Medium
Very Unlikely	Very Low	Very Low	Very Low	Low	Low

17. To support the Risk Analysis process and the identification of Risk levels for each threat, indicators have been developed as per the following guide;

Risk Acceptability

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

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

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

a. **Identify programme / project goals**. In higher risk situations there will be a need to prioritize these goals. More important goals may dictate that the organization accept a higher level of risk to achieve results.
b. **Identify and assess the threats faced**. These are the obstacles that threaten the achievement of programme goals.
c. **Identify the risk** by looking at the likelihood and impact of the threats affecting the UN and each agency. Impact assessment is very important. Understanding how bad something could be is

essential to discussion of acceptable risk. In other words, how bad an event can we accept?

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

21. Over all, there is a need to answer a number of critical questions.
    a. "How important is the activity?"
    b. "Will the anticipated gains justify accepting a high level of risk?
    c. Has enough been done to lower the risk to a level that is reasonable to expect staff to take?"
    d. "Do we think that the risks we have identified are manageable?"

22. If the answers to the above are “yes” then consideration should be given to implementing the programme. If the answers are "no" then alternative options should be considered to achieve the programme goals.

    Approval and Finalization of SRAs (including dispute resolution process)

23. The process for approval and finalization of the SRA is contained in the SRA guidance in the SOM, however, the salient steps are:

    a. CSA/SA submits draft SRA to DO/SMT, and copies to DRO Desk Officer informally.

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

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

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

    e. DRO Desk Chief officially endorses and returns the SRA to the DO.[8]

[8] The process described remains applicable for the SRA that is applicable to the UNSMS. For the military and police components’ portion of the SRA (Military and Police Annexes to the SRA), the Head of Mission and Heads of military and police components are the review and approval authorities. The approved SRA, including military and police annexes, will be provided to DSS and to the relevant DPKO/OO Integrated Operational Team. DSS will not endorse the military and police annexes.

Training

24. As agreed by the Secretary General, Chief Executive Board (CEB) and the UNSMS Network, training in the SRM methodology is mandatory for all DOs, SMT members and security professionals.[9]

25. All United Nations officials who have specific security responsibilities within the Framework for Accountability must be

[9] In addition to the listing of paragraph 24, SRM training is mandatory for all Heads of Mission, Heads of military and police components and military and police personnel contributing to the SRM process.

cognizant of the Security Risk Management model and the SRA process.

Guidelines for Determining Acceptable Risk

Background

1. Security risk management is an integral part of all UN activities. Agencies, funds, and programs must normally decide, according to their mandates and programmatic responsibilities, what program activities are necessary and appropriate. They must adapt their internal procedures for delegating responsibility, bearing in mind the Framework for Accountability. Country-level representatives are expected to reflect the priorities and interests of their respective organization in the SMT.[10]

[10] This paragraph applies to all components of a peacekeeping mission.

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

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

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

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

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

Acceptable Risk Decision: Programme Priority, Risk and Decision Makers

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

Risk Analysis Likelihood	Impact Negligible	Minor	Moderate	Severe	Critical
Very likely	Low	Medium	High	Very High	Unacceptable
Likely	Low	Medium	High	High	Very High
Moderately Likely	Very Low	Low	Medium	High	High
Unlikely	Very Low	Low	Low	Medium	Medium
Very Unlikely	Very Low	Very Low	Very Low	Low	Low

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

7. Whether risk is acceptable at any level lower than "unacceptable" (black) is a question of programme priority. The table below suggests definitions of Programme Criticality, level of program decision making, and the highest level of risk at which this program is acceptable.[11]

[11] [12] For military and police components, programme criticality is determined by the Heads of military and police components. Final decisions (on final risk acceptance) for low/very low/medium and high residual risk are made by the Head of Mission. For Very High risk, the USG DPKO is the final decision maker.

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

8. Combining the risk matrix (see color code) and the new categories for programme importance and decision-maker, we now have a clearer understanding of who makes the decision on acceptable risk. Each box with the matrix shows the minimum level of programme criticality that would be acceptable.[12]

Acceptable Risk Decisions

Acceptable Risk Decisions	***(Each box within the matrix shows the minimum level of program criticality that would be acceptable)***				
	(Colors represent risk levels in SRA table above as established by the Designated Official)				
Program Importance	All	Essential, Critical & Extreme	Critical & Extreme	Extreme	Unacceptable
Program Decision	Rep	Rep + HQ	HQ + Rep	Exec. Head	No UN Presence
Final Decision	DO	DO	DO	USG DSS	Secretary-General
Program Importance	All	Essential, Critical & Extreme	Critical & Extreme	Critical & Extreme	Extreme
Program Decision	Rep	Rep + HQ	HQ + Rep	HQ + Rep	Exec. Head
Final Decision	DO	DO	DO	DO	USG DSS
Program Importance	All	All	Essential, Critical & Extreme	Critical & Extreme	Critical & Extreme
Program Decision	Rep	Rep	Rep + HQ	HQ + Rep	HQ + Rep
Final Decision	DO	DO	DO	DO	DO
Program Importance	All	All	All	Essential, Critical & Extreme	Essential, Critical & Extreme
Program Decision	Rep	Rep	Rep	Rep + HQ	Rep + HQ
Final Decision	DO	DO	DO	DO	DO
Program Importance	All	All	All	All	All
Program Decision	Rep	Rep	Rep	Rep	Rep
Final Decision	DO	DO	DO	DO	DO

The following policy for UN Minimum Operating Security Standards does not apply to military and police components, excepting those individual military and police officers placed under the UN Security Management System by the Head of Mission.

POLICY FOR
UNITED NATIONS MINIMUM OPERATING SECURITY STANDARDS

Introduction

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

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

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

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

MOSS

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

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

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

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

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

Responsibilities and Standards

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

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

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

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

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

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

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

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

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

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

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

UNITED NATIONS MINIMUM OPERATING SECURITY STANDARDS (UN MOSS)

Country MOSS Tables must justify, through the rigorous application of the Security Risk Assessment (SRA) process, the inclusion or exclusion of each of the items listed below

While the intention is to maintain flexibility and management discretion, common-sense will dictate those measures (such as vehicle safety equipment and fire precautions) which should be mandatory in all locations regardless of the prevailing security situation

1. TELECOMMUNICATIONS

1.1. Emergency Communications System

a. Where the SRA indicates a need, establish an **Emergency Communications System (ECS)** throughout the country, and its operational locations, in order to:

(1). Provide communications between DO, SA, SMT, Wardens and UN medical personnel within in the Capital.

(2). Provide communications between ASC and DO/SA and UN medical personnel.

(3). Provide communications between the ASC and the Area SA, SMT within the Area.

(4) To enable communications between the DO/SMT/SA and relevant UN Offices outside the country (including DSS).

b. **Mobile satellite telephones** should be provided to all CCCs, DOs and CSA/SAs and Agency Security Officers as well as for other key managers as decided by the SMT.

c. The ECS is to be tested and practiced at regular intervals.

d. The ECS network should be capable of operating 24 hour/7 days per week (24/7) should need arise.

1.2. Radio Communications

a. When VHF/UHF communications are employed (in accordance with need identified in the SRA), a **Security channel** for DO, SA and SMT members, and where applicable ASC, ASMT members, UN medical personnel and wardens, must be incorporated into radio networks.

b. All UN vehicles are to be equipped with **VHF/UHF radios**. In addition, “Field Vehicles” (those which travel into the countryside or move between urban areas)

are to have **a second radio system, usually HF or an alternative communication system (e.g. satellite phone)**.

c. SOPs for regular radio checks at residences and while moving are to be established.

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

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

2. SECURITY INFORMATION AND STRUCTURE

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

a. Security Risk Assessment.

b. UN Field Security Handbook (FSH).

c. Security Operations Manual.

d. Country/Area-specific Security Plan.

e. Country/Area-specific MOSS.

f. Security Standard Operating Procedures.

g. Relevant country maps.

h. Country PEP Protocol.

2.2. **Warden Systems**

a. Established and operational.

b. Exercised regularly.

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

a. Established for all UN offices and facilities.

b. Exercised every six months (or more frequently if SRA so indicates)

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

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

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

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

3. MEDICAL

3.1. Response to Medical Emergencies

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

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

c. Each country is to have a **MASS CASUALTY PLAN** appropriate to the risks in country and the response capacity of the local emergency services.[13]

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

[13] In the context of this policy, the term 'country' means mission.

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

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

3.2. Medical Equipment

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

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

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

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

4. EQUIPMENT and SUPPLIES

4.1. **Emergency power supply** available for charging and operation of **common-systems** communications equipment, office external security lighting and other essential equipment. Adequate reserve stocks of fuel to be maintained.

4.2. **Emergency Food, Water, Medical, Sanitary and Shelter Supplies** (in non-perishable form) to be stocked in preparation for use in concentration points, bunkers and safe rooms, storm shelters as appropriate for the country and situation.

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

5. UNITED NATIONS VEHICLES

5.1. All UN Vehicles

a. Must be operated by properly licensed operators.

b. All UN vehicles appropriately registered with the Host Government and properly maintained.

c. All vehicles identified, where appropriate, with UN logos/flags/decals as determined by prevailing local conditions.

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

5.3. UN Vehicle Equipment

5.3.1. All vehicles (regardless of location)

a. First aid kit.
b. Fire extinguisher
c. Spare wheel, jack and appropriate tools.
d. Reflector triangles, battery-powered lantern, seat belts.

5.2.2. All Field Vehicles (according to country situation):

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

6. OFFICES, PREMISES AND FACILITIES PROTECTION

6.1. All UN Managed Buildings

a. All buildings occupied by UN to be compliant, where feasible, with international building, safety and fire regulations or the applicable laws of the host country as appropriate (including construction for resistance to earthquakes or other natural hazards, according to local conditions).

b. Appropriate access control measures based on size and location of premises.

c. Separate entrances for personnel and visitors, where feasible and appropriate, in compliance with established standards (if/where applicable).

d. Secured parking for authorized vehicles where appropriate.

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

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

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

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

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

c. Shatter Resistant Film on windows and frame catchers.

d. Bunkers/reinforced rooms.

e. Surveillance and access control systems.

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

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

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

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

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

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

(3). Adjusting work patterns to limit the exposure of UN personnel within the government premises.

7. SECURITY TRAINING AND BRIEFINGS

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

a. Country-specific security orientation briefing

b. Summary/Extract of Country Security Plan and Evacuation Plan

c. Relevant Country/Area-specific Security Plan, SOPs and policies.

d. Compliance with all UN security policies.

e. Copy of current MOSS and MORSS applicable to the duty station.

f. Briefing and written handout on medical arrangements available in country and how to access them or call for emergency medical assistance.

g. A copy of the Country PEP Protocol, which should specify PEP custodian arrangements, location of PEP kits, and procedure for obtaining assistance in the event of possible exposure to HIV/AIDS .

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

7.3. **Training:**

a. All UN personnel to complete Basic Security for UN Personnel (BSUNP) and /or Advanced Security In The Field (ASITF) online or by CD-ROM, as required for the duty station,.

b. All personnel to receive cultural sensitivity briefings appropriate to country before or on arrival.

8. RESIDENTIAL SECURITY MEASURES

a. Minimum Operating Residential Security Standards (MORSS) will continue to be approved as a separate country table, in accordance with MORSS procedures as updated from time to time.

b. MORSS must take account of the relevant conclusions of the SRA with respect to the local law and order situation.

9. ADDITIONAL MEASURES:

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

a. **Personal Protective Equipment** (helmets, body armour etc) to be stocked adequate for all personnel needs as indicated by the Security Risk Assessment, and SOPs establishing conditions for issue, carriage in vehicles and mandatory wearing.

b. **Armoured Vehicles.** In addition to providing a means of evacuating personnel under fire in extremis, armoured vehicles are an option where access is needed to areas which are marginally under the "acceptable risk" threshold, and where there is potential for resumption of conflict or fluidity of nearby conflict areas.

EXAMPLE COUNTRY MOSS TABLE FORMAT (for ILLUSTRATIVE PURPOSES/SUGGESTION ONLY)

United Nations Minimum Operating Security Standards

[COUNTRY NAME]

[Date]

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

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

United Nations Minimum Operating Security Standards – [Country]

2. SECURITY INFORMATION AND STRUCTURE				
No.	**Item**	**Standard Requirement**	**Country Specific Requirements, Equipment & Procedures**	**Remarks**
2.1	Documentation	a. Country/Area-specific Security Risk Assessment b. UN Field Security Handbook (FSH) c. Security Operations Manual d. Country/Area-specific Security Plan e. Country MOSS f. Security Standard Operating Procedures g. Relevant country maps h. Country PEP Protocol i. Security SOP booklet	As per standard requirement to be available at the DO's office, agency offices, and each duty station, in addition: j. Mine area maps (provided by UNMAS); k. Maps/lists displaying permissible/non-permissible roads/areas; l. Maps displaying areas where armoured or vehicles with ballistic blankets fitted have to be used; m. Cell phone coverage map (maintained by FAO)	Requirements are mandatory
2.2	Warden System	Warden system for national and international staff established and functional in all duty stations. Note: zone warden systems to be implemented in case international staff is authorized to reside in private residences.	a. Warden system for international staff to ensure emergency response coordination and staff concentration among UN (and NGO) compounds in a duty station - established and operational in all duty stations where more than one office and/or approved staff accommodation are located; b. Agency based warden system for national staff; c. Warden meetings monthly; exercise every 3 months, training every 6 months.	Requirement is mandatory Country-wide arrangements are presently implemented from Nairobi.
2.3	Staff Ceiling	Requirement for Security Phase IV areas.	a. Staff ceilings for international staff (assigned and on mission) to be established for all duty stations; b. Staff ceilings to be reviewed monthly (standing item on ASMT agenda).	ASMT recommends staff ceilings, SMT approves.
2.4	Building Emergency/ Evacuation Plan	Established for all UN offices and facilities	a. Building emergency/evacuation plans exercised every 6 months	Requirement is mandatory
2.5	SMT and ASMT Meetings	To be conducted and documented as per UN Security Policy Handbook.	SMT and SMT Working Group Meetings alternate weekly (DO determines participation - attendance is mandatory) – ASMT meetings weekly	Requirement is mandatory
	Security Clearance Procedures	System in place for approving security clearances into country, recording travel notifications, and tracking personnel movements inside the country.	a. Full ISECT implementation for external and internal travel, including Phase V areas b. ISECT profiles for all staff (agencies responsible that ISECT profiles are updated)	Requirement is mandatory
2.6	Incident Reporting	a. All security incidents are reported using "SIRS"	b. Other reports as per Field Security Handbook c. Agency FSAs report incidents simultaneously to parent agency and CSA	Requirement is mandatory

2.7	Crisis Coordination Centre (CCC)	a. Established for all UN offices and facilities;	b. CCCs established in [City] and all main operational hubs; c. Exercised every six months (or more frequently if SRA so indicates) - crisis management exercises only if no actual crisis occurred – otherwise prepare "lessons learned".	Establishment of SIOC by [planned date].

United Nations Minimum Operating Security Standards – [Country]

3. MEDICAL SUPPORT				
No.	**Item**	**Standard Requirement**	**Country Specific Requirements, Equipment & Procedures**	**Remarks**
3.1	Response to Medical Emergencies	g. Casualty Evacuation Plans: immediate medical attention, identification or procurement of appropriate means of transportation, and location of appropriate primary health care facilities (inside the country). h. Medical Evacuation Plans: medical and administrative procedures necessary for evacuation of sick or injured personnel from the country, including the authority for authorization of evacuation and use of an air ambulance service where necessary. i. Establish and maintain area–specific casualty and medical evacuation plans; j. Establish and maintain Mass Casualty; k. Register of locally available medical facilities, emergency response services, and contact numbers to be maintained up to date and made available in ECS (classified as per UN PKO medical standards;) l. All staff to be trained in Basic First Aid; m. Security staff and appropriate number of other staff trained and certified in trauma and mass casualty incident response; n. Establish medical plan and PEP Protocol;	o. Adequate number of stress counsellors dedicated to [Country] based staff; p. Adequate number of paramedics under supervision of a UN physician; q. UN medical officer to supervise stabilisation centres trained and certified in Advanced Trauma Life Support (ATLS) and Pre-hospital Trauma Life Support (PHTLS) or equivalent; r. Adequate air rescue capacity, minimum one pressurised aircraft with ALS on stand-by at all times;	Response times to be reduced - objectives to be accomplished before end of 2009: • CASEVAC - trauma stabilization by paramedic max. 1 hour after incident; • Air MEDEVAC and admission to Level II hospital max. 3 hours after incident; Note: Quarterly report to DSS on progress

3.2	Medical Equipment	a. All vehicles to carry Vehicle First Aid kits (specifications as per Security Technical Standards Manual). b. Emergency Trauma Bags (ETBs) distributed according to number of trained UN staff. c. One Basic First Aid kit per building (or per floor in buildings with more than 50 personnel). d. PEP Kits (which must be replaced by their due expiry dates) will be distributed through the country PEP Kit protocol (which is to be attached to the Country Security Plan as an annex, and available in all radio rooms and duty personnel folders)	First aid kits, trauma bags, PEP kits as per requirement, in addition: e. Establish stabilization centres with ATLS and PHTLS capacity in all operational hubs (5 by September 2009 – all hubs by December 2009) f. Ambulances (or ambulance type vehicles with ability to fit stretchers) in main operational hubs; g. Establish UN dispensaries in selected locations (SMT decision); h. Support local hospitals to increase MCI and response capacity (e.g. ambulances) i. PEP kits stocked in UN dispensaries + 2 PEP kits per custodian (usually FSCO/FSA)	Note: Quarterly report to DSS on progress

CONTINUED FOR ALL MEASURES IN THE BASELINE

Annex B

SRA Matrix Format

The UN Operational Context								The Problems			The Solutions	
Threat Assessment		Programme Assessment	Vulnerability Assessment		Risk Analysis						Mitigation (Proposed Strategies and Options)	Risk Level (Residual)
	Situation		UN Weaknesses	UN Strengths	Impact	Likelihood	Risk Level (Current)					

Security Level System Guide

Introduction

The Security Level System is based on a Structured Threat Assessment (STA) that provides a standard methodology of answering questions, and selecting and inputting numerical values into an automated system that produces a Security Level.

Aim

The aim of the Security Level System is to provide an objective description of the security environment of a particular area or location in which the UN must operate. It does so based on a structured analysis of the threat that exists in the area or location, and which is conducted in such a way as to reduce subjectivity and thereby provides the UN with a threat measuring tool which is consistently applied across global operations and therefore builds system-wide reliability of the resulting information. In accomplishing the analysis in this manner, it is more likely that the analysis done by different people for the same location will be more coherent and was demonstrated more consistent. The structured nature of the process provides a specific basis for reasoned discussion to arrive at a coherent result. Lastly, the Security Level System identifies specific levels of oversight provided by the Department of Safety and Security and others which reinforces accountability.[13]

[13] The Heads of military and police components will provide military and police-related input to support the Structured Threat Assessment.

The Structured Threat Assessment in Security Level System will form the foundation for security threat briefings by DPKO to Troop and Police Contributing Countries' Meetings.

The Security Level System

The proposed Security Level System consists of six levels and is designed as a security management tool for the global UN System. The Security Level is prepared by security professionals, with the input and the approval of the DO and SMT. It provides security decision-makers with a snapshot of the existing security environment in a specific geographic area or location and can be used to make comparisons, setting priorities, and allowing staff to make the necessary preparations. It is important to note that the Security Level System is based on a logical analysis of threat and therefore should not be compared to the previous Security Phase system. Making comparisons across the two systems can be confusing and should be discouraged. See Figure 1 for the new Security Level system.

The Security Level System reduces or eliminates automatic linkages to specific security measures, such as relocation or evacuation, or to personnel entitlements, such as Hazard

Pay. It is important to note that the Security Level is determined solely based on the existing threat in an area and not on the level of risk. The Security Risk Assessment is used to determine the level of risk from each specific threat against the UN and the determination of mitigating measures for each risk to arrive at a residual risk will only be possible after completion of the Security Risk Management process.

SecLev	Security Management Actions	Authority	Level of oversight
6 Extreme	SMT meets at least once a week Security Clearance, based on new operational and security plan, to be approved by USG DSS; Exceptional mission travel into area only.	SG	
5 High	SMT meets at least once a week Re-evaluation of critical staffing needs based on programme priority reassessments by agency heads (Staff in non-critical posts relocated) Critical mission travel into area only	DO	USG DSS
4 Substantial	SMT meets at least once a week Re-evaluation of essential staffing needs based on programme priority reassessments by agency heads Programme imperative mission travel into area only	DO	Director DSS/DRO (validation within 24 hrs)
3 Moderate	SMT meets at least monthly External conferences must be authorised by DO	DO	Director DSS/DRO (validation within 24 hrs)
2 Low	SMT meets at least quarterly a year Security clearance system put in place External Conferences must be notified to DO	DO	Director DSS/DRO (validation within 24 hrs)
1 Minimal	SMT meets at least twice a year Notification of official travels	DO	Director DSS/DRO (validation within 24 hrs)

Figure 1: Proposed Security Level system

Structured Threat Assessment

The situation analysis of the Threat Assessment in the Security Risk Assessment is the basis of the STA. The STA consists of five general threat categories of which each is assessed using three standard component parts of any threat – Intent, Capability and Inhibiting Context. Evaluating these five categories of threat in the STA methodology allows the determination of a Security Level but that is not the end of the process. The STA is just one part of the Threat Assessment which is one step of the existing Security Risk Assessment process. The STA is designed to complement and strengthen the SRA process by improving the situational threat analysis step. See Figure 2 which illustrates how the STA fits into the SRA process.

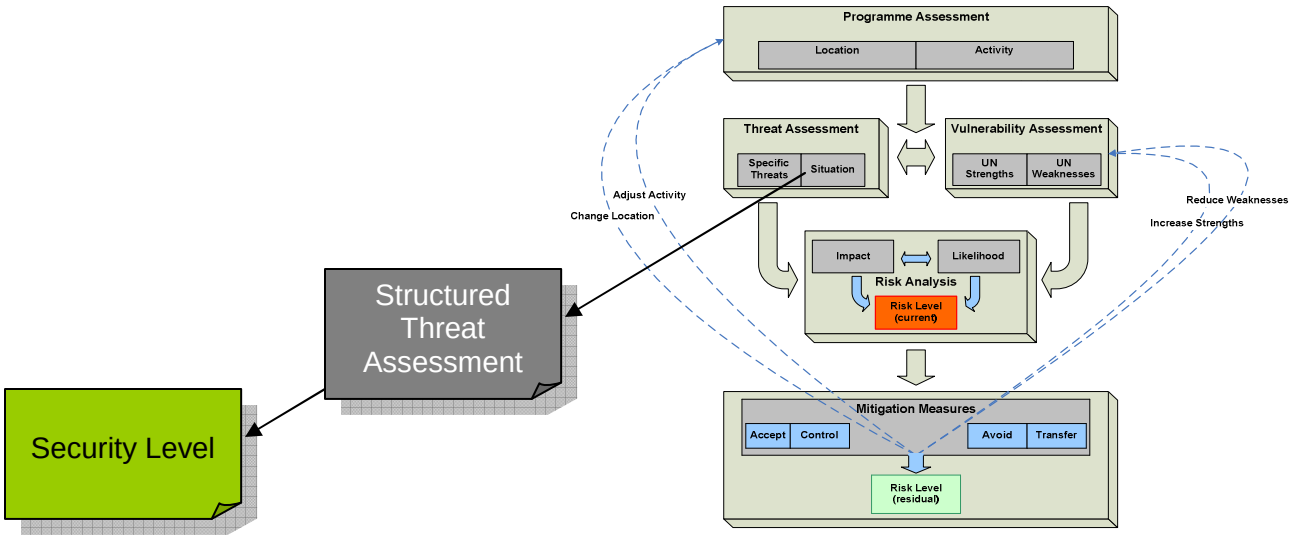


Figure 2: How the STA fits into the existing SRA process

It is important to note that the STA is not a predictive tool. It is based on current and historical information, but does not try to model or measure threats, but it does describe threats across a range of categories as they exist now in a particular geographic area or location at the current time. It does so by selecting an appropriate descriptor for the components of Intent, Capability and Inhibiting Context and assigning the most appropriate descriptor and placing that numerical value in the assessment column. This process allows threats to be graded, and when all five threat categories are assessed, the aggregated total provides an overall level of danger present in that area or location.

The features and benefits of this system are listed below and clearly demonstrate the advantages of the STA process and the Security Level System.

Feature	**Benefit**
Structured threat assessment	Reduces subjectivity; increases reliability; allows for comparison; improved oversight
Includes five categories of threat	Allows location specific environment to be

	described
No linkage to specific security measures	Avoids 'one size fits all' measures
Is a part of the existing SRA process	Avoids duplication of work

As previously stated, the STA describes the current security environment of a particular location at a particular time. It does this by looking at five general threat categories:

1. **Armed Conflict**
2. **Terrorism**
3. **Crime**
4. **Civil Unrest**
5. **Hazards**

These categories provide a complete picture of the security environment that exists in any one particular area or location. Other underlying causes of danger may be present in that particular environment such as political unrest or ethnic violence; however, the associated threats will inevitably be manifested under one or more of the general threat categories above.

The Security Level System Analytical Concept

The analytical concept behind the Security Level System (SLS) is known as Multi-Attribute Utility Analysis. Although a technical term, the principles behind this analysis are quite simple. The SLS combines three techniques called decomposition, externalization and sensitivity analysis.

"Decomposition" breaks the problem down into its component parts,

"Externalization" takes the problem and puts in into a computer matrix, and

"Sensitivity analysis" assigns different weights to each component.

The SLS uses the five general threat categories listed below to describe the general level of dangerousness (decomposition) in a geographical area or location. The SLS uses a structured threat assessment consisting of three-components to evaluate each threat category. The SLS also lays out the assessment on a clear matrix for ease of analysis (externalization).

A structured threat assessment is not enough to establish a security level, however, because, at their most dangerous, some threat categories, such as armed conflict and terrorism, are more dangerous to the UN than other threat categories at their most dangerous. Therefore, the SLS gives each threat category a different weight (sensitivity analysis) so that the resultant Security Level better reflects the reality it represents.

Extensive tests of the SLS showed that without weighing the five general threat categories differently, the SLS was not valid because it did not properly differentiate areas with different levels of danger. The exact assignment of weights for each component is a complex process, but once you use the model you will see that it works.

Information Timeframe Used in the STA

The key factors in completing the STA are significant pieces of information and the history of events impacting on the situation in the country at the time of the assessment. It is natural to ask how far back in history should a security professional go to arrive at the appropriate levels of Intent, Capability and Inhibiting Context. There is no set rule regarding a time limit on historical information. Certainly there are incidents such as the bombing attack of the US Embassy in Nairobi, Kenya in 1998 that demonstrated a group's ability to carry out an attack of this magnitude in Nairobi. However, it is important to note that in the 11 years since this attack, no other diplomatic mission or entity has been the target of a terrorist attack in Nairobi. Due to the time factor and its importance and currency, including this information has to be carefully considered in constructing the STA for Nairobi in the current timeframe.

It is important that information which is relevant to the situation today be used while there certainly a history of incidents in the past that may not be necessarily relevant to the current situation.

Categories of Threat

The STA contains five general categories of threat as generally described as follows:

a. Armed Conflict describes organized violence by groups fighting each other. The UN, like other non-involved parties, would most likely be indirectly affected by this threat.

b. **Terrorism** refers to violence by individuals or groups against civilians or other non-combatant targets. The UN could be directly or indirectly affected by this threat.

c. **Crime** describes illegal activities undertaken for economic or personal gain. It may or may not involve violence. The UN could be directly or indirectly affected by this threat.

e. **Civil Unrest** refers to organized demonstrations or unauthorized disturbances to public order e.g., rioting and looting. It may or may not involve violence. The UN could be directly or indirectly affected by this threat.

f. **Hazards** are natural events such as earthquakes and extreme weather or human-caused incidents such as large scale industrial accidents which can lead to destruction, injury or death.

Each general threat category is evaluated using three characteristic components that are key to all threats:

a. **Intent**: the intention or disposition of a threat to cause harm
b. **Capacity**: the ability of a threat to cause harm
c. **Inhibiting Context**: the qualities which exist in the environment which might act as incentives or deterrents to a threat. (**NB**: These are not mitigating measures developed by the UN)

Examining threats in this manner provides a common basis to describe each threat according to its willingness to do harm, its ability to do harm and the aspects of the environment, such as the norms of the community or the capacity of the host government or local authorities, which may constrain or encourage a threat. Applying these components provides the consistency of the Security level System for the UN globally.

Descriptors

For each threat category, a set of descriptors of Intent, Capability and Inhibiting Context have been developed to allow the user to assign an indicative value to each component of the threat being evaluated. The more serious the threat - the more danger it represents and the higher the value it would receive. The values from each of the Intent, Capability and Inhibiting Context components are then combined to produce an overall score for that particular category as illustrated in Figure 3.

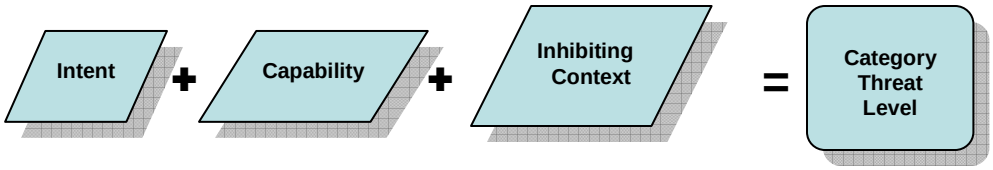


Figure 3: The three elements of threat for each category are combined to give an overall score

After evaluating all five general threat categories the scores are aggregated to produce an overall score which determines the Security Level for that particular geographic area or location as shown in Figure 4.

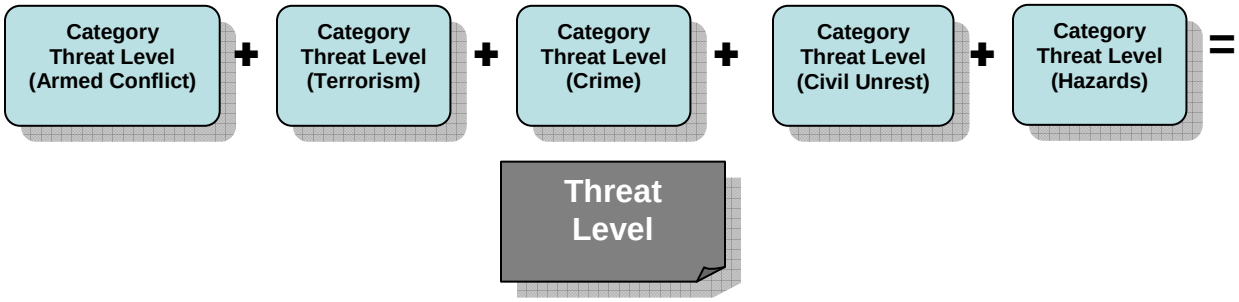


Figure 4: The scores for each category are combined to provide an overall threat level

Scores and Charts

Note that in no case is the threat level ever zero (the lowest possible score would be 1 + 1 + 1 = 3). This reflects the reality that, regardless of location, there exists some level of danger, even if it is only from being at the wrong place at the wrong time. While the numerical values given to each descriptor are arbitrary, they are relative. That is, a location with an overall score of 15 is more dangerous (has more threat) than a location with an overall score of 9. Again, it is important to note that this process is one of description and not measurement. A location with an overall score of 12 is not necessarily precisely 3 times more dangerous than a location with an overall score of 4.

The advantage of a numerical system is that it can provide a score which can be graphed against a scale that can indicate the Security Level of a particular location. Furthermore, the Security Level of several locations, either at the individual category or aggregate level, can be effectively compared. Because defined security measures, mitigation and entitlements are no longer linked to the Security Level, this new process eliminates pressure to achieve a certain Security Level because of these three factors.

Once the locations have had their aggregate score calculated they can be plotted on the 15 point scale that is

divided into 6 levels to determine a Security Level. See Figure 5.

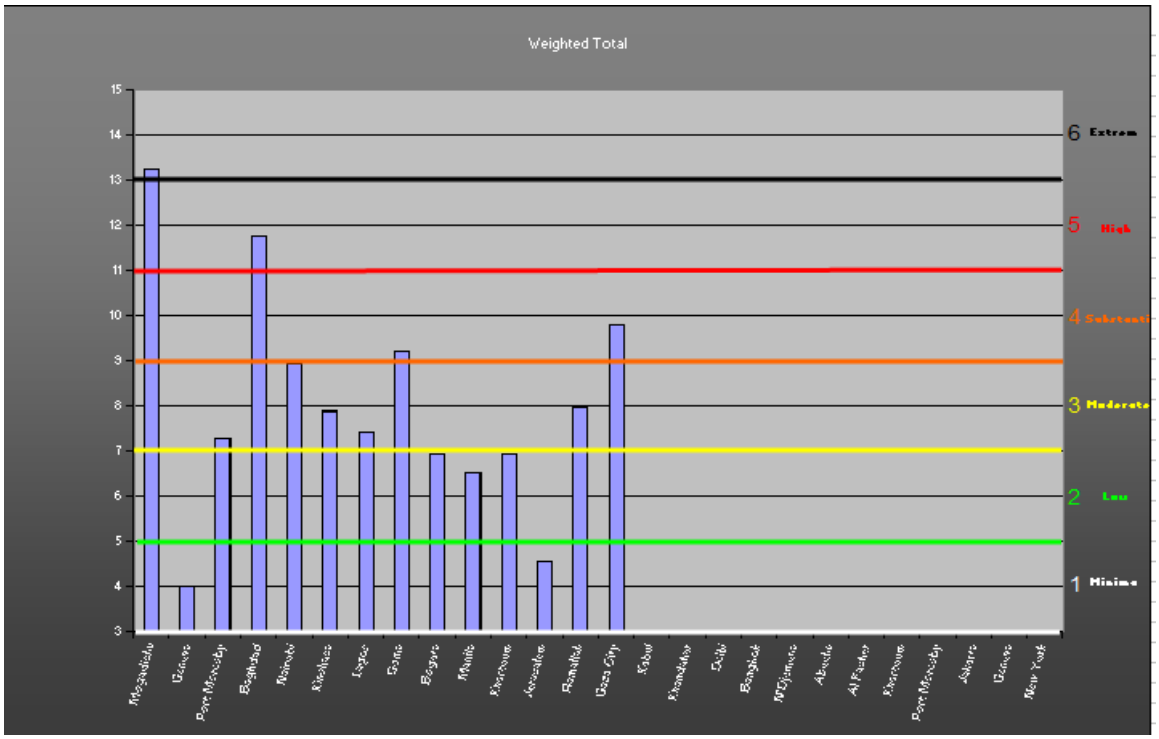


Figure 5: Location threat scores plotted against a 6 level Security Levels.

Since the threat assessment is structured and broken down into categories, it is possible to see how the elements of threat work in a particular location. For example, we can see in Figure 6 that Port Moresby's threat of crime is high, but that the other four general categories are low and in this case it is crime that contributes to raising the Security Level.

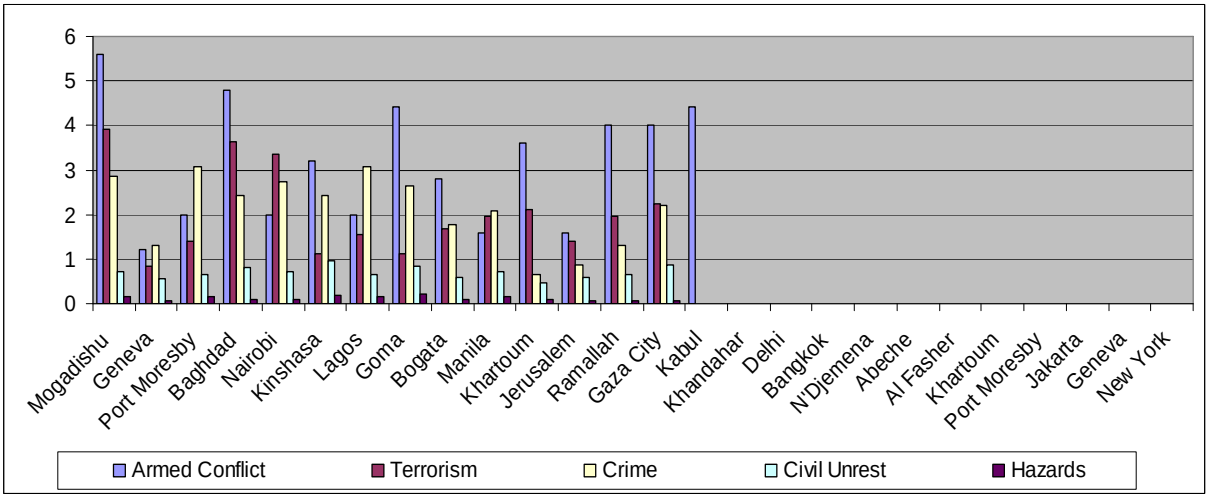


Figure 6: Security Levels by location, broken down to show individual category scores.

By contrast, it is also possible to compare locations across a single threat category. In figure 7 we can examine the general category of armed conflict and judge its relative degree of danger accordingly in several locations. The example consists of cities from numerous different countries; however, completing this process for all locations in a given country provides the Security Management Team with the ability to compare the category of Armed Conflict in all locations in a given country. This can be replicated for each category.

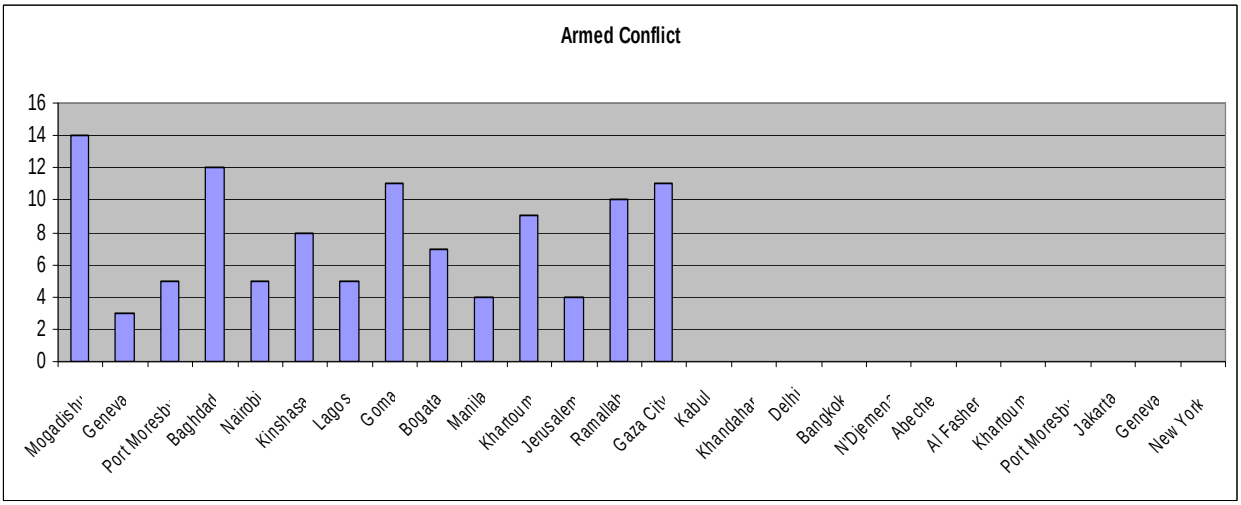


Figure 7: Comparison of location by category scores for Armed Conflict

Oversight

The Security Level System not only further empowers the Designated Official by providing additional authority but also strengthens the oversight of DSS for each level. Figure 8 illustrates both the authority of the DO in the “green” ellipse and the oversight by DSS in the “red” ellipse.

SecLev	Security Management Actions	Authority	Level of oversight
6 Extreme	SMT meets at least once a week Security Clearance, based on new operational and security plan, to be approved by USG DSS; Exceptional mission travel into area only.	SG	
5 High	SMT meets at least once a week Re-evaluation of critical staffing needs based on programme priority reassessments by agency heads (Staff in non-critical posts relocated) Critical mission travel into area only	DO	USG DSS
	No dependents	DO	Through USG/DSS for approval by SG
4 Substantial	SMT meets at least once a week Re-evaluation of essential staffing needs based on programme priority reassessments by agency heads Programme imperative mission travel into area only	DO	Director DSS/DRO (validation within 24 hrs)
	Decision as to whether dependants remain	DO recommends	Through USG/DSS for approval by SG
3 Moderate	SMT meets at least monthly External conferences must be authorised by DO	DO	Director DSS/DRO (validation within 24 hrs)
2 Low	SMT meets at least quarterly a year Security clearance system put in place External Conferences must be notified to DO	DO	Director DSS/DRO (validation within 24 hrs)
1 Minimal	SMT meets at least twice a year Notification of official travels	DO	Director DSS/DRO (validation within 24 hrs)

Figure 8: Oversight process

Applying the STA and SLS

If we take a hypothetical example, we can see how the system works (see Figure 9).

a. Looking at the threat of armed conflict for a particular location, we might determine that, given the information available, that the opposing parties have made clear statements of their intent to resort to violence. We would therefore rate their Intent as a 3.

b. Furthermore, their Capability is significant, given their experience, training, and equipment; we would rate this as a 4.

c. Lastly, the cease fire agreement is unstable, but is holding up. We could rate this as a 3.

d. The overall threat level for the category of Armed Conflict would therefore have a weighted value of 13.

The process would be repeated for each of the remaining four categories and once completed the Security Level would be determined by clicking on the SLS chart.

		Intent	Capability	Inhibiting Context
Armed Conflict	1	No intention to used armed/military force	No or very limited presence of hostile military-type capability (no or very limited military-type weapons, training, etc.)	Strong deterrent against initiating conflict
	2	Indications that military force is seen as an option or statements threatening attack but political solution still possible	Small arms/Automatic (light) Weapons (AK47, mortars, RPG) but minimal military-type training/experience and loosely organized	Pressure/other incentives/agreements against hostilities
	3	Clear statements on imminent attack and peaceful options exhausted	Organized and structured forces with increased mobility and/or standoff/indirect (medium) weapon capability	Peace talks or unstable peace/cease fire agreement
	4	Isolated/Limited/ Sporadic armed conflict occurring	Organized and structured forces w/ HW deployed and/or large numbers of forces and intensified military operations	No restraint/pressure to prevent continuation or outbreak of conflict
	5	Full-scale armed conflict occurring	Organized structured forces w/ HW deployed or large number of forces fully engaged	Armed conflict already occurring in area

Figure 9: Example of how threat element scores are assigned.

Definitions of Intent, Capability and Inhibiting Context for Each Category

Armed Conflict involves the use of weapons and physical force organized by countries or other large groups, and exists wherever there is armed fighting between states, protracted armed violence between government authorities and organized armed groups or between groups within a state. See Figure 3: Descriptors for Armed Conflict.

		Intent	Capability	Inhibiting Context
Armed Conflict	1	No intention to used armed/military force	No or very limited presence of hostile military-type capability (no or very limited military-type weapons, training, etc.)	Strong deterrent against initiating conflict
	2	Indications that military force is seen as an option or statements threatening attack but political solution still possible	Small arms/Automatic (light) Weapons (AK47, mortars, RPG) but minimal military-type training/experience and loosely organized	Pressure/other incentives/agreements against hostilities
	3	Clear statements on imminent attack and peaceful options exhausted	Organized and structured forces with increased mobility and/or standoff/indirect (medium) weapon capability	Peace talks or unstable peace/cease fire agreement

	4	**Isolated/Limited/ Sporadic armed conflict occurring**	**Organized and structured forces w/ HW deployed and/or large numbers of forces and intensified military operations**	**No restraint/pressure to prevent continuation or outbreak of conflict**
	5	**Full-scale armed conflict occurring**	**Organized structured forces w/ HW deployed or large number of forces fully engaged**	**Armed conflict already occurring in area**

Intent:

1. ***No intention to use armed/military force***:

a. External: There is no armed conflict (peace agreement in force, no territorial, political, ideological, religious disputes with neighbouring states),

b. Internal: No organized armed group in opposition to the government.

2. ***Indication that military force is seen an option or statements threatening attack, but political solution still possible:***

a. External: Tension between neighbouring countries exists; politicians make threatening statements, small scale border incidents, including harassing fire occur.

b. Internal: Political opposition within a state starts recruiting militants into organized armed groups and threatens the government to use force.

3. ***Clear statements on imminent attack and peaceful options exhausted:***

a. External: Number of border incidents increased. Politicians instigated hate media campaign. Diplomatic demarches (recall of ambassadors, breaking off of diplomatic relations) are launched. Armed forces of neighbouring countries are engaged in border conflicts, peace talks are suspended, and ultimatums are issued.

b. Internal: Organized armed groups that threatened the government to use force. Isolated guerrilla actions throughout the country occur. The government issued ultimatum to opposition and started building up forces in the area of opposition armed groups operations. Small scale engagements are possible. Cease-fire agreement is seriously challenged. Conflicting parties conduct limited scale military operations (raids, probing actions, cordon and search operations, sporadic exchange of artillery fire and air strikes, ambushes)

4. ***Isolate/Limited/Sporadic armed conflict occurring:***

Peace talks are interrupted, ultimatum is expired, and war may be declared. Cease-fire agreement is broken. Part of the country may be declared independent or annexed. Conflicting parties engaged in limited scale combined armed operations (multiple artillery and air strikes limited by area of conflict, counter battery artillery fire, use of armour, guerrilla warfare limited by area of operations)

5. ***Full-scale armed conflict occurring***

War or counter-guerrilla operation is occurring. The entire country/part of country is declared a war zone. All peace agreements are broken. Conflicting parties are fully engaged in armed conflict.

Capability:

1. ***No or very limited presence of hostile military-type capability (no or very limited military type weapons, training, etc):***

Neighbouring countries are neutral or are in a political/military alliance. There is no organized armed opposition force within the country. Disorganized armed groups without coordinating structure equipped with improvised weapons and side arms.

2. ***Small arms/automatic weapons, but minimal military-type training, experience and loosely organized:***

This is mainly the case with internal armed conflict, when opposition is building-up its armed groups both within and/or outside the country. Armed groups do not have a military-type structure, training camps and is equipped with automatic weapons (semi-automatic rifles, submachine guns, light machine guns and grenade launchers).

3. ***Organized and structured force but without deployed heavy weapons capability:***

Conflicting parties are in possession of heavy weapons which are not primarily deployed outside military camps and barracks. However, some of the heavy weapons can be used for harassing fire or surge operations (air strikes and/or counter battery fire). Armed elements may be placed at an enhance stage of alert. Military check points and static/mobile patrols with automatic weapons may be visible in the area. Military exercises may be organized around the area. Additional manpower and materiel may be mobilized.

4. ***Organized and structured force with heavy weapon deployed and/or large number of forces and intensified military operation:***

Ongoing mobilization. Heavy weapons (artillery, mortars, rocket launchers, armour, air assets, and warships) and/or large number of forces are deployed to positions or at designated areas at high readiness of alert. Military units are replenished and reinforced. Troops are moving towards confrontation line/area of concern, manning firing position and frequently using heavy weapons capability.

5. ***Organized structured forces with heavy weapons deployed or large number of forces fully engaged:***

Conflicting parties are engaged with full strength armed forces (manpower and materiel) including heavy artillery, rockets, armour, air assets, warships in part of or throughout the whole country (territory).

Inhibiting Context

1. ***Strong deterrent against initiating conflict:***

There is no political or social base for initiating an armed conflict. The relations with neighbouring countries and with opposition within the country are stable.

2. ***Pressure/other incentives/agreements against hostilities:***

There is strong political and/or social pressure against initiating conflict. Peace/cease-fire agreements are in force and fully honoured.

3. ***Peace talks or unstable peace/cease fire agreement:***

Peace/cease-fire agreements are unstable and seriously challenged, but political and/or social pressure on conflicting parties exists. Violations of peace/cease-fire agreements intensify. Peace talks are ongoing. Special envoys and facilitators conduct missions to the area of conflict.

4. ***No political or other restraint/ pressure to prevent continuation or outbreak of conflict:***

Peace/cease-fire agreements are expired or broken at least by one of conflicting party. Peace talks are interrupted. International facilitators and special envoys have left the area of conflict.

5. ***Armed conflict already occurring in area:***

Conflicting parties are fully engaged in combat.

Terrorism

		Intent	Capability	Inhibiting Context
Terrorism	**1**	**Intent to use terrorism against the UN acknowledged worldwide**	**No known terrorist capability (threats and harassment only tactic)**	**Security forces effective**
	2	**Intent to use terrorism and/or small-scale attacks**	**Limited to small-scale/individual basic operations**	**Security effective and/or social support of cause**
	3	**Wide-spread small-scale attacks on local infrastructure**	**Some isolated but coordinated operations that produce limited effects**	**Security moderately effective and/or active assistance to terror cells in some areas**
	4	**Sustained or large-scale attacks and/or statements or actions demonstrating intent to target UN**	**Demonstrated capacity in wider-range and varied terror attacks**	**Security forces challenged to prevent terrorist activities**
	5	**A group has already attacked the UN and is still operational in the area**	**Demonstrated ability in all terror tactics to produce mass destruction and/or causalities (complex attacks)**	**Minimal ability to deter terrorist attacks. Terrorists have safe havens**

The United Nations has not adopted a single definition for terrorism. For the purposes of the STA and noting that there are numerous definitions of terrorism, an aggregate of those elements that recur most frequently have resulted in the following definition:

> Terrorism is a tactic primarily used by non-state actors, who can be an acephalous entity as well as a hierarchical organisation, to create a psychological climate of fear using threats or actions in order to compensate for the legitimate political power they do not possess. It can be distinguished from guerrilla warfare, political assassination, criminal abduction, or economic sabotage, although organisations that practise terror can resort to these too.

Please note, these guidelines are just a guide to assist in assigning relevant descriptors that identify the conditions on the ground that best suit the situation. They are not all

inclusive and some scope for flexibility must be given to local conditions and circumstances.

Intent

1***. Intent to use terrorism against the UN acknowledged worldwide:***

The default lowest level is the de facto "global threat of terrorism" and the fact that the UN is a named target. For the purposes of this level, generic and non-specific threats to resort to terrorism locally may also be recognised and be included at this level.

2. ***Intent to use terrorism and/or small-scale attacks:***

Specific warnings have been received from the host government or other member state entities indicating that terrorist acts may be under preparation. This may also include situations whereby there have been the occasional small scale local terrorist acts with the intent to instill fear without necessarily aiming to kill.

3. ***Wide-spread small-scale attacks on local infrastructure:***

There is a local terror campaign on-going, targeting local government institutions and public places, but not directed at the UN. Incidents are small scale, limited to small IEDs, possible abduction and targeted assassination. No VBIEDs or PBIEDs. Incidents are not mass casualty in nature. This level could also include situations where the UN has received specific information from the host government and/or member states that terrorist group (s) have moved from a preparedness stage to an operational stage with specific target profiles that may include the UN.

4. ***Sustained or large-scale attacks and/or statements or actions demonstrating intent to target UN:***

There is a local terror campaign on-going, targeting local government institutions and public places with intent to create mass casualty incidents. This may include the use of VBIED/PBIED and armed attacks, but also assassination, abduction and other terrorist tactics. There are express statements indicating that the UN is a target.

5. ***A group has already attacked the UN and is still operational in the area:***

There is a sustained local/regional terror campaign with the intent to cause mass casualty incidents. The use of

VBIED/PBIED is common and full range of other terrorist tactics apparent. AND/OR - A local terror campaign as per '3' or '4' above, where the UN has been attacked by the existing group or credible information suggests an attack is imminent.

Capability

1. ***No known terrorist capability (threats and harassment only tactic):***

There is no known capability in the region or area of concern. This level may also be assigned when there are generic but unconfirmed reports that some operatives may be apparent in the extended regional/geographic area.

2. ***Limited to small-scale/individual basic operations:***

There is limited and uncoordinated capability. Individuals operate independently with limited resources. There is minimal access to (and use of) military type hardware and/or explosives.

3. ***Some isolated but coordinated operations that produce limited effects:***

There is now limited, but coordinated capability. Individuals operate in a coordinated fashion, with planning, guidance and/or leadership. There is still minimal access to (and use of) military type hardware and/or explosives and thus limited range of tactics, but can include targeted assassination and kidnapping.

4. ***Demonstrated capacity in wider-range and varied terror attacks:***

In this level there is a demonstrated ability to plan, resource and conduct small scale coordinated attacks. This may also include the ability to deploy multiple coordinated small scale IED operations (not suicide operations). There is evidence of access to wider range of resources.

5. ***Demonstrated ability in all terror tactics to produce mass destruction and/or causalities (complex attacks):***

In this level there is a demonstrated ability to plan, resource and conduct complex attacks, including coordinated multiple IED, PBIED, VBIED attacks, guerrilla tactics, kidnappings and targeted assassinations. Mass casualty events common.

Inhibiting Context

1. ***Security forces effective:***

Security and Intelligence Services are professional, trained and effective. In the context of the country, there is no or very limited social support for the terrorist cause.

2***. Security effective and/or social support of cause:***

The country has a professional and trained security and intelligence services, but the social support network within sections of the community are apparent limiting the capability of security and intelligence services to deter.

3. ***Security moderately effective and/or active assistance to terror cells in some areas:***

In this level the security and intelligence services are assessed to be moderately effective. This would include situations where the social support network actively assists or facilitates terror operations.

4. ***Security forces challenged to prevent terrorist activities:***

In this level security and intelligence services are apparent, but are challenged by the situation. Significant parts of the local community actively assist and facilitate operations. There is some freedom of movement for the operatives apparent.

5. ***Minimal ability to deter terrorist attacks. Terrorists have safe havens:***

There is minimal ability to deter attacks. Operatives have established safe-havens and are able to move freely throughout large areas of the country/region.

Crime

		Intent	Capability	Inhibiting Context
Crime	**1**	**Property crime, seldom violent**	**Generally lone unarmed criminals**	**Police/criminal justice system effective and crime is socially unacceptable**
	2	**Opportunistic crime against individuals, seldom violent**	**Generally lone criminals, sometimes armed**	**Crime is not socially acceptable; police/CJ system not fully effective**

	3	Violent crimes focus on relatively affluent elements of the community	Lone armed criminals and/or unarmed criminals operating in small teams	No major social constraints on crime; police/CJ system stressed
	4	Wide-spread violent crimes	Armed criminals operating in small teams	Police/CJ system significantly challenged
	5	Prevalence of violent w/frequent fatalities and/or focus on the UN	Organized armed criminal gangs	Minimal social or Police/CJ controls on criminal activity

Sources of information

As much as possible the assessment of this specific threat must be based on statistics. When statistics are not reliable or not available information must be sought from press reports, reporting of incident by staff members, the diplomatic community, local staff, medical and religious sources, foreign travel advisories, etc.

In addition, the way the local population protects itself can sometimes provide some useful information. The almost systematic installation of barbed wire on perimeter walls and or the recourse to private security guards can be some good indicators.

Intent:

This variable must take into account the type of crime so as to capture the nature and dangerousness of criminal acts. It ranges from petty crimes such as ordinary thefts to violent crimes which may result in the death of the victim (s). One cannot provide an exhausting list of violent crimes but the following criminal acts should be regarded as such: murder, assassination, kidnapping, sexual assault, assault and battery. One has to note that in some countries or areas crimes are committed by the security forces themselves. Such crimes should be included when assessing the specific threat of crime. [14]

Capability:

This variable is a measurement of the dangerousness of criminals based on whether they generally operate individually or in teams or gangs and/or whether they are armed. It is obvious that an unarmed individual represents a lesser threat than a gang of armed criminals. What needs to be considered is the trend. The assessment should not be based on a one off incident.

[14] Police components will utilize Criminal Information Analysis data and methodologies to support criminal threat assessment.

Inhibiting context

This variable is a measurement of the efficiency of both law-enforcement authorities and the criminal justice system in preventing, investigating crimes and in arresting and prosecuting criminals. It also takes into account whether the local population tends to turn a blind eye or condones criminal activities.

Civil Unrest

		Intent	Capability	Inhibiting Context
Civil Unrest	**1**	**Peaceful crowds only**	**<100 people**	**Effective crowd control or crowd self-controlled**
	2	**Some crowd become disruptive**	**<500 people**	**Crowd control not fully effective**
	3	**Crowds become violent/localized riots**	**<1000 people**	**Crowd control mechanisms stressed (#s, equipment, etc.)**
	4	**Extensive/wide-spread violent crowds/riots (UN possible target)**	**<5000 people**	**Challenged crowd control mechanism or some possibly to allow anti-un protests**
	5	**Violent crowds/riots targeting UN**	**5000+ people**	**Minimal crowd control mechanisms**

Civil Unrest attempts to identify the threatening components of a deteriorating situation exemplified by the formation of public gatherings (organized demonstrations or unauthorized gatherings) that turn violent. Experience has shown that the key components of Civil Unrest are the mood and its size. Once the crowd becomes violent its capacity for danger increases exponentially with the introduction of weapons (stones, Molotov cocktails [petrol bombs] and guns). A combination of these factors results in the degree of threat exhibited by the crowd.

Mood (Intent). The 'mood' of a crowd can change dramatically. A crowd may begin peaceful and calm, but can be whipped up into a frenzy that may be channeled into violence by individuals or groups of carefully placed agitators. Or, a crowd may form with a stated angry intent (a crowd forming to demonstrate specifically against the UN for its presence or policies) which can be inflamed by agitators, or by ill-disciplined crowd control measures that utilize excessive force.

Size of the crowd (Capability). As crowds increase in size they develop internal dynamics (such as mob violence and mass hysteria) that can either take on a momentum of their own and create danger to anyone present, or can be utilized by 'agitators' to create a specific result . A small crowd gathered to demonstrate with peaceful intent carries relatively little threat, however as the crowd increases in size its internal dynamics change (i.e., its sheer mass – a crowd of 5000 +) and consequently, even without weapons, it develops a potential threat profile.

The matrix above captures these variable dynamics in the first 2 columns (Intent & Capability). Clearly, the Inhibiting Context then becomes the effectiveness of the crowd control mechanism and this can be measured by its size and organized structure; its physical capability in terms of resources and specialist crowd control equipments, and the degree of professional training and control exhibited by the controlling force. The more resourced and effective these measures, the less likely the threat from the crowd will develop out of control. Consequently, the least threat comes from a small crowd with non-violent intent that is contained by effective control measures. The greatest threat comes from a large crowd with violent intent (and has weapons) and that is not contained by control measures.

Definitions

Peaceful crowd: A gathering that has no stated violent intent, is not armed, is fully self-controlled and respects the attendance of crowd controlling measures.

Crowd elements becoming disruptive: A gathering that begins peacefully with perhaps a stated peaceful intent, but that exhibits signs of aggression from individuals, small elements or organized groups. Some elements of the crowd may resent the presence of crowd control measures. A mood-change may be evident.

Crowds become violent / localized riots: Violent behaviour is clearly evident in the crowd; this may be directed at the targeted objective of the crowd's purpose (i.e.; an opposition group, institution or authority (including the UN)), or against the crowd control entity (be it police, military, paramilitary or militia forces). Violence includes the use of improvised weapons and projectiles (stones, glass, metal, petrol bombs, locally made weapons or conventional small arms). Localised riots indicates larger elements of the crowd breaking away in organized (loosely or cohesive) groups to confront the target of the crowds purpose, authority or crowd control entity with

escalating violence. The destruction of civil and private property may be clearly evident (burning cars, breaking shop windows and looting). The mood of the crowd may become increasingly violent and the dynamics may change to include mob behaviour and mass hysteria.

Mob behaviour and Mass Hysteria: Mob behaviour is a phenomenon that encourages 'innocent' and 'normal' people to conduct acts of extreme violence (which they would not normally do) under the influence of a growing emotional hysteria within the group.'

Extensive/wide-spread violent crowds/riots (UN possible target): Mass gatherings that break down into numerous crowds with violent intent, or organized crowds rioting across several different locations (but with the same purpose), which are sometimes coordinated and sometimes spontaneous. The threat from these crowds could result from the violence and hysteria within the crowd, or from the response of the crowd control entities (which may retaliate with the use of extreme violence). The threat to UN individuals and premises may be 'wrong place – wrong time' [Staff members encountering the crowd, or a crowd passing by a UN office and venting against it opportunistically].

Violent crowds/riots, targeting UN: The crowd is violent and has either been agitated to change its original purpose to then target the UN, or has formed with the intent of targeting the UN and is escalating its levels of violence directing it at either UN staff members or UN property and assets.

Hazards

Hazards		History	Intensity/severity	Warning/ Preparedness
	1	Not prone to hazard events	Limited	Effective warning and preparedness systems in place
	2	Hazard events occur occasionally	Moderate	Partial/limited warning and/or preparedness systems in place
	3	Hazard events occur frequently	Severe	Warning and/or preparedness systems in place not fully effective
	4	Prone to predictable hazard events and/or hazard event imminent	Devastating	Warning and/or preparedness systems are untested or unknown
	5	Prone to sudden onset hazard events	Multiple and devastating	No warning and/or preparedness systems in place

In the first four threat categories we have used the variables of Intent, Capability and Inhibiting Context to

conduct our assessment. Due to the nature of this category these variables are not appropriate to achieve the proper analysis for this category; therefore, History, Potential Intensity/Severity and Warning/Preparedness are more appropriate and are used for this particular category.

Natural hazards and natural disasters may sound like the same thing but there is a small but vital difference - natural hazards do not automatically cause natural disasters.

Natural hazards may encompass effects like earthquakes, volcanic eruptions, landslides, tsunamis, floods and drought - any physical event that happens naturally. They may occur quickly, called a rapid onset hazard, or build up gradually, called a slow onset hazard. They can happen over small local areas, regions or affect the whole country.

A natural hazard is an event that will have a negative effect on people or the environment. Many natural hazards are related, e.g. earthquakes can result in tsunamis, and drought can lead directly to famine and disease. One concrete example of the division between hazard and disaster is Hurricane Katrina, which was a disaster, whereas Hurricanes are the hazard. Hazards are consequently relating to a future occurrence and disasters to past or current occurrences. As with other threats natural hazards should be based on both current and historical information.

Natural Disasters come about when the effects of a natural hazard cause serious problems for the people they affect, either in maintaining or improving their standard of living. This can be an economic effect (destroying crops for example), a social one (e.g. families being separated), or both.

The precise definition of a natural disaster is an event which causes a serious disruption and is triggered by a natural hazard causing human, material, economic or environmental losses, which exceed the ability of those affected to cope. The intensity/severity of the event will be affected by the ability to affect early warning/ preparedness.

A slow onset natural hazard may unfold alongside and within development processes, the hazard can be felt as an ongoing stress for a longer period of time, e.g.; weeks/months, or even years; drought is a prime example of a natural hazard that often turns into a natural disaster

by causing crops to fail which causes food shortages and then famines.
A rapid onset natural hazard is one which is triggered by an instantaneous shock. The impact of this hazard may unfold over the medium or longer term; an earthquake is a prime example of a sudden onset disaster.

A natural disaster is understood to be an outcome of both natural hazard and human vulnerability coming together, the coping capacity of society influences the extent and severity of damages received. Natural hazards are natural phenomena occurring in the biosphere that may comprise a damaging event and that in turn may be modified by human activities, such as environmental degradation and urbanization.
Human vulnerability is a condition or process resulting from physical, social, economic and environmental factors, which determine the likelihood and scale of damage from the impact of a given hazard. Human vulnerability includes within it the vulnerability of social and economic systems, health status, physical infrastructure and environmental assets. Coping capacity is the manner in which people and organizations use existing resources reactively, to limit losses during a disaster event.
When reviewing this process it is important to note that that early warning technologies are available for almost all types of hazards, and are in operation in many parts of the world. In some locations, useful forecasts or Nowcasts (short-term weather forecast) are possible even for hazards such as flash floods and climate impacts. Over the last decade, disasters have affected about 2.5 billion people and claimed the lives of nearly 900,000 people.
Warning and Preparedness: The security professional should consider the regional/national/local capacity for hazard monitoring and early warning services e.g. are the right parameters being monitored? Is there a sound scientific basis and available capacity for making forecasts at the regional/national levels? Can accurate and timely warnings be generated locally by the national/regional/local authorities?
The user should also consider the national and community response capabilities, e.g. are national/regional response plans up to date and tested? Are local capacities and knowledge made use of? Are people prepared and ready to act on warnings, is their a relevant communications system in place to facilitate these warnings?
It is important to register for and utilize specific tools to assist with natural hazards/disasters, the most prominent is the Global Disaster Alert and Coordination System (GDACS) (http://www.gdacs.org) which can provide near real-time alerts about natural disasters around the world and tools to facilitate response coordination, including

media monitoring, map catalogues and Virtual On-Site Operations Coordination Centre.

Web based STA tool

To support the standardization of determining Security Levels, DSS has developed a web-based STA matrix for use by all security professionals and others who are responsible for completing the STA to determine a Security Level. The system is designed to permit rapid and effective assessments for Security Levels and, in addition, allows DSS Desk Officers immediate access to completed assessments. The global use of the web-based Security Level System will further strengthen the UNSMS by allowing advice and feedback to the security professional, and to assess and compare, in real time, the security situation in different duty stations of the country. It will also provide a means to track trends and permit comparisons to other countries and locations. The web-based SLS will be finalized shortly and procedures for its use distributed to all security professionals.