CHAPTER IV

Security Management

Section A

SECURITY RISK MANAGEMENT

Promulgation Date: 18 April 2016
Technical Review: 10 October 2017

A. Introduction

1. The Security Risk Management (SRM) process was launched by the United Nations Security Management System (UNSMS) in 2004 as a system–wide managerial tool to analyse and manage safety and security risks to United Nations personnel, assets and operations. It was last updated in 2009 with additional guidelines, training tools and templates.

2. In July 2010, the Inter-Agency Security Management Network (IASMN) formed a working group for broader enhancements of the SRM process. Reviews of the SRM process and the resulting recommendations and decisions indicated that the following areas could be further enhanced:
   (a) The reliability and validity of the assessment of security risks;
   (b) The context-specific SRM strategies;
   (c) Dynamic, responsive and flexible application of the SRM process, to changes in the situation and programming;
   (d) Structured decisions on risk management measures and acceptance of risks; and
   (e) Management and oversight of the implementation of approved SRM measures.

3. As a result, a revised SRM process has been developed and tested across the spectrum of security environments. It supports valid, context specific, and timely Security Risk Assessments and risk management decisions to ensure that programmes are delivered within an acceptable level of security risk. The revised process supports security professionals and security decision-makers to effectively manage security risks.

B. Purpose

4. The purpose of this policy is to provide United Nations security decision makers, programme managers and security professionals with the concept, principles and applicability of the SRM process as defined by the UNSMS.

5. This policy must be read in conjunction with the UNSMS Security Risk Management Manual (“SRM Manual”) which provides details of the theory, practices and procedures of the SRM process. The SRM Manual contains directions on how to carry out the SRM process and how to apply the SRM tools.

C. Scope and Applicability

6. This policy is applicable to all UNSMS organizations as well as all individuals defined in Chapter III, Section A of the *Security Policy Manual* (SPM) ("Applicability of the United Nations Security Management System"). All references to the United Nations herein refer to the United Nations and United Nations system organizations participating in the UNSMS.

D. Policy principles

7. The primary responsibility for the safety and security of the United Nations rests with the host Government.[1] In addition, all actors in the UNSMS have security management responsibilities and accountability in line with the Framework of Accountability for the UNSMS ("Framework of Accountability").[2]

8. In cooperation and collaboration with relevant host Government entities, United Nations managers take security management decisions based on technical advice provided by United Nations security professionals.

9. The goal of the UNSMS SRM is to enable programmes and operations of United Nations personnel, premises and assets.

10. Security Risk Management is essential to achieving the United Nations goals by decreasing the effect of threats. Security Risk Management offers a structured approach to identifying and assessing the threats to the United Nations, enabling identification of SRM measures to reduce the level of assessed risk and enhancing the decision-making process in line with the Framework of Accountability, UNSMS policies and guidelines. It allows managers to maximize programme opportunities and to allocate security-related resources in ways that enable programme delivery within acceptable levels of risk.[3] It is vital for achieving the planned and envisioned programme results for the UNSMS organizations, especially in complex and dangerous environments.

11. Security decisions must be in line with existing UNSMS policies and guidelines.

12. The UNSMS only has the remit for three areas of safety: road safety, fire safety and aviation safety. Thus, there are many other areas of safety not covered by the UNSMS

[1] For more details, refer to UNSMS *Security Policy Manual,* Chapter II, Section D ("Relations with Host Countries on Security Issues").

[2] For more details, refer to UNSMS *Security Policy Manual,* Chapter II, Section A ("Framework of Accountability"), which outlines the roles and accountability of all actors with security management responsibilities in the United Nations Security Management System.

[3] For more details, refer to the Programme Criticality Framework which has been endorsed by the HLCM in March 2013 and by the CEB in October 2013.

(and, therefore, the SRM process), including medical issues, occupational health and safety, and structural engineering.

E. Security Risk Management concept

13. Any United Nations objective, from global strategic goals to local programme plans, may fail because of various obstacles. In the security context, obstacles are called threats. All managers must identify threats and evaluate how these threats may affect their objectives. In many of the places where we work, the effect of threats, if not managed, can be fatal to personnel and can result in cessation of programmes.

14. Security Risk Management is the process of identifying future harmful events ("threats") that may affect the achievement of United Nations objectives. It involves assessing the likelihood and impact of these threats to determine the assessed level of risk to the United Nations and identifying an appropriate response. Security Risk Management involves four key strategies: controlling, avoiding, transferring and accepting security risk. Security risks are controlled through prevention (lowering the likelihood) and mitigation (lowering the impact).

15. Risk is the combination of the likelihood of a threat being carried out and the subsequent impact to the United Nations. Security measures can either be used to prevent vulnerability from being exploited or mitigate the impact of exploitation, or both.[4] One way to think of risk management is that it is the systematic determination and implementation of timely and effective approaches for managing the effects of threats to the Organization. SRM is merely the management of security-related risks.

16. In the SRM process, likelihood and impact are assessed on a 1-5 scale and combined in a risk matrix as follows:

Risk Matrix		Impact				
		Negligible	Minor	Moderate	Severe	Critical
LIKELIHOOD	Very Likely	Low	Medium	High	Very High	Unacceptable
	Likely	Low	Medium	High	High	Very High
	Moderately Likely	Low	Low	Medium	High	High
	Unlikely	Low	Low	Low	Medium	Medium
	Very Unlikely	Low	Low	Low	Low	Low

Figure 1: Risk Matrix

[4] When discussing the management of risks, the UNSMS has adopted the terms "prevention" and "mitigation"; taking measures to reduce likelihood is called "prevention" while taking measures to reduce impact is called "mitigation".

F. The Security Risk Management process structured approach

17. The SRM process is a structured approach to evaluating security risks to ensure that a comprehensive threat and risk analysis leads to effective security decision-making and to the implementation of SRM measures. The SRM process endeavours to be:
    (a) Objective, fact-based, logical and systematic;
    (b) Globally applicable in a consistent, de-politicized manner;
    (c) Reliable (achieve similar results when different people use it);
    (d) Valid (accurately represent the security environment on the ground); and
    (e) User-friendly without being over-simplistic.

    The SRM process is an ongoing process with nine steps:

    Step 1: Setting the Geographical Scope and Timeframe;
    Step 2: Situational Analysis;
    Step 3: Programme Assessment;
    Step 4: Threat Assessment (General and Specific);
    Step 5: Security Risk Assessment;
    Step 6: Security Risk Management Decisions;
    Step 7: Security Risk Management Implementation;
    Step 8: Acceptable Risk; and
    Step 9: Follow up and Review.

18. Each step of the risk management process and how each step interacts with other steps is explained below in figure 2 below.

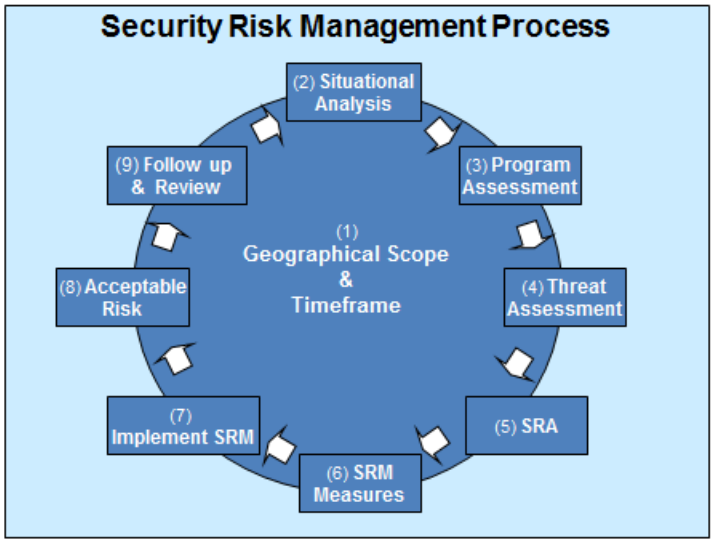

Figure 2: Security Risk Management Process Structured Approach

G. Roles and Responsibilities in the SRM Process

19. The *Framework of Accountability* identifies the following roles and responsibilities with regard to the implementation of the SRM process:
    (a) Security professionals are responsible for initiating, conducting and monitoring all phases of the SRM process.

    (b) Security decision makers are responsible for decisions made throughout the SRM process, including those associated with SRM measures and acceptable risk.

    (c) The Designated Official (DO) is the only decision maker who can approve SRM measures for an SRM Area. Where an Area Security Coordinator (ASC) is appointed, he or she will present the SRM recommendations for the Security Area to the DO for approval.

    (d) The SMT members advise and support the DO in the decision making process. The approval process for each SRM Area MOSS will be as follows:
        i. The SRM measures will be presented to the DO and SMT for consideration as part of the Area SRM process.
        ii. SMT members will be given a minimum of four weeks to consider the measures during which time they should seek endorsement, support and advice from their HQs, as required.
        iii. Considering the advice of the SMT members, the Area SRM will be approved or not by the DO at a formal SMT meeting. The SRM measures approved in the Area SRM will become the MOSS for that area. This will be a part of the SMT minutes.

    (e) Once the area MOSS approved by the DO, the responsibility for implementing rests with all UN Personnel as members of the UNSMS and UNSMS Organizations with a presence in that area. Specific management responsibilities for implementation are to be identified prior to the approval of the measures is mandatory for all.

    (f) UNDSS supports the monitoring of the SRM implementation in consultation with the Chief Security Adviser and/or security professionals who advise the Designated Official and the SMT.

    (g) Any security decision maker can accept recommendations that follow an ad hoc SRM process, unless these recommendations would be less effective in reducing the risk than the requirement already approved by the DO. Less effective ad hoc SRM recommendations would require DO approval.

20. Accountability for the conduct and quality of Programme Criticality Assessments lies with the Resident Coordinator or the Special Representative of the Secretary-General/Head of Mission, as applicable. The DO uses the results of the Programme Criticality Assessment

and takes decisions on acceptable risk at the country level.[5] In situations of a very high residual risk, the final decision on acceptable risk lies with the Under-Secretary-General for Safety and Security.

21. The review of the SRM process, including recommended SRM measures and monitoring of the implementation of approved measures when necessary, must be a standing agenda item for all Security Management Team meetings.

H. Definitions

22. For the purpose of this policy, the definitions of key terms are as follows:

Security Risk Management	The systematic determination and implementation of timely and effective approaches for managing the effects of threats to the United Nations.
Threat	A potential cause of harm initiated by deliberate actions.
Hazard	A potential cause of harm resulting from non-deliberate actions.
Risk	The likelihood of a harmful event occurring and the impact of the event if it were to occur. (Risk = Likelihood x Impact)

Conditions of Risks within the SRM Process:

• **Present Risk**	The security risk based on the threats, and the security measures and procedures currently in place.
• **Projected Risk**	The expected security risk if recommended security measures and procedures were to be in place.
• **Residual Risk**	The security risk remaining after approved security measures and procedures have been implemented.
• **Risk Rating**	A rating of the risk based on an assessment of the likelihood and impact from very low to unacceptable.
Likelihood	A rating of the assessed potential for a harmful event to effect the Organization.

[5] Decision of the Secretary-General, 12 January 2016, Meeting of the Policy Committee.

Impact	A rating of the assessed potential harm that an event would have (if it were to occur) on the Organization.
Vulnerability	A weakness that can allow a threat or hazard to cause harm.
Vulnerable	Inadequate SRM measures and procedures meant to address a threat.
Capability	The capacity or ability of threat actors to cause the threat event as described.
Intent	The motivation or disposition of a threat actor to cause the threat event as described.
Event Description	Clear description of a harmful event that the SRM process will examine (must include the effect on the Organization).
SRM Area	Geographic scope defined for the application of the SRM process.
MOSS	Once approved by the DO, the output of the Area SRM process is the MOSS and as such is area and, in some cases, agency specific.
Programme Assessment	A process by which the security professional formally comprehends the programme requirements of the UNSMS organizations.

I. Training Requirement

23. All United Nations officials who have specific security responsibilities within the Framework of Accountability shall be cognizant of the SRM concept and process. Training on SRM shall be mandatory.

24. The United Nations Department of Safety and Security (UNDSS) shall develop a training specifically tailored for DOs, Security Management Team members, security professionals and managers of United Nations system organizations, and coordinate the delivery of such training courses.

J. Final Provisions

25. This policy is to be made available to all United Nations personnel.

26. This policy enters into force on 18 April 2016 with revisions made October 2017.

27. The UNSMS *Security Policy Manual* (SPM), Chapter IV, Section A: "Policy and Conceptual Overview of Security Risk Management" (April 2009); Chapter IV, Section B: "Security Level System"; Chapter IV, Section C: "Guidelines for Determining Acceptable Risk", and Chapter IV, Section N: "Policy for United Nations Minimum Operating Security Standards" (MOSS) are hereby abolished and replaced by the provisions of this policy.