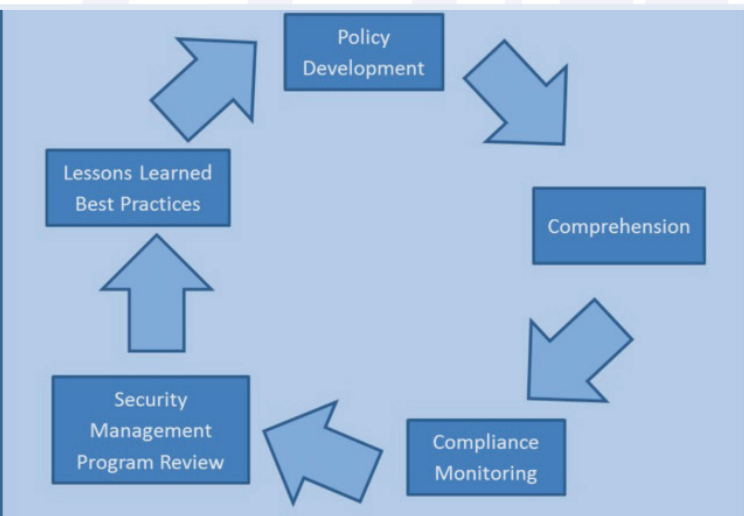


CHAPTER V

Compliance with Security Policies and Procedures



Section D

COMPLIANCE, EVALUATION AND BEST PRACTICES

A. Introduction:

1. The goal of the United Nations Security Management System (UNSMS) is to enable UN programmes and activities within acceptable levels of security risk. To achieve this goal, the UNSMS has established a robust set of policies, procedures and guidelines that lay the foundation for the management of security at the operational and managerial level. These policies, procedures and guidelines are implemented in country- and programme-specific contexts.
2. To ensure that the policies of the UNSMS remain robust and focused on ensuring the most effective security management programmes, the UNSMS has established a policy feedback loop meant to ensure that policy development is informed by best-practices and lessons learned that came from a review of our security management programmes and the monitoring of compliance status.
3. The Policy feedback loop comprises the following five elements (see Figure 1 below):
 - a. Policy Development
 - b. Comprehension
 - c. Compliance Monitoring
 - d. Security Management Programme Review
 - e. Lessons Learned / Best Practices

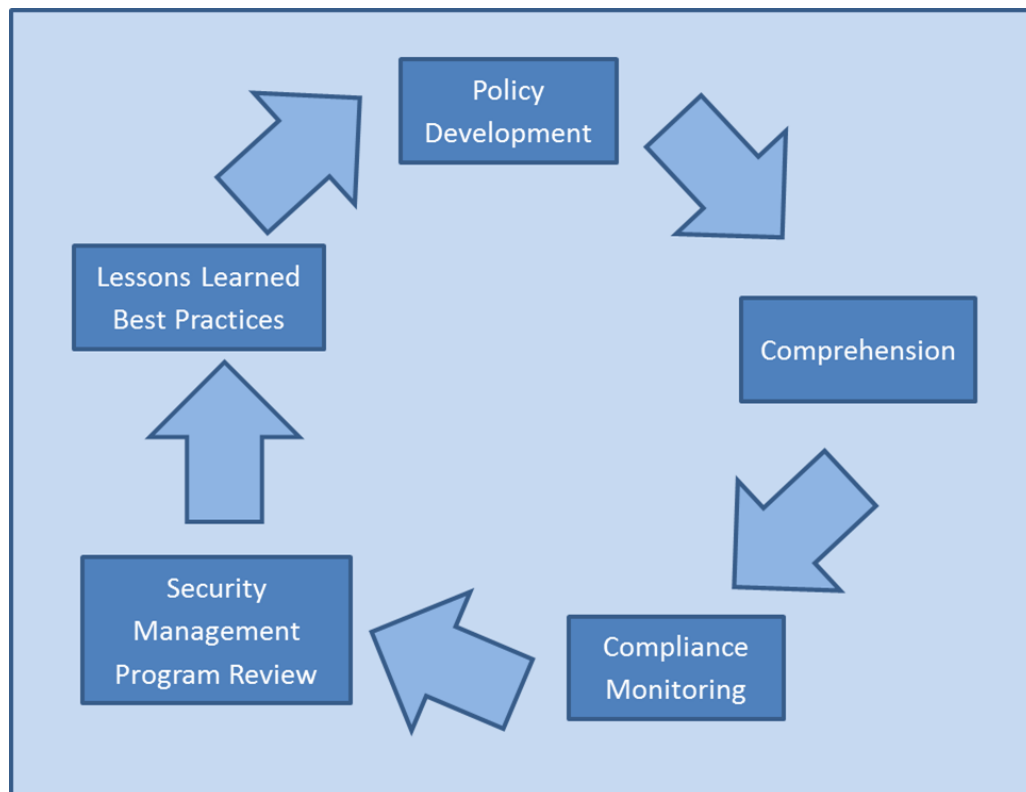


Figure 1

4. **Policy development** activities are undertaken by IASMN through the production, revision and updating of security policies and related tools. Once approved by HLCM, policies become applicable and binding within all UNSMS entities.
5. **Comprehension** of the policies are articulated through professional learning and development activities and other comprehension-building initiatives conducted by UNDSS and UNSMS entities. This element aims to facilitate the understanding and implementation of policies, communicate compliance standards, roles and responsibilities and motivate adherence.
6. The remainder of the elements from the policy feedback loop comprise the contents of this policy and are explained in detail below.

B. Purpose:

6. The purpose of this policy is to provide a common institutional framework for the elements of the policy feedback loop related to compliance monitoring, security management programme review and lessons learned/best practice, as well as the operational approach and arrangements to facilitate the implementation of the policy. Compliance monitoring and security management programme review are primarily meant to be proactive steps taken to identify and address security management-related issues before they occur.

C. Applicability:

7. The “Compliance, Evaluation and Best Practice policy” applies to UNDSS and all other UNSMS entities.

D. Definitions

8. For the purposes of this policy, the following definitions apply:
 - a. **Compliance:** Status of conformity and adherence to the policies, manuals, procedures and guidelines of the UNSMS.
 - b. **Compliance Monitoring** is a management tool that involves systematic oversight and collection of indicators of progress, or lack thereof, in implementing security risk management measures and security policies.
 - c. **Security Management Programme:** a set of activities aimed at ensuring the safety and security of UN personnel and assets for enabling UNSMS entities implementing their mandates.
 - d. **Lessons Identified:** Past events or actions that could develop into lessons learned if properly analyzed and actioned.
 - e. **Lessons Learned:** Learning, either positive or negative, drawn from Lessons Identified with a purpose of increasing the effectiveness and efficiency of particular activities by applying or avoiding them in future similar situations and which could

be developed into Best Practices. Lessons Identified only become Lessons Learned when they are properly actioned with a purpose of increasing the effectiveness and efficiency of similar activities.

- f. **Best Practices:** Process or procedure for performing an activity that has been applied and proven effective in at least one situation and could have applicability in another similar situation in future.

E. Policy Framework

9. The compliance monitoring and security management programme review functions ensure the effective and efficient implementation of security management policies and procedures, as part of the UNSMS efforts to enable the implementation of United Nations programmes and mandates, in as safe and secure a manner as possible.
10. Compliance monitoring is a regular part of the oversight and management of the security management programme. Monitoring the adherence to security policies, and of the implementation of Security Risk Management (SRM) measures and procedures (SRM Manual, Step 9, “Monitoring and Review”), through regular assessments and monitoring practices, are essential features to ensure the effectiveness of a security management programme.
11. Security management programme reviews focus on the results, design and implementation of the security management programme. Programme evaluation determines the relevance, performance, efficiency and impact of a security management programme.
12. Although distinct, compliance monitoring and security management programme reviews are mutually complementary. Evaluations, as a component of the Programme Review are based as much as possible on information acquired from monitoring activities. Compliance monitoring and security management programme reviews are used as a management tool, emphasizing accountability and compliance.
13. A sustained and expanding culture of accountability, transparency and quality improvement is a strategic vision of the UNSMS. Compliance monitoring and security management programme reviews are essential to accountability, learning and decision making.
14. Compliance monitoring and security management programme review play a key role in ensuring the UNSMS is a learning entity that develops and revises security management policies and procedures that are most effective for successful security management programmes on the ground.
15. Both activities allow for the identification of lessons learned and resultant best practices that shall be channeled in the process of developing and updating security policies.

F. Compliance Monitoring

16. Monitoring the implementation of SRM measures and adherence to security policies at the operational level is a proactive measure meant to ensure a safe environment for UN personnel and programme delivery (see SRM Manual, Step 9, “Monitoring and Review”)
17. Compliance with security management policies is a key requirement for the effective functioning of the UNSMS and its associated security management programmes. UNDSS and other UNSMS entities are responsible for monitoring their compliance with UNSMS policies and to take then necessary corrective action on incidences of non-compliance.
18. Compliance monitoring will consist of **general** and **specific/targeted** techniques that may include:
 - a. Self-assessment.
 - b. Peer reviews.
 - c. Continuous document reviews.
 - d. Compliance audits (as necessary).
19. **General Compliance Monitoring** will be conducted by UNDSS and UNSMS entities through the following tools:
 - a. UNDSS develops and maintains the procedures and issues the guidelines that govern both UNDSS centralized document reviews¹ at desk level and UNDSS decentralized in-country self-assessments.
 - b. UNSMS entities shall maintain their own internal compliance monitoring tools, informed by IASMN best practices.
20. **Specific/targeted Compliance Monitoring.** UNDSS and UNSMS entities shall retain the capacity of deploying compliance audits to address specific compliance-related challenges or instances of non-compliance. These audits shall complement the general compliance monitoring system as described in paragraph 19 above. Where audits are intended to review multiple UNSMS entities, USG UNDSS, as chairperson of the IASMN, shall determine the scope and composition of compliance audit teams, in consultation with applicable UNSMS entities, to achieve greater inclusivity and representation.
21. **Reporting and Corrective Actions** - When an UNSMS entity fails to meet a policy or SRM requirement, non-compliance exists. The DO shall report instances of non-compliance to the applicable UNSMS entity so that that entity can take corrective actions to prevent recurrence by eliminating the cause(s) of an existing non-compliance. The DO shall inform USG UNDSS on these instances for a follow up with the respective UNSMS entities

¹ The centralized document review is a formal examination of mandatory security documents and processes defined by UNSMS policies produced or maintained by the Senior Security Professional within the Designated Area, including, *inter alia*, Security Risk Management process, SSIRS, security plans, SMT minutes, etc. The purpose of the examination is to verify whether the documents and processes are in alignment with the policy requirements both in terms of formalities and content.

headquarters level. Reciprocally, UNSMS entities are also encouraged, through their respective headquarters security focal points, to inform the USG UNDSS of suspected non-compliance of UNDSS activities.

G. Security Management Programme Review

22. The security management program review encompasses preventive and *post facto* evaluation activities. Preventive activities include security programme evaluation and management reviews. The *post-facto* interventions consist of Board of Inquiries, other type of inquiries, and fact-finding mechanisms.

23. Preventive

- a. **Security Programme Evaluation** is a systematic and objective determination of the relevance and effectiveness of the UNSMS in the Designated Area. The evaluation function in UNDSS will be implemented through different types of evaluation activities that will be based on the needs that it serves and the level in which are applied. The programme evaluation function is guided by the norms and standards defined by the United Nations Evaluation Group².
- b. **Management Reviews**, including UNDSS Security Assistance Visits and interagency support missions, will address security management deficiencies that have come to the attention of UNDSS and/or UNSMS entities. These reviews are of a thematic nature and focus on a single or cross-cutting security management issue or activity. The review shall be conducted within the framework of current security policies and procedures and in accordance with the specific Terms of Reference

24. Post Facto

- a. **UNSMS Board of Inquiry.** As indicated in *Security Policy Manual*, Chapter V, Section G, a Board of Inquiry is an analytical and managerial tool to review investigation reports and record the facts of critical security incidents involving UNSMS entities, including whether the occurrence took place as a result of the acts or omissions of any individual(s). The purpose of a Board of Inquiry is to identify gaps or deficiencies in the application of UNSMS policy, procedures or guidelines, and to inform lessons learned.
- b. **Other Inquiries:** There may be other, *post facto*, inquiries by UNDSS or UNSMS entities, based on the internal procedures of respective UNSMS entities.

H. Lessons Learned and Best Practices

25. The purpose of Lessons Identified, Lessons Learned and Best Practices collected, synthesized and shared through a formalized process are aimed to:

² The United Nations Evaluation Group (UNEG) is an interagency professional network that brings together the evaluation units of the UN system, including UN Departments, specialized agencies, funds and programmes.

- a. Enable staff and partners in UNSMS entities to benefit from institutional memory and collective experience and expertise;
 - b. Ensure that the collective experience and institutional memory are reflected in system-wide policy and standards development;
 - c. Facilitate the transfer of knowledge and its efficient management;
 - d. Improve efficiency and productivity of the Department's security activities and those of the UNSMS.
26. Lessons Learned and resulting Best Practices will be shared and incorporated into designing, developing and implementing security policy and training where applicable
27. UNDSS will develop the procedure for establishing an enabling system and methodology for capturing, processing, disseminating and managing knowledge from Lessons Learned to Best Practices.

I. Roles and Responsibilities

28. UNDSS shall maintain procedures to review and assess the adherence with applicable security policies, including implementation of required SRM measures and procedures. (SRM Manual, Step 9, "Monitoring and Review")
29. UNDSS, as the custodian of the compliance monitoring and security management programme review function, shall coordinate and support the implementation of the policy.
30. UNDSS shall provide support to the development, design and implementation of UNSMS entities' self-evaluations when so requested.
31. UNDSS shall submit an annual report to the IASMN on the results and impact of the compliance monitoring and security management programme review functions. This report shall present a consolidated picture of results and a summary of cross-cutting issues and learning insights based on the activities undertaken during the reporting year.
32. The Security Focal Points for UNSMS entities, as per their internal accountability framework, will address gaps in implementing SRM measures and procedures to ensure action is taken to address non-compliance.
33. Designated Officials and Representatives/Heads of UNSMS entities at country level shall ensure that appropriate actions are taken to implement this policy.

J. Final Provisions

34. In implementing the compliance monitoring, evaluation and best practices policy, UNDSS shall work closely with other compliance and/or evaluation units of other United Nations entities and inter-agency and interdepartmental mechanism including the United Nations Evaluation Group.

35. UNDSS and the IASMN shall periodically review the implementation and effectiveness of this policy.
36. This Policy enters into force on 1 January 2019.