



INTERNAL AUDIT DIVISION

REPORT 2023/078

Audit of the compliance function in the Department of Safety and Security

The Department needed to document a conceptual framework for compliance monitoring and reporting taking into account its existing mechanisms and clearly defining roles and responsibilities for accountability

20 December 2023

Assignment No. AP2023-500-01

Audit of the compliance function in the Department of Safety and Security

EXECUTIVE SUMMARY

The Office of Internal Oversight Services (OIOS) conducted an audit of the compliance function in the Department of Safety and Security (DSS). The objective of the audit was to assess the effectiveness and efficiency of the design of the DSS compliance function regarding its oversight role in the United Nations security management system (UNSMS). The audit focused on: (a) governance and oversight framework; (b) compliance monitoring mechanisms; and (c) compliance reporting.

Overall, the Department needed to document a conceptual framework for compliance monitoring and reporting taking into account its existing mechanisms and clearly defining roles and responsibilities for accountability. The lack of such a framework prevented DSS from collecting, analyzing and consistently reporting on compliance exceptions. Additionally, the work plans of the Compliance, Evaluation and Monitoring Section (CEMS) in DSS, with responsibility for coordinating and monitoring the implementation of standard security policies and procedures, were not sufficiently detailed to cover all the areas stipulated in its mandate. DSS had also not dedicated adequate resources to CEMS for effective delivery of its mandate.

OIOS made nine recommendations. To address issues identified in the audit, DSS needed to:

- Facilitate the development of an overarching conceptual framework for compliance monitoring, evaluation and reporting on security policy standards by UNSMS organizations, for adoption by the Inter-Agency Security Management Network (IASMN);
- Submit the IASMN-adopted overarching conceptual framework to the Chief Executive Board's High-Level Committee on Management to guide United Nations security management system organizations to adopt the framework and to periodically certify their compliance to it;
- Include status updates on compliance and monitoring of UNSMS policies and procedures as a standing agenda item during IASMN plenary sessions;
- Establish annual work plans for CEMS that detail all mandated tasks to outline how implementation and monitoring would be achieved, including tracking progress made against mandated tasks;
- Dedicate adequate capacity and expertise to its compliance and monitoring function within its existing resources to effectively deliver its mandate;
- Strengthen the implementation of the policy on compliance monitoring by clarifying the mandatory minimum components to be included in decentralized compliance reviews and documenting the supporting guidelines, including on monitoring alternatives;
- Prepare annual reports on its compliance monitoring activities and results and present them to IASMN for corrective action as required by the security policy manual;
- Develop an action plan to address the challenges identified in the policy implementation assessment to strengthen controls over compliance with standard security policies and procedures; and
- Include mandatory training targets and compliance rates against them by UNSMS security personnel/officials in reports to IASMN.

DSS accepted seven recommendations and partially accepted two. It had initiated actions to implement the accepted recommendations.

CONTENTS

I. BACKGROUND	1-2
II. AUDIT OBJECTIVE, SCOPE AND METHODOLOGY	2-3
III. AUDIT RESULTS	3-10
A. Governance and oversight framework	3-6
B. Compliance to security policies and monitoring	6-7
C. Compliance reporting	7-10
IV. ACKNOWLEDGEMENT	10
ANNEX I	Status of audit recommendations
APPENDIX I	Management response

Audit of the compliance function in the Department of Safety and Security

I. BACKGROUND

1. The Office of Internal Oversight Services (OIOS) conducted an audit of the compliance function in the Department of Safety and Security (DSS) based at United Nations Headquarters in New York.
2. By its resolution 59/276, dated 23 December 2004, the General Assembly established DSS to provide leadership, operational support and oversight of the United Nations security management system (UNSMS). The Secretary-General's bulletin ST/SGB/2013/5 on the organization of DSS defined its core functions to include:
 - a) Provide leadership of operational support to and oversight of UNSMS;
 - b) Provide leadership, strategic guidance and an integrated coordination framework to enable the conduct of United Nations activities;
 - c) Provide security expertise to all UNSMS entities and lead cooperation and collaboration among these entities;
 - d) Lead the development across UNSMS entities of standardized security policies and procedures under the umbrella of the Inter-Agency Security Management Network (IASMN); and
 - e) Deliver integrated, efficient and coherent security support to United Nations field operations.
3. According to A/77/6 (Sect. 34), proposed programme budget, dated April 2022, DSS provided support to approximately 180,000 personnel and 400,000 of their dependants in more than 125 countries and thus, played a crucial role in enabling UNSMS member organizations to execute their programmes worldwide, including at Headquarters, offices away from Headquarters, field missions, funds, programmes and specialized agencies, and other inter-governmental organizations.
4. UNSMS organizations conform to standard policies and procedures related to the security of personnel, premises, assets, and operations. The goal of UNSMS is to enable UNSMS organizations to conduct their activities within acceptable levels of security risk. Its governance mechanism includes:
 - a) IASMN, consisting of senior managers who have oversight of security functions within each member organization of UNSMS. IASMN reviews existing and proposed policies, procedures and practices of UNSMS and their implementation, and provides recommendations on these to the High-Level Committee on Management (HLCM) of the United Nations System Chief Executives Board for Coordination (CEB);
 - b) HLCM, which has as a standing item on its agenda a comprehensive review of policies and resource-related issues pertaining to the entire UNSMS. HLCM reviews the recommendations made by IASMN and either decides on them directly or recommends their endorsement and implementation to CEB, which is chaired by the Secretary-General; and
 - c) The Secretary-General, who has delegated to the Under-Secretary-General (USG) for DSS (USG DSS) the authority to make executive decisions on UNSMS-related matters for the United Nations. USG DSS leads and coordinates UNSMS at both Headquarters and field locations, represents the Secretary-General on all UNSMS-related matters and serves as the Chair of IASMN.
5. The responsibilities of USG DSS further include: (a) developing UNSMS policies, practices and procedures; (b) coordinating with UNSMS organizations to ensure compliance with and support for security

aspects of their activities; and (c) preparing relevant reports of the Secretary-General and advising the Secretary-General on all UNSMS-related matters.

6. For the year 2023, DSS' resource requirements totaled \$141.63 million. These resources are provided from three funding streams: (a) regular budget \$124.54 million; (b) other assessed budget \$4.03 million; and (c) estimated extra-budgetary funding \$13.06 million. DSS activities are also funded through the jointly funded activities (JFA) stream, which amounted to \$163.32 million in 2023.

7. To further DSS' mandate, the compliance, evaluation and monitoring function was established in 2006 to plan, coordinate and monitor the implementation of standard security policies and procedures throughout the UNSMS organizations in close coordination with them. It was intended that this would be accomplished by monitoring and integrated and coordinated field compliance missions.

8. As of April 2023, the Compliance, Evaluation and Monitoring Section (CEMS) within the Strategic Planning Service (SPS), Office of the Under-Secretary-General (OUSG) was headed at the P-5 level. In addition to the P-5 post, the Section comprised three posts, one at the P-4 level and two at the P-3 level. CEMS received its resources from the regular budget, other assessed budget and JFA. In addition to CEMS, the Division of Regional Operations (DRO) in DSS conducts compliance and monitoring functions via its regional desks. DRO is responsible for the management of regional operations for safety and security and serves as the safety and security focal point for field duty stations, providing primary operational and technical support.

9. Comments provided by DSS are incorporated in italics.

II. AUDIT OBJECTIVE, SCOPE AND METHODOLOGY

10. The objective of the audit was to assess the effectiveness and efficiency of the design of the DSS compliance function regarding its UNSMS oversight role.

11. The audit was conducted from June to October 2023 in New York. Based on an activity-level risk assessment, the audit scope covered higher and medium risk areas in the design of the UNSMS compliance and monitoring function within the UNSMS security policy framework. The audit focused on: (a) governance and oversight framework; (b) compliance monitoring mechanisms; and (c) compliance reporting.

12. The audit methodology included: (a) review and analyses of relevant policies, guidelines and reports; (b) discussions and interviews with DSS and other concerned officials; and (c) analytical reviews, walk-throughs and sample testing of key controls.

13. The audit was conducted in accordance with the International Standards for the Professional Practice of Internal Auditing.

III. AUDIT RESULTS

A. Governance and oversight framework

There was a need for DSS to revise the framework for compliance function

14. Compliance with the UNSMS security policy framework is a shared responsibility among the various UNSMS organizations. Nevertheless, it was critical that DSS establish an effective compliance, evaluation and monitoring mechanism to fulfill its mandated oversight role of: (a) issuing standardized security management policies; (b) periodically evaluating and updating them for continued relevance and effectiveness; and (c) monitoring compliance of the policies and standards throughout UNSMS.

15. UNSMS' policy on compliance, evaluation and best practice, a part of the Security Policy Manual (SPM), entered into force on 1 January 2019, stipulating DSS's role as custodian of the UNSMS compliance monitoring function and being responsible for coordinating and supporting the implementation of the policy. According to the policy, the UNSMS compliance management system consists of general compliance components comprising (a) DSS centralized document review and decentralized in-country reviews and (b) UNSMS organizations own monitoring mechanisms; and specific compliance monitoring. The policy further requires DSS to develop and maintain the procedures and issue the guidelines that govern general DSS compliance monitoring.

16. Regarding compliance monitoring reporting, the SPM stipulated the reporting of ad-hoc non-compliance incidents to the respective entities as well as to the USG DSS and encouraged the reporting of suspected non-compliance with DSS guidelines to the USG DSS. It further specified that an annual report on the results and impact of the compliance monitoring and security management programme review functions was to be submitted to IASMN. Furthermore, as per the SPM, senior security managers of UNSMS organizations were to report on their organization's compliance with UNSMS policies, procedures and Security Risk Management (SRM) measures.

17. The division of labour and allocation of responsibilities for entity compliance with UNSMS policies (including DSS' role in providing oversight over compliance) were also articulated in the SPM. Therefore, the audit determined that the compliance monitoring mandate of DSS as defined had been articulated to the UNSMS organizations.

18. However, its implementation was impeded by the following:

- a) CEMS did not have an overview of the monitoring mechanisms that UNSMS organizations had in place. Systematic interactions between CEMS, DRO and UNSMS member organizations including security advisers on UNSMS compliance management matters did not take place.
- b) CEMS did not have visibility of the tools developed and used by member organizations for compliance monitoring. Also, no standardized process was in place for member organizations to submit their monitoring results to CEMS. This impaired CEMS' role as custodian of the UNSMS compliance management system, thereby weakening the oversight role of DSS.
- c) CEMS's role regarding general and specific compliance monitoring was not defined. Also, any exceptions noted from such exercises were not being communicated to CEMS under the current system of policies.

19. Considering the broad setup of the UNSMS with over 50 members, some with reporting lines within the Secretariat to the Secretary-General and other non-Secretariat entities, the lack of an overarching compliance framework inclusive of centralized and decentralized mechanisms with defined end-users of reporting prevented CEMS from collecting, analyzing and consistently reporting on compliance exceptions. Given the importance of the safety and security of United Nations personnel and assets in the Organization's global operations, it is important that HLCM instruct UNSMS organizations to facilitate the DSS evaluation, monitoring and reporting role to ensure application of standard security policies and procedures throughout the UNSMS organizations.

20. This would reinforce the UNSMS organizations' shared responsibility for the safety and security of United Nations personnel and assets. It would, however, require DSS to propose an overarching conceptual framework for compliance monitoring, evaluation and reporting on standard security policy standards throughout UNSMS and table the framework for adoption at the IASMN. The framework needed to: (a) specify the roles of CEMS, DRO, security advisers as well as those of UNSMS members' own monitoring mechanisms; (b) define compliance objectives, roles and shared safety and security responsibilities; and (c) clarify the supporting guidelines regarding operationalization of the framework, including the definition of reporting requirements to CEMS and to senior management and governing bodies.

(1) To complement and strengthen the current United Nations security management system (UNSMS) policy on compliance monitoring, DSS should facilitate the development of an overarching conceptual framework for compliance monitoring and reporting on security policy standards by UNSMS organizations, for adoption by the Inter-Agency Security Management Network.

DSS accepted recommendation 1.

(2) The USG DSS should, as chair of the Inter-Agency Security Management Network (IASMN), submit the IASMN-adopted overarching conceptual framework for compliance monitoring, evaluation and reporting on standard security policies and procedures to the Chief Executive Board's High-Level Committee on Management to guide United Nations security management system organizations to adopt the framework and to periodically certify their compliance to it.

DSS accepted recommendation 2.

IASMN plenary sessions needed to include compliance as a standing agenda item

21. The IASMN Steering Group (IASMN SG) meets twice a year, generally in May and November, to facilitate the work of the IASMN. A review of the IASMN SG agendas from 2019 through 2023 noted that they deliberated on updates on various initiatives, as well as progress on implementing IASMN recommendations, including those on working methods, policy, budget, communications systems, residential security and gender.

22. Meeting minutes indicated that IASMN SG also covered UNSMS priorities such as strengthening compliance, oversight, lessons learned and best practices in their May and November 2022 and May 2023 sessions. According to the April 2019 IASMN SG meeting minutes, DSS was to present an annual report to the IASMN on the implementation and compliance with security policies in the designated areas. The status update was marked as complete; however, IASMN SG review of annual compliance reports on the implementation of security policies was last documented in 2012.

23. In addition, the IASMN plenary sessions met twice a year, typically in January and June. From 2019 through 2023, they reviewed and made recommendations on topics such as strengthened compliance, oversight and lessons learned. This included a review of a report titled, ‘Lessons Learned on the UNSMS response during the 2021 Afghan Crisis’ in the November 2022 SG session. The lessons learned exercise had been conducted between July and October 2022 by an inter-agency team comprising UNSMS representatives and led by an independent consultant. The report made 18 recommendations.

24. In June 2023, DRO issued a communication detailing improvement to the SRM and the Safety and Security Information Recording System (SSIRS), including the UNSMIN¹ SRM website, which had been updated with training courses and tutorials. DSS had considered procuring software to track the recommendations arising from DSS evaluations and lessons learned but as the cost was too high, it was now considering developing an internal tracking tool to monitor these recommendations.

25. As above, while UNSMS’ compliance and monitoring was repeatedly listed as a priority area, it was not included as a standing agenda item at either the IASMN SG or the plenary IASMN sessions. Deviations from the UNSMS framework of policies and procedures were not being discussed as a standing item. Given the importance of compliance and monitoring to UNSMS policies and procedures, this needed to be included as a discussion point in at least one of the IASMN plenary sessions.

(3) The USG DSS should, as chair of the Inter-Agency Security Management Network (IASMN), include status updates on compliance and monitoring of United Nations security management system policies and procedures as a standing agenda item during IASMN plenary sessions

DSS accepted recommendation 3 and stated that this reporting would follow IASMN adoption of the overarching conceptual framework by the end of 2024.

CEMS mandated tasks needed to be translated into work plans, ensuring there is adequate capacity and expertise to deliver its compliance monitoring mandate

26. CEMS prepared work plans but the plans did not include details regarding the timing, priority and responsibility for relevant activities, and applicable monitoring mechanisms. For example, the 2022 work plan listed the goal of strengthening and professionalizing the evaluation function within the Department. Related actions included revising and drafting a stand-alone evaluation policy, and success criteria was that all evaluations were to be managed and/or conducted in accordance with the plan. However, as the plan did not include assigned individuals and timelines, there was lack of clarity regarding the timeframes within which the tasks were to be implemented.

27. The 2023 CEMS workplan listed four evaluations (started in 2022), one lessons learned exercise, three new evaluations and an exercise for a new compliance framework for 2023. However, the work plan did not provide details regarding UNSMS compliance and monitoring, e.g., centralized document reviews at Headquarters, including CEMS’ associated tasks of being the custodian of the compliance function. Furthermore, CEMS did not note progress or completion made against the tasks detailed in the workplans.

28. DSS stated that this was because CEMS staffing had fluctuated over the years. For instance, in 2021, CEMS was staffed by one individual. By the end of 2022, there were four staff members, but in 2023, of the four staff members, one was on sabbatical leave, and one on temporary assignment to a field mission. Being at half capacity, CEMS was of the opinion that tracking progress against the workplan was not an

¹ United Nations Security Managers Information Network

accurate representation of progress made. OIOS notes that supplementary resources were not provided to mitigate the staffing fluctuation. Furthermore, given the focus on evaluations, lessons learned and best practices, there was a need to strengthen the dedicated DSS compliance and monitoring capacity.

- (4) DSS should establish annual work plans for the Compliance Evaluation Monitoring Section that detail all mandated tasks to outline how implementation and monitoring would be achieved, including tracking progress made against mandated tasks.**

DSS accepted recommendation 4.

- (5) DSS should dedicate adequate capacity and expertise to its compliance and monitoring function within its existing resources to effectively deliver its mandate.**

DSS accepted recommendation 5 and stated that the USG proposal to the Fifth Committee included an additional P2 post for CEMS.

B. Compliance to security policies and monitoring

DSS documented policy and operational level guidelines on desk reviews

29. The SPM defined compliance monitoring as systematic oversight and indicator collection. In the UNSMS policy, it is the third element in the feedback loop, following policy development and comprehension and preceding security management programme review, lessons learned and best practices.

30. The SPM section on compliance, evaluation and best practices, in effect since January 2019, and the SRM manual, revised March 2019, represent the central guidelines on compliance monitoring procedures in the UNSMS.

31. Centralized desk reviews, decentralized in-country assessments, and UNSMS entities' own monitoring tools constitute general compliance monitoring as per the SPM, which could be complemented by specific compliance monitoring, e.g., compliance audits, on an as-needed basis.

DSS documented policy and operational level guidelines on desk reviews

32. Centralized document review is a formal examination of mandatory security documents and processes defined by UNSMS policies, such as the SRM process, SSIRS, security plans and security management team (SMT) minutes produced or maintained by the senior security professional within the designated area. The purpose of the review is to verify whether the documents and processes are in alignment with the policy requirements both in terms of formalities and content.

33. In addition to the above, supporting guidelines elaborating provisions on the monitoring requirements, such as standard operating procedures, DSS DRO desk officers' terms of reference, technical manuals, for example, the SSIRS user manual and the guidelines on the use of the electronic travel advisory, as well as templates for compliance reviews (e.g., for compliance with residential security measures) had been documented.

34. Interviews with DSS security officers, both at Headquarters and the field, as well as reviews of supporting documentation, such as policies (e.g., SPM), manuals (e.g., Security Management Operations Manual and SRM Manual), and results of entity desktop reviews (e.g., monthly DRO Security Plan and SRM reviews), showed that the guidelines governing centralized desk reviews were adequate and that the

defined reviews were conducted as stipulated, and the DSS DRO desk officers followed up with field entities on matters of non-compliance with UNSMS or identified optimization potential. For example, in May 2023 DRO desk officers followed up with five countries in high risk conditions that had expired security plans and highlighted the need for SRM finalizations for the African region.

DSS needed to strengthen guidelines on decentralized monitoring components and monitoring alternatives

35. Discussions with security advisers in the field and DSS personnel at Headquarters showed that decentralized compliance assessments in the fields generally did not follow a standardized approach, and thus, were not comparable across designated areas. In the absence of a centrally defined standard or minimum requirement, security advisers created compliance checklists for their specific designated areas, covering for example, physical checks of implemented security requirements of United Nations common premises. While the need for adaptations and flexibility could be justified by different security risk profiles across geographical areas, the lack of defined mandatory minimum components of decentralized compliance monitoring posed the risk of significantly deviating interpretations across areas, and thus, could not assure a certain minimum standard to be covered by such reviews. A major exception to this were compliance reviews for residential security measures (RSM), which included a decentralized monitoring component, and for which comprehensive guidelines were documented.

36. DSS DRO security assistance visits constituted another decentralized monitoring mechanism. Security assistance visits were comprehensive field visits aimed at reviewing, inter alia, the local SRM strategies, the local United Nations integrated security structure and its capacity to provide security advisories, analyses, training, and emergency response support, and to assess the implementation of SRM measures that were recommended by earlier missions.

37. Security assistance visits, however, did not follow a standardized methodology and were generally not comparable across geographical areas and duty stations. The scope of the visits could vary according to local circumstances, requirements and exigences. Also, security assistance visits did not follow a set schedule but were planned as needed, e.g., after a security crisis to evaluate preparedness for future situations. According to interviews with DSS personnel, DSS DRO security assistance visits represented spot checks, defined in the SPM as an alternative monitoring mechanism.

38. The SPM and the SRM manual listed monitoring alternatives (self-assessments, peer reviews, document reviews, compliance audits, spot checks, surveys, and external monitoring) based on needs, but lacked clarity on their scope, criticality, and timing.

(6) DSS should strengthen the implementation of the policy on compliance monitoring by clarifying the mandatory minimum components to be included in decentralized compliance reviews and documenting the supporting guidelines, including on monitoring alternatives.

DSS accepted recommendation 6.

C. Compliance reporting

DRO generated various operational reports on implementation of UNSMS security requirements

39. DSS DRO drafted several operational reports on the implementation of security requirements of UNSMS. These reports were communicated within DSS DRO and included, inter alia, (a) standardized monthly reports on the status updates of SRMs and security plans incorporating a list of DSS DRO regional sections and the number of assigned designated areas; (b) number of expired SRMs/security plans and the

rate of compliance with the requirement for up to date SRMs/security plans; and (c) annual reports on RSM requirements, including a statement of countries with RSMs, the measures in place and the costs.

40. Overall, the approach to reporting compliance monitoring results in DSS focused on immediate or ad-hoc reporting of cases of non-compliance to senior management, aiming to initiate remedial action without delay.

DSS needed to submit annual reports to IASMN on its compliance monitoring activities

41. Systematic and regular reporting of compliance at managerial and governing body level over standard security policies and procedures is necessary to identify emerging risks within the compliance discipline of the UNSMS and to initiate systematic mitigating measures. This would complement immediate ad-hoc reporting, aimed to initiate remedial action without delay.

42. The SPM chapter on compliance, evaluation and best practices includes the following high-level provisions on the reporting of compliance monitoring results within the UNSMS.

- a) The Designated Official (DO) to report instances of non-compliance to the applicable UNSMS organization for corrective actions to prevent recurrence and to USG DSS for follow-up with the respective UNSMS organization at Headquarters level; and
- b) DSS to submit an annual report to IASMN on the results and impact of the compliance monitoring and security management programme review (evaluation) 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.

43. While the first provision is aimed at taking instant corrective action, the annual report would 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. The last annual compliance reports submitted to IASMN by DSS was in 2012. Since then, annual compliance reports have not been presented during the IASMN SG or plenary sessions. Given that compliance monitoring is a priority and is relevant to remedy issues of non-compliance and to develop a progressive implementation plan to address outstanding issues, DSS needed to document and present to IASMN annual reports on compliance monitoring and its results.

44. The absence of a documented overarching compliance reporting framework or process to guide the drafting of annual consolidated reports DSS impaired the preparation such reports and thus DSS oversight function.

(7) DSS should prepare annual reports on its compliance monitoring activities and results and present them to the Inter-Agency Security Management Network for corrective action as required by the security policy manual.

DSS accepted recommendation 7 and stated that this reporting would follow the adoption by IASMN of the overarching conceptual framework by the end of 2024.

DSS needed to develop an action plan to address the challenges identified in the policy implementation assessment

45. In June 2020, DSS launched a policy implementation assessment. Its purpose was to provide a picture of the status of implementation of 27 selected UNSMS policies that are a part of the SPM. Among others, the security policies covered in the assessment included: (a) relations with host countries on security

issues; (b) SRM; (c) security planning; (d) security of United Nations premises; (e) close protection operations; (f) armed private security companies; and (g) fire safety. The assessment was carried out via a survey, which comprised 118 questions, distributed among 150 security recipients in five geographic locations reflecting key requirements for each selected policy

46. Overall results of the policy implementation assessment indicated that the status of implementation of the 27 assessed security policies either met or approached the requirements. There was, however, a consensus among the respondents on the following challenges:

- a) The need for a compliance monitoring and reporting mechanism;
- b) Paramountcy of agencies, funds and programmes management commitment;
- c) Limited financial and human resources;
- d) Lack of adequate arrangement for DSS representation with the host government;
- e) Excessive number of policies and delays in updating them; and
- f) Overwhelming and bureaucratic SRM process

47. Further, Annex 2 of the assessment report titled, ‘Challenges in implementing UNSMS policies,’ listed 37 challenges in implementing UNSMS policies by the assessment respondents. Some of these included the following:

- a) The policies continue to be a guide;
- b) The current policies were core to the work in the field but monitoring their levels of compliance and ensuring follow-up actions with a progressive implementation plan was an absolute necessity to ensure full compliance;
- c) The DSS organizational culture requiring its officials and security operations to ensure client satisfaction empowered senior clients to threaten concerned DSS officials to weaken recommendations regarding non-compliance issues or be replaced. This was harming the integrity of DSS officials and undermining the implementation of standard security policies and procedures; and
- d) There was no mechanism to address non-compliance with UNSMS policies.

48. While the results of the assessment were shared with IASMN, DSS had not prepared an action plan to address the identified challenges Accordingly, there was no reporting on the progress in its implementation.

(8) DSS should develop an action plan to address the challenges identified in the policy implementation assessment to strengthen controls over compliance with standard security policies and procedures.

DSS partially accepted recommendation 8 and stated that the challenges identified in the 2020 policy implementation assessment would inform the development of the overarching compliance framework rather than a separate action plan.

DSS needed to include mandatory training targets and related compliance rates by UNSMS security positions/officials in reporting to IASMN

49. DSS reports on security training for 2018 to 2020 indicated that security training was provided to three target audiences: (a) UNSMS organizations personnel; (b) managers with security responsibilities,

including DOs and SMT members; and (c) security personnel and other members of the integrated security workforce. The training included the basic security awareness course (BSAFE), attended by 443,520 personnel from 2018 to 2020. Additional training courses included the safe and secure approaches to field environments (SSAFE), women’s security awareness training and individual first aid kit training. The training courses delivered to managers with security responsibilities included: (a) Headquarters DO briefings organized by the DRO; and (b) local in-person briefings conducted by the principal and chief security advisers and the mandatory SMT online training. Also, training courses delivered to security personnel and other members of the workforce included: (a) SRM online for security professionals; (b) security certification programme; and (c) physical security in-person training.

50. In 2021, the delivery of security-related training for UNSMS personnel continued to be impacted by the pandemic. During the same year, demand for psychosocial support and resilience-building training remained high, and online security training continued to be the main source of training. Additionally, in 2021, field trainers requested support from Headquarters to ensure they were delivering high-quality training in accordance with standards. In response, the DSS Training and Development Section created a series of videos for field trainers to support them in implementing new modules and to demonstrate participatory approaches. These modules included: (a) introduction and context; (b) threats; (c) personal vulnerabilities; and (d) risk reduction.

51. With the easing of the pandemic, DSS resumed in-person training to accommodate more participants. In 2022, training delivered included: (a) SSAFE; (b) field security associates training programme; (c) security certification programme; (d) physical security training; and (e) revised close protection officer certification. The audit determined that DSS had delivered relevant training to security personnel and issued comprehensive training reports.

52. However, the DSS training reports included only the numbers of staff completing DSS training. Except for the BSAFE training, no mandatory training targets were available. The lack of these impeded the calculation of training compliance ratios. While absolute numbers provide a suitable overview of the magnitude and relevance of specific training courses, ratios are essential to monitor developments in required completion of mandatory courses over a period of time.

(9) DSS should include mandatory training targets and compliance rates against them by United Nations security management system security personnel/officials in reports to the Inter-Agency Security Management Network.

DSS partially accepted recommendation 9 and stated that its implementation would be restricted to compliance rates by DSS personnel for internal reporting only (as well as reporting to relevant United Nations departments or bodies). However, as DSS-provided training included other audiences, its reporting on training activities needed to incorporate them as well.

IV. ACKNOWLEDGEMENT

53. OIOS wishes to express its appreciation to the management and staff of DSS for the assistance and cooperation extended to the auditors during this assignment.

Internal Audit Division
Office of Internal Oversight Services

STATUS OF AUDIT RECOMMENDATIONS

Audit of the compliance function in the Department of Safety and Security

Rec. no.	Recommendation	Critical ² / Important ³	C/ O ⁴	Actions needed to close recommendation	Implementation date ⁵
1	To complement and strengthen the current United Nations security management system (UNSMS) policy on compliance monitoring, DSS should facilitate the development of an overarching conceptual framework for compliance monitoring and reporting on security policy standards by UNSMS organizations, for adoption by the Inter-Agency Security Management Network.	Important	O	Receipt of the overarching conceptual framework for compliance monitoring and reporting on security policy standards by UNSMS organizations.	31 March 2025
2	The USG DSS should, as chair of the Inter-Agency Security Management Network (IASMN), submit the IASMN-adopted overarching conceptual framework for compliance monitoring, evaluation and reporting on standard security policies and procedures to the Chief Executive Board's High-Level Committee on Management to guide United Nations security management system organizations to adopt the framework and to periodically certify their compliance to it.	Important	O	Receipt of documentation evidencing DSS' submission of the IASMN-adopted overarching conceptual framework to HLCM to guide UNSMS organizations to adopt the framework and to certify their compliance to it.	31 March 2025
3	The USG DSS should, as chair of the Inter-Agency Security Management Network (IASMN), include status updates on compliance and monitoring of United Nations security management system policies and procedures as a standing agenda item during the IASMN plenary sessions.	Important	O	Receipt of documentation evidencing inclusion of status updates on compliance and monitoring of security management system policies and procedures as an agenda item during IASMN plenary sessions.	31 December 2025

² Critical recommendations address those risk issues that require immediate management attention. Failure to take action could have a critical or significant adverse impact on the Organization.

³ Important recommendations address those risk issues that require timely management attention. Failure to take action could have a high or moderate adverse impact on the Organization.

⁴ Please note the value C denotes closed recommendations whereas O refers to open recommendations.

⁵ Date provided by DSS in response to recommendations.

STATUS OF AUDIT RECOMMENDATIONS

Audit of the compliance function in the Department of Safety and Security

Rec. no.	Recommendation	Critical ² / Important ³	C/ O ⁴	Actions needed to close recommendation	Implementation date ⁵
4	DSS should establish annual work plans for the Compliance Evaluation Monitoring Section that detail all mandated tasks to outline how implementation and monitoring would be achieved, including tracking progress made against mandated tasks.	Important	O	Receipt of CEMS work plans detailing all mandated tasks, including tracking progress against mandated tasks.	31 March 2024
5	DSS should dedicate adequate capacity and expertise to its compliance and monitoring function within its existing resources to effectively deliver its mandate.	Important	O	Receipt of evidence that adequate capacity and expertise is dedicated to DSS' compliance and monitoring function.	30 June 2024
6	DSS should strengthen implementation of the policy on compliance monitoring by clarifying the mandatory minimum components to be included in decentralized compliance reviews and documenting the supporting guidelines, including on monitoring alternatives.	Important	O	Receipt of updated policy on compliance monitoring clarifying the mandatory minimum components to be included in the decentralized compliance reviews and documenting the supporting guidelines, including on monitoring alternatives.	31 March 2025
7	DSS should prepare annual reports on its compliance monitoring activities and results and present them to the Inter-Agency Security Management Network for corrective action as required by the security policy manual.	Important	O	Receipt of the first annual report on DSS compliance monitoring activities presented to IASMN for corrective action as required.	31 December 2025
8	DSS should develop an action plan to address the challenges identified in the policy implementation assessment to strengthen controls over compliance with standard security policies and procedures.	Important	O	Receipt of the overarching compliance framework incorporating measures to address the challenges identified in the policy implementation assessment.	31 December 2024
9	DSS should include mandatory training targets and compliance rates against them by United Nations security management system security personnel/officials in reports to the Inter-Agency Security Management Network.	Important	O	Receipt of the first report to IASMN incorporating mandatory training targets and compliance rates against them by United Nations security management system security personnel/officials.	31 December 2024

APPENDIX I

Management Response

Management Response

Audit of the compliance function in the Department of Safety and Security

Rec. no.	Recommendation	Critical ¹ / Important ²	Accepted? (Yes/No)	Title of responsible individual	Implementation date	Client comments
1	To complement and strengthen the current United Nations security management system (UNSMS) policy on compliance monitoring, DSS should facilitate the development of an overarching conceptual framework for compliance monitoring and reporting on security policy standards by UNSMS organizations, for adoption by the Inter-Agency Security Management Network.	Important	Yes	CEMS/SPS	First quarter of 2025	
2	The USG DSS should, as chair of the Inter-Agency Security Management Network (IASMN), submit the IASMN-adopted overarching conceptual framework for compliance monitoring, evaluation and reporting on standard security policies and procedures to the Chief Executive Board's High-Level Committee on Management to guide United Nations security management system organizations to adopt the framework and to periodically certify their compliance to it.	Important	Yes	USG UNDSS	First quarter of 2025	
3	The USG DSS should, as chair of the Inter-Agency Security Management Network (IASMN), include status updates on compliance and monitoring of United Nations security management system policies and procedures as a standing	Important	Yes	USG UNDSS	2025 onwards	This reporting would follow the adoption by the IASMN of the overarching conceptual framework by the end of 2024

¹ Critical recommendations address those risk issues that require immediate management attention. Failure to take action could have a critical or significant adverse impact on the Organization.

² Important recommendations address those risk issues that require timely management attention. Failure to take action could have a high or moderate adverse impact on the Organization.

Management Response

Audit of the compliance function in the Department of Safety and Security

Rec. no.	Recommendation	Critical ¹ / Important ²	Accepted? (Yes/No)	Title of responsible individual	Implementation date	Client comments
	agenda item during the IASMN plenary sessions.					
4	DSS should establish annual work plans for the Compliance Evaluation Monitoring Section that detail all mandated tasks to outline how implementation and monitoring would be achieved, including tracking progress made against mandated tasks.	Important	Yes	SPS	March 2024	
5	DSS should dedicate adequate capacity and expertise to its compliance and monitoring function within its existing resources to effectively deliver its mandate.	Important	Yes	SPS	June 2024	The USG proposal to the 5 th Committee includes an additional post for CEMS (P2)
6	DSS should strengthen the implementation of the policy on compliance monitoring by clarifying the mandatory minimum components to be included in decentralized compliance reviews and documenting the supporting guidelines, including on monitoring alternatives.	Important	Yes	SPS and DRO	First quarter of 2025	
7	DSS should prepare annual reports on its compliance monitoring activities and results and present them to the Inter-Agency Security Management Network for corrective action as required by the security policy manual.	Important	Yes	CEMS	2025 onwards	This reporting would follow the adoption by the IASMN of the overarching conceptual framework by the end of 2024
8	DSS should develop an action plan to address the challenges identified in the policy implementation assessment to strengthen controls over compliance with standard security policies and procedures.	Important	Partially	DRO and SPS	December 2024	The challenges identified in the 2020 policy implementation assessment will inform the development of the overarching compliance framework rather than a separate action plan.
9	DSS should include mandatory training targets and compliance rates against them by United Nations security management	Important	Partially	TDS	December 2024	This recommendation should be restricted to compliance rates by UNDSS personnel and for internal

Management Response

Audit of the compliance function in the Department of Safety and Security

Rec. no.	Recommendation	Critical ¹ / Important ²	Accepted? (Yes/No)	Title of responsible individual	Implementation date	Client comments
	system security personnel/ officials in reports to the Inter-Agency Security Management Network.					reporting only (as well as reporting to relevant UN departments or bodies)