SAVING LIVES
CHANGING LIVES

Internal Audit of Security in Field Offices

Office of the Inspector General
Internal Audit Report AR/24/19

WFP
World Food Programme

December 2024

Contents

I. Executive summary

Introduction

1. As part of its annual workplan, the Office of Internal Audit conducted an audit of security in field offices.

2. WFP field security expenditure totalled USD 89.5 million in 2023 – a significant increase compared to recent years. The audit assessed how WFP implements and monitors field offices' compliance with established security frameworks; maintains a state of readiness; responds to changes in physical security conditions; and coordinates with the UN security apparatus to safeguard the physical security of its employees and partners.

Audit conclusions and key results

3. Based on the results of the audit, the Office of Internal Audit reached an overall conclusion of **major improvement needed**. The assessed governance arrangements, risk management and controls were generally established and functioning, but, at the same time, they need major improvement to provide reasonable assurance that the objectives of the audited entity/area should be achieved. Issues identified by the audit could negatively affect the achievement of the objectives of the audited entity/area. Prompt management action is required to ensure that identified risks are adequately mitigated.

4. The WFP Security Framework of Accountability, combined with WFP security processes, enabled operations in conflict-affected areas and highly insecure environments where personnel and partners faced abrupt changes in physical security conditions. In 2023, these measures supported operations in increasingly challenging contexts, where humanitarian workers were exposed to deteriorating security environments.

5. The audit report contains the following three observations with high-priority agreed actions in the areas of governance, set-up and digital systems supporting the implementation of the security framework and collaboration with the UN apparatus and other stakeholders:

Gaps in operationalization of security governance structures and resource allocation (Observation 1)

Accountability for the safety and security of personnel, premises and assets at the field level was not consistently paired with the profile and authority required to make and implement security decisions. Budgeting for security personnel in field locations was inconsistent and lacked a standardized approach or rationale that mirrored the security risks assessed. In some instances, the seniority of security profiles and contract types did not align with security needs, particularly in emergency situations.

Existing mechanisms do not ensure that budgetary allocations are aligned with evolving security needs in volatile contexts, nor do they provide adequate oversight of local security budgets. There were coordination gaps in asset and resource utilization at the field level, including prepositioning. For example, the absence of a coordinated strategy for acquiring and utilizing essential security measures, such as armoured vehicles and protective equipment, coupled with funding reductions, increased program criticality, and the need for resource optimization limited operational efficiency, in some field locations.

Gaps in the digital transformation process (Observation 4)

Several digitization initiatives were ongoing during the audit fieldwork, including updates to legacy systems to monitor compliance with field security processes and procedures, and the launch (in 2023) of new digital systems to support operations in complex emergencies. The lack of interoperability among data sets and insufficient critical data sharing in corporate systems, as well as shortcomings in the design and change management processes for digital transformation, limited the effectiveness of new tools in supporting decision-making.

Ineffective cooperation with key partners in field locations (Observation 7)

WFP's larger presence in remote field locations, without a clear definition of duty of care obligations and timely and relevant security information, increased WFP's risk exposure. In locations with challenging access and operational environment constraints, the UNSMS decision-making process was not always fit for

purpose, and delayed issue escalation for decision making, including, for example, implementing alternative working arrangements and relocating or evacuating staff and their families.

The framework for collaboration and security coordination with local cooperating partners was unclear and led to inconsistencies and gaps in security information-sharing. Incomplete implementation of the Saving Lives Together framework with international cooperating partners further increased exposure and hindered effective field operations, including delaying distribution cycles.

6. The Office of Internal Audit would like to thank managers and staff for their assistance and cooperation during the audit.

II. Context and audit scope

Background

7. As a United Nations (UN) organization, WFP participates in the UN Security Management System (UNSMS) and has a seat in its executive group. The roles and responsibilities of UNSMS members concerning security risk management are included in the UNSMS framework of accountability.[1] The core responsibility for the security of UN personnel rests with the host government, while WFP has a duty to reinforce and supplement the capacity of the host country to fulfil its responsibilities.

8. As a frontline organization, WFP has adopted a "stay and deliver" approach, which is accomplished in coordination and cooperation with the United Nations Department for Safety and Security (UNDSS).

9. In May 2023, the Executive Director signed a circular to align WFP's Security Management Policy and Framework of Accountability with the UNSMS Framework of Accountability.[2] This framework defines the responsibilities and accountabilities of security actors within the organization and applies to all WFP personnel and eligible dependants, consultants, interns, service contract and special service agreement holders.

Security operations

10. The primary objective of security risk management at WFP is to enable the organization to conduct its activities within acceptable levels of risk while ensuring the security of personnel, eligible dependants, premises, operations and assets.

11. Security at WFP field offices involves several actors, including regional directors, country directors, heads of offices, area offices, field offices and headquarters Security Division. The responsibilities of each actor are defined in the WFP Security Framework of Accountability.

12. In 2023, field office security costs increased significantly, with personnel costs expenses increasing to USD 54.4 million, up from USD 37.8 million in 2021.

13. The operational context for WFP field operations continues to evolve, with escalating security risks. In recent years, personnel in many field locations have faced increased threats, including the risk of collateral damage in conflict-affected areas. For example, military takeover, the presence of non-state armed groups and internal conflict have compounded these pressures, with some locations experiencing security risks at very high and even unacceptable levels.

14. In 2023, 1,734 safety and security incidents affected WFP operations, a figure largely consistent with incidents in 2022 and 2021.[3] However, a higher proportion of major incidents impacted WFP personnel compared to previous years. There was a rise in fatalities among WFP staff, largely due to active conflict and the regional crisis across multiple field operational locations.

15. WFP coordinates security operations in country offices with other UNSMS organizations, in line with the in-country security architecture. The Designated Officials are accountable to the Secretary-General, through the Under Secretary-General, UNDSS, for the safety and security of all individuals covered by UNSMS in their designated area. Designated Officials are supported by a range of UN security professionals and the Security Management Team (SMT), as well as the Under-Secretary-General, UNDSS.

16. WFP is also a member of Saving Lives Together, a framework of collaboration between international non-governmental organizations (NGOs) and UNSMS.

[1] https://www.un.org/en/safety-and-security/governance

[2] OED2023/010 WFP Security Management Policy and Framework on Accountability.

[3] The figure comprises incidents affecting WFP personnel, cooperating partners and contractors only when providing services directly related to WFP programmes.

Objective and scope of the audit

17. The objective of the audit is to provide assurance on the effectiveness of governance, risk management and internal control processes related to the management of security in WFP field offices. Such audits contribute to the annual overall assurance statement to the Executive Director on governance, risk management and internal controls.

18. The audit covered the period from 01 January to 31 December 2023, and reviewed transactions and events from other periods where necessary.

19. The audit focused on three lines of enquiry:

(i) Do the UNSMS/WFP Security Policy Frameworks adopted and implemented in WFP enable an effective security risk management culture in the field?

(ii) Does WFP collect, monitor, analyse and communicate security-related information for effective and efficient decision making?

(iii) How does WFP coordinate with UNSMS and partners to effectively support and enable programmatic delivery while balancing acceptable risk levels?

20. The audit scope was aligned with the ongoing Humanitarian Access audit to promote the efficient use of WFP resources. Areas already reviewed by the Humanitarian Access audit were excluded to prevent redundancy, ensuring that both audits complemented each other effectively.

21. This audit also leveraged field visits conducted as part of country office audits of WFP operations in Mali, Burkina Faso and Myanmar, all of which were part of the Office of Internal Audit's 2024 workplan, as well as a desk review of documentation relating to WFP operations in Haiti.[4] The audit carried out analyses of large sets of data and information across the entire organization and held interviews, focus group surveys and discussions with staff and management at headquarters, regional bureaux and country offices, as deemed appropriate.

22. In carrying out this audit, the review team was supported by an independent external security consulting service provider.

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

[4] The internal audit of WFP operations in Haiti, initially included in the Office of Internal Audit's workplan for 2024, was postponed due to the security situation in the country at the time of this audit fieldwork.

III. Results of the audit

Audit work and conclusions

24. Seven observations resulted from the audit, relating to security governance structures, risk management, security strategy and digital transformation, security operations, and duty of care and coordination with the UN security apparatus.

Governance framework and risk management

25. Led by the WFP security focal point, the Security Division coordinates WFP's safety and security responses, providing guidance and technical support across all levels. This includes field security operations, headquarters security, information management, and policy and partnerships units, supported by regional security officers and country-level security personnel.

26. WFP security professionals follow dual reporting lines: direct day-to-day supervision within their country offices and regional bureaux and functional reporting within the Security Division.

27. At the time of the audit fieldwork, the Security Division was reviewing its strategic objectives for the 2024–2025 biennium and had updated several policies and procedures to reflect current operational practices, including functional compliance mechanisms in consultation with the field. In 2024, the division was repositioned with higher seniority, in line with best practices, due to the criticality of its role.

28. In September 2024, the Security Division launched the Security Strengthening Programme, which was presented externally to the Executive Board in November 2024. Initiated for extra-budgetary allocation, the programme aims to enhance WFP's security measures, particularly in field operations, aligning with WFP's broader risk management strategies and operational priorities.

Observation 1: Gaps in operationalization of security governance structures and resource allocation

Governance and staffing structure

29. The decision-making process for budgeting for security personnel at country office level was inconsistent across field locations and lacked a standardized approach or rationale. This resulted in varied security structures that did not adequately address the security needs of various field locations or match the assessed security risks. The definition of field security roles, as well as the seniority and number of security professionals across regional bureaux and country offices, differed and was sometimes unclear.

30. While UNSMS articulation of accountabilities, roles and responsibilities was clear and further detailed in WFP's recently updated Framework of Accountability, there were gaps in the delegation of security authority at the field level with instances where security profiles were varying and/or lacking because of staffing changes or prolonged vacancies. Some responsibilities were temporarily unassigned with unstructured and varying communication lines.

Security resource allocation and oversight

31. Security asset and resource utilization at field level was not effective, including prepositioning. Budgetary constraints, coupled with lengthy acquisition lead times, further complicated the procurement of essential security equipment, such as armoured vehicles and protective equipment, increasing personnel exposure to danger. While in some instances WFP mitigated pressing security risks through evacuations and relocations, direct threats from shifting security landscapes remained a concern.

32. Security cost categories were mapped as cross-cutting and mingled with other costs, such as those related to the Technology or Management Services Division, limiting visibility and traceability of allocations, and increasing the risk of duplicating some costs. An analysis of cost categorizations indicated significant fluctuations in some cost categories across periods and field locations. Rapid fluctuations in the field security context complicated budget forecasting and allocation, requiring flexible planning to manage unprecedented changes in the security risks assessed.

Underlying causes: Strategy, mandate and authority |Insufficient authority and/or accountability; process and planning| Unclear roles and responsibilities; policies and procedures | Absence or inadequate corporate policies/guidelines; resources – people| Insufficient staffing levels; resources – funds| Insufficient financial/cost management.

Agreed Actions [High priority]

The Security Division will:

1) Clarify and disseminate criteria to guide country offices in defining the minimum-security personnel profile required at country office locations.

2) Review security reporting lines to ensure accountability; and enhance the corporate country director induction programme by incorporating an effective and efficient security module to increase awareness of these reporting lines.

3) Clarify the process, responsibilities and timelines for review of local cost-shared budgets.

4) Assess cost categorization to avoid duplication and overlaps in security services and equipment and maximize resource utilization; and, following the Programme and Operations Division-led reform of the Country Strategic Plan process, prepare guidelines for best practices in the Country Portfolio Budget process.

Timeline for implementation

1) 30 06 2025
2) 30 06 2025
3) 30 06 2025
4) 30 06 2025

Observation 2: Data access limitations and misalignment of security performance indicators with security objectives

Data access for security in WFP field operations

33. WFP's primary security objective is to support the organization's "Saving Lives, Changing Lives" mandate by ensuring the safety of personnel, dependants and operations through a proactive approach to security risk management. This was not adequately supported by readily accessible and clearly defined information and data. For example, personnel lists and dependants' data were not regularly updated or shared in a timely manner with those charged with security responsibilities, due to issues such as manual processes or ineffective data flows among relevant stakeholders across WFP divisions. The absence of essential data, such as locations, impaired the efficient implementation of field security procedures and decision making in crisis situations (see observation 4 Gaps in the Digital Transformation Process).

Key Performance Indicator alignment with security objectives for programme delivery

34. At the time of audit reporting, the Security Division was reviewing the key performance indicators (KPIs) it uses to measure, track and report on compliance with security requirements to better align its efforts with the corporate risk level and performance management objectives. Initially, these KPIs primarily focused on the Security Division's internal performance, without adequately reflecting its broader role in safeguarding

operations, particularly programmatic delivery of WFP field operations. There was a lack of clarity on how the security input to safeguard operations was determined and measured, as well as insufficient tracking and reporting of KPI completion rates.

35. Insufficient monitoring of the KPIs, coupled with low reporting completion rates, resulted in both lower scores in 2023 compared to 2022 and affected reporting uptake at the field level. The weighted scoring of KPIs placed excessive emphasis on training scores while neglecting broader security objectives and was inconsistently applied across field locations.

Underlying causes: Process and planning | Insufficient coordination – internal or external; Oversight and performance | Performance measures and outcomes inadequately measured/established.

Agreed Actions [Medium priority]

The Security Division will:

1) While digital enhancement is ongoing (see observation 4 Gaps in Digital Transformation Process), in collaboration with Human Resources, establish a protocol for regular data access and sharing with the Security Division, to facilitate security personnel's access to up-to-date information.

2) As part of the Security Strengthening Programme, support country offices by providing standards and tools for consistent and reliable Operational Information Management at country office level.

3) Finalize the review of existing KPIs and develop a set of new Key Risk Indicators, for an integrated approach that aligns security compliance with corporate performance and risk management processes.

4) In the new security KPIs and Key Risk Indicators, specify performance indicators that aim to address the limitations of the current KPIs.

Timeline for implementation

1) 30 06 2025
2) 30 09 2025
3) 30 06 2025
4) 30 09 2025

Observation 3: Insufficient security risk management and preparedness

Security risk management

36. Security risk management in the corporate risk register, country-specific risk registers and area security risk management[5] were not clearly and systematically linked or defined. Security risk management tools were not well-suited for managing rapidly evolving security risks. For example, the area security risk management documents reviewed during the audit were long, repetitive and unclear about the threat environment and risks to WFP. These issues, combined with limited visibility and coordination at country office level, led to parallel risk management efforts, negatively affecting decision making and the management of WFP-specific security risks.

37. Area security risks were not consistently updated, nor were mitigating measures consistently communicated to other relevant parties within the country office risk management structure. With an exposure and footprint more significant than other organizations within UNSMS, existing security risk reporting and escalation processes require improvement to be adequate for WFP operations with volatile security risks.

[5] The Security Risk Management process was launched by UNSMS in 2004 as a system–wide managerial tool to analyse and manage safety and security risks to UN personnel, assets and operations. It was last updated in 2009 with additional guidelines, training tools and templates.

38. In multiple instances, security crisis-management coordination challenges at the UNSMS level required WFP to take proactive measures. The review of evacuation and relocation processes highlighted weaknesses such as delays in formalizing procedures and, in some cases, vague plans that did not adequately mitigate the various threats during execution. Crisis response preparedness was not periodically rehearsed, limiting the identifications of gaps and the ability to address critical security needs in advance.

Security training programmes and accessibility

39. The development of a security awareness culture through training programmes faced several challenges. Training needs and the actual delivery of training were not consistently aligned with specific security threats at the country level. The training framework and budgetary allocations did not adequately address the needs of country offices. Specifically, (i) there was a misalignment between the assessed security risks at the country office level and the availability of relevant training, e.g. some regions had a higher uptake of First Responder training than regions assessed to have higher security risks; and (ii) there were significant regional variations in the uptake of mandatory security training, with only 18 percent of security personnel in some regions completing the required training.

40. Accessibility to personnel security training data was limited, as data were not fully integrated with existing WFP corporate systems, reducing visibility of travel requirements and training compliance. In particular, mandatory security training data were hosted on the UNDSS platform, with records tracked by WFP in Excel, making it difficult to monitor personnel's training status before travel. The WFP Security Division indicated it is planning an integration with the WFP learning system.

Underlying causes: Tools, systems and digitization | Absence or late adoption of tools and systems; resources | Absence of/insufficient staff training | Policies and procedures | Absence or inadequate corporate policies/guidelines.

Agreed Actions [Medium priority**]**

The Security Division will:

1) As part of the Security Strengthening Programme, establish a road map to integrate security risk management into WFP's emerging corporate risk management structures in alignment with corporate compliance mechanisms as per the broader Risk Management Division corporate framework.

2) Advocate at UNSMS level for revisions to the Security Risk Management Manual, Policy on UNSMS Personnel Information Management System and Travel Clearance, to address existing data gaps.

3) Assess the possibility for training materials to include multiple languages to improve accessibility, compliance and broader inclusivity, taking into account funding availability.

4) Revise the divisional strategy for security training in the context of the Security Strengthening Programme, to align this exercise with identified Strategic Workforce Planning Exercise recommendations.

Timeline for implementation

1) 30 09 2025
2) 30 09 2025
3) 30 09 2025
4) 30 09 2026

Security Strategy and digital transformation

41. The Security Division initiated a digital transformation project that initially began in 2013 and gained traction in 2023 to support the new Security Strategy. The Digital Road Map[6] was developed to address the need for improved efficiency and the reallocation of resources from manual processes. After identifying gaps, the Security team decided to implement early versions of the new tools and applications (prototypes) to iteratively test and refine their features and functionalities.[7]

42. With the support of digital platforms, the Security Division aims to enhance coordination efforts among headquarters, regional bureaux and country offices. The audit team conducted a review of change management for the newly implemented tools and analysed reported security incidents, including their escalation and resolution.

Observation 4: Gaps in the digital transformation process

Gaps in digital transformation change management

43. During the audit fieldwork, the Security Strategy for 2024–2025 was still in draft form, as were its associated measures, including the digital transformation process. The absence of clearly defined timelines for action from key stakeholders outside the Security Division (required to support implementation of the digital transformation process) impacted the adoption of the new tools and applications and extended the transition period for achieving the Security Division's objectives.

44. During the digital transformation transition phase, stakeholder engagement and support for implementing new tools and application upgrades, communication and user training were insufficient. Delays, including corporate and leadership buy-in, impacted the definition and achievement of milestones and slowed the adoption process.

Security systems and tools not integrated

45. There were gaps in the interoperability of new tools with existing corporate systems, resulting in inefficiencies and suboptimal integration of end-to-end processes. For example, the tool for tracking security assessment recommendations was not integrated with the corporate tool for facilities management, which affected the consistency of mapping all facilities in each location. The process of sharing and updating personnel data with human resources corporate data was also not integrated, hindering optimal data flow and real-time updates for crisis response and security operations. For the current information-sharing set-up and interim solution see Observation 2 Data access limitations and misalignment of security performance indicators with security objectives.

46. Databases for the Framework of Accountability Compliance Tool (FACT) questionnaire and the security assistance mission recommendation were not integrated, potentially hindering the alignment of security assessments and limiting the ability to track the status of quarterly self-reporting against open recommendations. As a result, gaps identified in compliance with security risk management policies and procedures may not be fully or timely addressed, or followed up on, impacting oversight and preventing a comprehensive view of field operations.

[6] The road map was endorsed by WFP's Chief Information Officer and Chief Data Officer in the second quarter of 2024, aligning this initiative with the IT Strategy and Data Strategy endorsed by the Executive Director at the beginning of 2024.

[7] The roll-out of digital tools included the Security Tracking and Reporting System (STARS), which replaced the Incident and Information Management System (SIMSAS) to establish a consistent reporting framework that ensures timely, accurate and actionable security information is available, facilitating effective decision making and rapid response to incidents; eTremp, which enables security professionals to access and manage security assistance mission recommendations and observations; and the Framework of Accountability Compliance Tool (FACT), which replaces the Quarterly Assurance Statement to streamline compliance confirmation and security task completion.

Non standardized reporting

47. At the time of the audit fieldwork, implementation of feedback on the FACT tool roll-out was pending, with updates required to enhance its functionality. The responses to the FACT tool questionnaire had data quality issues, with security officers and focal points reporting unclear guidance on the required responses. The frequency of FACT tool quarterly assessments would benefit from revisiting, to enhance response rates and data quality.

48. Security Operational Reports were not standardized across regional bureaux and country offices, leading to inconsistent methodologies. This extended reporting timelines and complicated reporting analysis by the dedicated Security Division unit. Survey respondents indicated that while flash reports were generally efficient, they would benefit from increased digitalization to streamline the process.

Underlying causes: Strategy, mandate and authority | Unclear direction for planning, delivery or reporting; tools, systems and digitization | Inappropriate implementation or integration of tools and systems; resources | Absence of/insufficient staff training.

Agreed Actions [High priority]

The Security Division will:

1) Finalize guidelines for the 2024–2025 Security Strategy and standardize reporting templates and methodologies for consistency.
2) Implement a unified analytical framework by aligning country and regional reporting analyses with headquarters, including training on a unified approach.
3) Engage stakeholders to streamline prototyping data linkage among various tools and applications, including assessing the possibility of a link with HR systems and Data as well as between eTremp and the facility management solution for seamless data flow among various tools and applications.
4) Review and address the limitations of FACT and include FACT completion in country director/country offices' KPIs. Evaluate integrating Flash reports into STARS and prepare Security Operational Reports based on STARS data to optimize use.
5) Prepare and communicate a clear and actionable digital transformation road map to advance the transition, including roll-out and end-user training, leveraging extra-budgetary funding related to the Security Strengthening Programme.

Timeline for implementation

1) 30 06 2025
2) 30 06 2025
3) 30 09 2025
4) 30 09 2025
5) 30 09 2026

Observation 5: Gaps in the incident management process impacting decision making

Roles and responsibilities

49. The standard operating procedure for incident management and reporting was not implemented effectively, despite clear roles, responsibilities, and accountabilities. The decision-making tree, which outlines the steps and criteria for escalating incidents to higher levels of authority based on their severity and accountability, had yet to be reviewed or validated.

Timeliness of incident reporting

50. There were indications that, in some instances, incidents had not been reported and significant delays were observed in the reporting of incidents from the time of occurrence[8] and in the review and release of incidents for closure[9] within the Security Tracking and Reporting System, potentially impacting timely escalation and resolution.

Data quality and resolution

51. There were data quality issues in the analysis of registered incidents. Data migrated from the legacy system were not adequately cleaned or normalized before their upload into the new system, resulting in inconsistencies. Errors and anomalies were not systematically identified or corrected despite steps in place to review and validate incidents during processing. Incidents were not always correctly categorized and there were duplicated entries despite the presence of a deduplication tool.

52. In STARS, a workflow step was not included after the review to indicate the resolution steps taken prior to the closure of an incident. Although a second-level review was implemented with a "released" status, no "closed" status was available to indicate that the necessary post-incident actions had been completed. There was insufficient documented evidence of actions taken.

53. No structured process was in place for sharing and managing knowledge related to observations and recommendations identified through incident declarations, lessons learned, and fact-finding reports conducted for specific incidents in collaboration with other actors within UNSMS. This limited the (i) continuous improvement of processes and procedures, and (ii) information available to field offices about any cross-cutting mitigation measures identified from proposed recommendations.

Underlying causes: Process and planning | Unclear roles and responsibilities; inadequate process or programme design; policies and procedures | Absence or inadequate corporate policies/guidelines; tools, systems and digitization | Inappropriate implementation or integration of tools and systems.

[8] Up to 25 percent of incidents were recorded 10 to 30 days after the occurrence, and 13 percent were recorded more than one month after the incident.

[9] 38 percent were processed between 11 to 30 days, and 15 percent at least one month after the incident.

Agreed Actions [Medium priority]

The Security Division will:

1) Develop new guidelines and standard operating procedures for incident management and analysis covering the entire process from initial incident reporting to review and release.
2) Ensure that defined roles, responsibilities and accountabilities (decision tree) for all individuals involved in incident management and reporting are aligned with security risk management accountabilities and emerging corporate structures on risk management.
3) Based on data from STARS, identify and define the reports and analyses relevant to both field offices and headquarters/regional bureaux, including their frequency and how they should support field offices' decision making mechanisms when incidents occur.
4) Implement the actions outlined in the (draft) Security Division Strategy 2024–2025:
   (i) Establish a knowledge management system by incorporating a "lessons learned" repository that includes case studies and best practices.
   (ii) Ensure that the established knowledge management system is accessible, while also providing tiered access levels to protect sensitive information. Conduct a feasibility analysis to assess the added value of implementing actions within STARS following an incident.
5) Review and clean the database that was migrated from SIMSAS.

Timeline for implementation

1) 30 06 2025
2) 30 09 2025
3) 30 09 2025
4) 31 12 2025
5) 30 06 2026

Security operations

54. Security assistance missions support country offices in complying with security processes and procedures in country office locations. In 2023, the Security Division conducted 24 security assistance missions across 289 locations, representing 25 percent of WFP locations globally. In January 2024, the Security Division adopted new guidelines recommending a security review of each WFP field location every two years.

55. Security assistance missions are conducted by external and internal security experts, overseen by regional security officers. The process is managed in E-tremp, a tool used for documenting and managing mission recommendations. The audit assessed the effectiveness and timeliness of security assistance mission processes.

Observation 6: Gaps in scheduling, processing and analysis of security assistance missions results

Scheduling of security assistance missions

56. The Security Division developed a risk-based approach to scheduling security assistance missions in 2023 based on criteria such as the date of the most recent mission, the complexity of operations and the number of outstanding recommendations. These criteria did not include essential considerations such as the country office's overall security rating from the area security risk assessment. Some regional bureaux did not adopt the risk-based approach for scheduling security assistance missions, as such, the criteria used were not standardized across the organization and, in some cases, the results of the assessments were not adequately documented.

57. Security assistance mission visits were not conducted consistently across field offices, with some locations receiving visits more frequently than others without clear rationale and prioritization. This increases security risks for operations and staff in field locations, where non-compliance issues may not be identified in a timely manner to prompt mitigating actions.

Security assistance mission process

58. The security assistance mission process is in large part manual, for example, adding and deleting facilities for security assistance mission visits; downloading and completing the mission checklist; and emailing the results to the Security Division. This increases the risk of errors and breaches of confidential security information. Steps such as selecting facilities for mission visits,[10] notifying country offices and conducting exit briefings are performed outside the E-tremp system, resulting in the absence of a documented audit trail.

Analysis of mission findings

59. The Security Division does not analyse observations arising from security assistance missions to identify recurrent findings and non-compliance patterns. This leads to repetitive issues within and across offices and a lack of efficiency in optimizing the process and improving service value.

Underlying causes: Resources – people | Insufficient staffing levels; process and planning | Inadequate process or programme design; tools, systems and digitization | Absence or late adoption of tools and systems; external factors beyond the control of WFP | Conflict, security and access.

[10] For action on this point see Observation 4 Gaps in the Digital Transformation Process

Agreed Actions [Medium priority]

1) The Security Division will:

   (i) Clarify and disseminate the scheduling criteria for security assistance missions and develop a standardized template for identifying country office priorities, along with a mechanism to enforce its use.

   (ii) Evaluate the feasibility of progressively involving roving security personnel from other regional bureaux or country offices to conduct security assistance missions.

2) The Security Division will improve E-tremp to reduce offline processing and include analytics capabilities for analysis of instances of non-compliance.

Timeline for implementation

1) 30 06 2025
2) 30 09 2025

Security coordination

60. The WFP Security Division manages security risks in coordination with UNDSS and other UNSMS actors. The SMT is the forum for consultation on security matters, while final decisions are taken by the relevant Designated Official. The SMT is informed by in-country security cells. The UNSMS Framework of Accountability defines the roles and accountability of various security actors, as well as the governance mechanisms at all levels.

61. The audit reviewed WFP's security decision making processes at the field office level; coordination with the SMT and security cells; and how WFP shares security information with its cooperating partners.

62. At the time of audit reporting, a corporate initiative was ongoing to clarify WFP's definition of duty of care and its implementation. A (draft) circular, applicable to all WFP employees regardless of function, title, contract modality or location, focuses on duty of care in the workplace but also extends beyond the workplace to cover official travel, missions and deployments. It does not cover WFP's obligations towards cooperating partners, vendors or other relevant third parties and their personnel.

Observation 7: Ineffective cooperation with key partners in field locations

Gaps in coordination within UNSMS

63. WFP's footprint, operational constraints and "stay and deliver" approach involve a more significant risk appetite than some UNSMS members. Specifically, WFP's mandate requires a presence in more remote locations and frontline areas during emergencies. In locations with challenging access and operational environment constraints, the UNSMS decision making process was not always fit for purpose, leading to delays in escalating issues and taking decisions, including, for example, implementing alternative working arrangements and relocating or evacuating staff and their families. In some cases, the review process was delayed and impractical during crises and this, coupled with a lack of clarity about duty of care obligations, exposed WFP personnel, assets and operations to high security risks.

64. UNDSS is the custodian of the security risk management reports. On a few occasions, the untimely publication of these reports led to the use of outdated information and recommendations that were not applicable for decision making, impacting the effectiveness of security risk assessments to inform the security assistance mission process. See Observation 3 Insufficient security risk management and preparedness and related agreed actions.

Coordination with cooperating partners

65. There are no defined processes and mechanisms to guide collaboration on security between WFP and local cooperating partners, who form the majority of partners in the field (up to 70 percent). Security information is shared on a case-by-case basis using emails, cell phones or during meetings. Roles and responsibilities regarding security coordination with cooperating partners at both country office and field office levels are not clearly defined.

66. Saving Lives Together, the security collaboration framework between UNSMS members and international NGOs, is not fully implemented. This may create gaps in communicating important security information between WFP and its international cooperating partners.

Underlying causes: Resources – people | Insufficient staffing levels; external factors beyond the control of WFP | UN or sector wide reform – UN security apparatus set-up; policies and procedures | Absence or inadequate corporate policies/guidelines| Resources – funds | Inadequate funds mobilization.

Agreed Actions [High priority]

1) The Security Division will review and strengthen relevant induction sessions to increase the capacity of security risk management professionals at all levels of the organization.

2) The Security Division, in collaboration with the NGO Partnership Unit and Legal Office, will:

   (i) define WFP security accountability and liability in field-level agreements; and

   (ii) explore the feasibility of a standardized method for security budget allocation and communication with partners.

3) As part of its Security Strengthening Programme, the Security Division will assess and define a road map for the project to strengthen the security risk management capacity of cooperating partners.

Timeline for implementation

1) 30 09 2025
2) 30 09 2025
3) 30 09 2026

Annex A – Agreed action plan

The following table shows the categorization, ownership and due date agreed with the audit client for all observations raised during the audit. This data is used for macro analysis of audit findings and monitoring the implementation of agreed actions.

The agreed action plan is primarily at the country office level.

#	Observation (number/title)	Area	Owner	Priority	Timeline for implementation
1	Gaps in operationalization of security governance structures and resource allocation	Governance Framework and Risk Management	Security Division	High	30 06 2025 30 06 2025 30 06 2025 30 06 2025
2	Data access limitations and misalignment of security performance indicators with security objectives	Governance Framework and Risk Management	Security Division	Medium	30 06 2025 30 09 2025 30 06 2025 30 09 2025
3	Insufficient security risk management and preparedness	Governance Framework and Risk Management	Security Division	Medium	30 09 2025 30 09 2025 30 09 2025 30 09 2026
4	Gaps in the digital transformation process	Security Strategy and Digital Transformation	Security Division	High	30 06 2025 30 06 2025 30 09 2025 30 09 2025 30 09 2026
5	Gaps in the incident management process impacting decision making	Security Strategy and Digital Transformation	Security Division	Medium	30 06 2025 30 09 2025 30 09 2025 31 12 2025 30 06 2026
6	Gaps in scheduling, processing and analysis of security assistance missions results	Security operations	Security Division	Medium	30 06 2025 30 09 2025
7	Ineffective cooperation with key partners in field locations	Security coordination	Security Division	High	30 09 2025 30 09 2025 30 09 2026

Annex B – Definitions of audit terms: ratings and priority

1 Rating system

The internal audit services of UNDP, UNFPA, UNOPS and WFP adopted harmonized audit rating definitions, as described below.

Table B.1: Rating system

Rating	Definition
Effective/ satisfactory	The assessed governance arrangements, risk management and controls were adequately established and functioning well, to provide reasonable assurance that issues identified by the audit were unlikely to affect the achievement of the objectives of the audited entity/area.
Some improvement needed	The assessed governance arrangements, risk management and controls were generally established and functioning well but needed improvement to provide reasonable assurance that the objective of the audited entity/area should be achieved. Issues identified by the audit were unlikely to significantly affect the achievement of the objectives of the audited entity/area. Management action is recommended to ensure that identified risks are adequately mitigated.
Major improvement needed	The assessed governance arrangements, risk management and controls were generally established and functioning, but needed major improvement to provide reasonable assurance that the objectives of the audited entity/area should be achieved. Issues identified by the audit could negatively affect the achievement of the objectives of the audited entity/area. Prompt management action is required to ensure that identified risks are adequately mitigated.
Ineffective/ unsatisfactory	The assessed governance arrangements, risk management and controls were not adequately established and not functioning well to provide reasonable assurance that the objectives of the audited entity/area should be achieved. Issues identified by the audit could seriously compromise the achievement of the objectives of the audited entity/area. Urgent management action is required to ensure that the identified risks are adequately mitigated.

2 Priority of agreed actions

Audit observations are categorized according to the priority of agreed actions, which serve as a guide to management in addressing the issues in a timely manner. The following categories of priorities are used.

Table B.2: Priority of agreed actions

High	Prompt action is required to ensure that WFP is not exposed to high/pervasive risks; failure to take action could result in critical or major consequences for the organization or for the audited entity.
Medium	Action is required to ensure that WFP is not exposed to significant risks; failure to take action could result in adverse consequences for the audited entity.
Low	Action is recommended and should result in more effective governance arrangements, risk management or controls, including better value for money.

Low-priority recommendations, if any, are dealt with by the audit team directly with management. Therefore, low-priority actions are not included in this report.

Typically audit observations can be viewed on two levels: (a) observations that are specific to an office, unit or division; and (b) observations that may relate to a broader policy, process or corporate decision and may have a broad impact.[11]

[11] An audit observation of high risk to the audited entity may be of low risk to WFP as a whole; conversely, an observation of critical importance to WFP may have a low impact on a specific entity but have a high impact globally.

3 Monitoring the implementation of agreed actions

The Office of Internal Audit tracks all medium and high-risk observations. Implementation of agreed actions is verified through the corporate system for the monitoring of the implementation of oversight recommendations. The purpose of this monitoring system is to ensure management actions are effectively implemented within the agreed timeframe to manage and mitigate the associated risks identified, thereby contributing to the improvement of WFP's operations.

The Office of Internal Audit monitors agreed actions from the date of the issuance of the report with regular reporting to senior management, the Independent Oversight Advisory Committee and the Executive Board. Should action not be initiated within a reasonable timeframe, and in line with the due date as indicated by Management, the Office of Internal Audit will issue a memorandum to management informing them of the unmitigated risk due to the absence of management action after review. The overdue management action will then be closed in the audit database and such closure confirmed to the entity in charge of the oversight.

When using this option, the Office of Internal Audit continues to ensure that the office in charge of the supervision of the unit who owns the actions is informed. Transparency on accepting the risk is essential and the Risk Management Division is copied on such communication, with the right to comment and escalate should they consider the risk accepted is outside acceptable corporate levels. The Office of Internal Audit informs senior management, the Independent Oversight Advisory Committee and the Executive Board of actions closed without mitigating the risk on a regular basis.

Annex C – Acronyms

E-tremp	Tool that enables security professionals to access and manage security assessment mission recommendations
FACT	Framework of Accountability Compliance Tool
KPI	Key Performance Indicator
NGO	Non-Governmental Organization
SIMSAS	Incident and Information Management System
SMT	Security Management Team
STARS	Security Tracking and Reporting System
UNDSS	United Nations Department for Safety and Security
UNSMS	UN Security Management System
WFP	World Food Programme