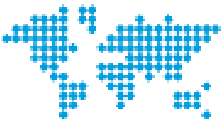
THEMATIC AUDIT

# AUDIT OF SECURITY MANAGEMENT AT UN WOMEN

UN WOMEN

THEMATIC AUDIT

# AUDIT OF SECURITY MANAGEMENT AT UN WOMEN



**INDEPENDENT EVALUATION AND AUDIT SERVICES (IEAS)**
Internal Audit Service (IAS)
UN WOMEN

14 July 2022
*IEAS/IAS/2022/001*

# TABLE OF CONTENTS

EXECUTIVE SUMMARY i

ACRONYMS AND ABBREVIATIONS iv

I. INTRODUCTION 1

II. BACKGROUND 1

III. AUDIT OBJECTIVES, SCOPE AND METHODOLOGY 3

IV. AUDIT RESULTS 5

A. OVERALL ASSESSMENT AND ACHIEVEMENTS 5

B. GOVERNANCE 5

C. SECURITY RISK MANAGEMENT 14

D. SECURITY OPERATIONS 16

E. SECURITY MONITORING AND COMPLIANCE 17

V. RECOMMENDATIONS AND MANAGEMENT ACTION PLAN 19

ANNEX 1. DEFINITIONS OF AUDIT TERMS RATINGS AND PRIORITIES 23

ANNEX 2. ROLES AND RESPONSIBILITIES FOR SECURITY MANAGEMENT 24

# EXECUTIVE SUMMARY

## Introduction

During its annual risk assessment, the UN Women Internal Audit Service (IAS) of the Independent Evaluation and Audit Services (IEAS) selected UN Women's security management process for review as it is a strategically important area for the Entity. UN Women personnel operate in a wide range of constantly evolving environments and must have the necessary strategic, risk management and support structures in place to protect them and the organization. The UN Women Executive Director is responsible and accountable to the UN Secretary-General for ensuring that the goals of the UN Security Management System are met within UN Women. The Executive Director implements the "no programme without security, no security without resources" strategy, as stated in the United Nations Security Management System Security Policy Manual, in all UN Women programmes and activities.

## Audit objective and scope

Management is responsible for establishing and implementing effective security governance, risk management, operational support and monitoring. The responsibility of internal audit is to assist management by providing assurance and advising management on the discharge of its obligations.

The audit objectives were to assess the effectiveness of security management, with focus on the following key areas:

A. **Governance:** policy, organizational structure and positioning, resources, roles and responsibilities, organizational security culture.
B. **Security risk management:** security activities, controls and risk management including identification, mitigation, risk escalation protocols and monitoring of key risks, including monitoring of residual risk.
C. **Security operations:** functions supporting security service provision.
D. **Oversight and monitoring**: security compliance and policy effectiveness.

The audit did not plan to cover occupational health and safety or business continuity and crisis management. While these areas are also the responsibility of the Security and Safety Service, the key focal point for security at UN Women, they are topics in their own right and would require their own audit.

This audit recognizes that the Security and Safety Service in headquarters has certain roles, responsibilities and parameters to ensure the effectiveness of security management. However, security management is effective only if all the responsible parties and executive management adequately manage the security risks at all levels of the organization, and timely and proper actions are embedded into all processes. While the Security and Safety Service has a responsibility to oversee and advise executive management, this audit did not only focus on the Security and Safety Service's work, but also covered other roles and processes that should contribute to effective security management.

IAS followed the *International Standards for the Professional Practice of Internal Auditing* in conducting this audit.

## Audit opinion and overall audit rating

IAS would like to begin by recognizing the following good practices and achievements in security management at UN Women, including:

- **Governance:** Strong UN-wide policy framework effectively leveraged by UN Women security experts (Security and Safety Service).
- **Security risk management**: Development of the Business Continuity and Crisis Management App (BCCMA).
- **Security operations**: Tracking of workload outputs by the Security and Safety Service team; and coverage of six regions by four Regional Security Specialists, some of whom are responsible for multiple regions across wide time zones (which is commendable, but also poses a risk as discussed in this report).

- **Oversight and monitoring**: In-house development and monitoring of the annual security compliance survey covering 142 locations.

IAS assessed the overall state of governance, risk management and internal controls for security management in UN Women as **Some Improvement Needed** meaning "The assessed governance arrangements, risk management practices and controls were generally established and functioning but need some improvement. Issues identified by the audit do not significantly affect the achievement of the objectives of the audited entity/area."

The most important improvement areas are as follows:

1. The positioning and authority of the Security and Safety Service could be made more independent, retaining functional reporting to DMA, but with proper access to the Executive Office for prompt decision making and security risk updates.
2. The security funding and budgeting process should be formalized in policy, and reported on periodically, enhancing transparency and effectiveness in governing existing security funding mechanisms to fully implement the strategy of "no programme without security, no security without resources".
3. There is a need (a) for improved appreciation and culture of security in the organization, spearheaded by senior management; and (b) to strengthen individual manager accountability for complying with security requirements. Heads of Office are required to attest to the content and submission of any security compliance elements; however, there is currently no consequence if it is found that submissions are incomplete or inaccurate, which could create false assurance because the organization relies on those submissions in managing its security risks.

IAS also identified the following additional areas for improvement:

- **Governance:** need for development of (a) a formal UN Women policy on security management; and (b) a corporate strategy on security management aligned with organizational strategic priorities and interventions based on security and business risks and needs to close the gap between the existing and desirable security arrangements for delivering strategic priorities and interventions without compromising the security of personnel and assets.
- **Security risk management**: need (a) to enhance corporate security risk management and guidance to field offices; and (b) for greater clarity and accountability for quality of the services provided by the United Nations Department of Safety and Security (UNDSS) (US$ 1 million in 2019 and US$ 1.4 million in 2020).
- **Security operations**: better monitoring of support services such as security-related travel; and better tracking of UN Women needs in terms of security procurement and maintenance in field offices.
- **Oversight and monitoring**: need for more spot checks and second line of defence validation of data reported in annual compliance surveys to ensure that the data reported represents the actual security situation given that senior management relies on the data for decision-making.

IAS made 11 recommendations to address the above areas for improvement. One recommendation is ranked high priority and 10 are medium priority. The extent to which recommendations can be fully addressed is contingent upon the availability of resources.

The high priority recommendation means *"prompt/urgent action is required to ensure that UN Women is not exposed to very high or high risks. Failure to take action could result in significant/ major negative consequences for UN Women."* The recommendation is presented below:

**Recommendation 1 (High)**: The Global Security Adviser to consolidate available information into an official policy on security management, including: (a) clearly defining the authority of the Global Security Adviser to act as a fully-fledged business process owner with timely access to the Executive Director; (b) a role for Regional Offices in terms of overseeing security risks and ensuring compliance with key security controls; (c) expanding and clarifying the Head of the Office role, including individual accountability with key expectations for successful performance in terms of complying with key security controls; (d) defining key principles for governing security budget management including the authority of the Security Service team to validate the adequacy of security expenditure and to prevent waste; and, (e) reference to the concept of duty of care.

In addition, IAS made 10 medium (important) priority recommendations, meaning *"action is required to ensure that UN Women is not exposed to risks. Failure to take action could result in negative consequences for UN Women".* These recommendations aim to: perform an end-to-end risk assessment of security management; develop a corporate security strategy; map existing responsibilities against capacity; finalize a functional analysis of the security function; consider a provision to review the terms of reference and selection process of security personnel hired by field offices; develop formal policy and guidance defining how security funds are obtained and used; develop a mechanism for consolidating information on all security funding and spending; consider appointing a Security Service coordinator for all budgets related to security; include the BSAFE compliance statistics in the Quarterly Business Review statistics; cross-validate some offices' security annual compliance; devise and implement a regular security communications protocol by senior management; establish an accountability mechanism for field office security management for security risk management; enhance corporate security risk management and guide field offices in their risk assessment; continue to request that UNDSS sign a Memorandum of Understanding and service level agreement; include a question on the quality and timeliness of UNDSS services in the internal UN Women annual compliance survey; streamline an internal workflow between the Security Service and supporting functions; track security goods and services entries in office procurement planning; devise an accountability mechanism for the security and safety compliance survey reporting when it is found to be significantly inaccurate; ensure that regional security specialists perform and document periodic spot checks of self-assessments; and, include key statistics on security compliance in the Quarterly Business Review.

Low priority issues are not included in this report but, if identified, were discussed directly with management and actions have been initiated to address them.

## Management comments and action plan

Management accepts the recommendations and has included an action plan within this report. However, management indicated that the extent to which recommendations are implemented will be partially contingent upon the availability of resources.

IAS believes that the current recommendations are reasonable and feasible to implement within a two-to-three-year period (by end of 2024), subject to resource availability. Improvement in key areas is subject to sufficient resources being made available or reallocated to enact the changes; senior management leadership; and clear articulation of management's vision on security management. Investment in this area would strengthen UN Women's governance, policy, strategy and decision-making for security management.

Lisa Sutton

Lisa Sutton, Director
**Independent Evaluation and Audit Services**

# ACRONYMS AND ABBREVIATIONS

| | |
|---|---|
| **BCCM** | Business Continuity and Crisis Management |
| **BCCMA** | Business Continuity and Crisis Management App |
| **DMA** | Division of Management and Administration |
| **ERM** | Enterprise Risk Management |
| **ERP** | Enterprise Resource Planning |
| **FoA** | Framework of Accountability |
| **HR** | Human Resources |
| **IAS** | Internal Audit Service |
| **IEAS** | Independent Evaluation and Audit Services |
| **PPG** | Policy, Procedure and Guidance |
| **SMT** | Security Management Team |
| **UNCT** | United Nations Country Team |
| **UNDSS** | United Nations Department of Safety and Security |
| **UNSMS** | United Nations Security Management System |

# I. INTRODUCTION

The IAS risk-based audit plan included an internal audit of security management because this is a strategically critical area, both in terms of UN Women programmes and operations and for the Entity's personnel. The most severe consequence of security failure is loss of life, potentially at scale, which has unfortunately happened in the UN system in the past. Security underpins all of UN Women's work and while often viewed as operational in focus, it can have important and also potentially devastating impacts on programmatic and strategic undertakings. Other impacts include reputational, legal and financial damage. Managing security risks is a critical priority for UN Women management.

As per the UN Women Security Framework of Accountability, the UN Women Executive Director is ultimately responsible and accountable to the UN Secretary-General for ensuring that the goals of the UN Security Management System are met within UN Women. The Executive Director is supported by an internal security architecture, and she is responsible for implementing the "no programme without security, no security without resources" strategy, as stated in the United Nations Security Management System Security Policy Manual, in all UN Women programmes and activities.

This is the first internal audit of security management in UN Women. The Joint Inspection Unit conducted a review of "Safety and Security in the United Nations System" in 2016. Key recommendations included the need to: update host country agreements to reflect current security threats; develop a system-wide policy for road safety; include appropriate security compliance mechanisms in personnel performance appraisals; improve the availability of evacuation plans; incorporate safety and security compliance indicators in management performance assessments; strengthen the use of social media and big data analysis; and develop a system-wide security surge policy. All recommendations had been marked as implemented by management, except one on updating host country agreements, as it had been closed by the Inter-Agency Security Management Network. IAS notes that the recommendations appear to have been implemented except for further improvement that could be made with respect to the recommendation on including security compliance indicators in management performance appraisals.

# II. BACKGROUND

Security policy framework

Under the UN Security Management System's (UNSMS) Framework of Accountability all UN organizations are required to develop their own security framework of accountability relevant to their organization. UN Women has adopted the system-wide UNSMS Security Policy Manual and the Security Management Operation Manual. See Annex 2 for roles and responsibilities in the UN Women Framework of Accountability.

Roles and responsibilities

The UN Women Security and Safety Service team (henceforth called the Security Service) is responsible for the day-to-day management of safety and security operations in UN Women on behalf of the Executive Director. As a support service, the Security Service resides with the Division of Management and Administration (DMA). The Security Service oversees and coordinates the security responsibilities of UN Women around the world: currently 142 locations globally (including both main offices in host countries and sub-offices). In addition to security, the team is also responsible for occupational safety and health and business continuity and crisis management. Specific responsibilities include (but are not limited to) – see Annex 2 for details:

- Security mainstreaming.
- Security risk management.
- Security advisory role.
- Gender mainstreaming in a range of inter-agency working groups and targeted evaluation of gender security policy provisions within UNSMS.
- Security and Safety Compliance Business Process.
- Operational support – surge missions and rapid deployment.
- Organizational resilience management – business continuity management and crisis management, planning, maintenance, testing and response regime.
- Occupational safety and health.

The Security Service has an intranet site cataloguing the services and functions it performs, as well as a range of detailed and high-quality guidance for UN Women personnel covering a range of topics.

In the field, the Head of Office (the Representative) has overall responsibility for security management and is sometimes supported by local security associates (of which there are only a few in the organization), and other personnel in the office such as the Operations Manager or other personnel with delegated security responsibilities. Offices also receive continuous support from the Security Service's Regional Security Specialists.

UN Women relies extensively on the UNDSS network, support and services around the world and other larger agencies to which UN Women often outsources local security and other support, especially where UN Women shares premises.

## Security Service structure

The Security Service is part of DMA at headquarters. The team is supervised by the Global Security Adviser (P5) who reports to the Deputy Director, DMA. The team includes a Global Security Specialist – Business Continuity Manager (P4) who is also deputy and responsible for Europe and Central Asia coverage. There are also three Regional Security Specialists (P3): one covering Asia Pacific and Middle East Regions (located in Bangkok); one covering two Africa Regions (located in Nairobi); and one covering America and the Caribbean (located in headquarters) and Occupational Safety and Health. The team also includes on a short-term basis, an administrative consultant, an Occupational Safety and Health consultant, a security analyst, a communications consultant, a safety consultant and two interns.

## Planning and budgeting

Table 1 shows budget data for the Security Service, including personnel based in headquarters and at Regional Offices, but not local security personnel in field offices, by year and funding type. Funding fluctuated from 2016 to 2018, stabilizing at approximately US$ 1.6 million from 2019 to 2021. The portion of the budget funded by Institutional Budget has declined over time despite UN Women's rapidly growing presence in the field in many high-risk locations, engagement in humanitarian activities and the Security Service's expanding scope of work. A large portion of the Security Service budget is funded by a security reserve under UN Women control that is generated through a charge of 2.5-3.5 per cent of staff payroll costs.

***Table 1 – Security Services budget allocations and funding types by year[1]***

| Type | 2016<br>Budget ($) | 2017<br>Budget ($) | 2018<br>Budget ($) | 2019<br>Budget ($) | 2020<br>Budget ($) | 2021<br>Budget ($) |
|---|---|---|---|---|---|---|
| Reserves | 1,695,620 | 1,970,000 | 736,486 | 947,420 | 1,354,312 | 1,302,529 |
| IB | 372,608 | 1,298,188 | 449,373 | 666,982 | 265,213 | 265,213 |
| **Total budget** | **2,068,228** | **3,268,180** | **1,185,859** | **1,614,402** | **1,619,525** | **1,567,741** |
| Expenditures: | n/a | 1,174,635 | 1,119,941 | 1,288,547 | 1,199,107 | 1,352,241 |
| Including charge to the reserve | n/a | n/a | 734,403 | 735,367 | 893,341 | 1,043,156 |

In addition to the Security Service's budget, security funding comes from both headquarters and field office levels. At the headquarters level, funding covers the Security Service, UNDSS annual fees (US$ 1 million in 2019 and US$ 1.4 million in 2020), the Jointly Financed Activities contribution for UN Women core personnel and financial support to field offices through Security and Safety Compliance Enhancement Funding. At the field level, security-related resources are funded through cost-share budgets and UN Women specific costs including the Entity's contribution to Jointly Financed Activities for non-core project personnel.

Organizational security costs are funded by Institutional and Core Budget, Extrabudgetary and direct project costs (see Table 5).

The Security Service budget includes an "Operational Budget" portion which is used to provide emergency funding support to UN Women offices on a one-off basis. Offices apply for funding through the Security and Safety Compliance Business Process, with specific criteria for approving funding requests.

## Field office risk management

At the country level, security risks are identified through the UN system-wide Security Risk Management Process (SRM) which is approved by Heads of Agency and the Designated Official for Security in each location. In all 142 locations where UN Women operates there are multiple SRM processes that detail security risks and specify mandatory measures to reduce security and safety risks to UN Women personnel, premises and assets. In all these locations, Regional Security Specialists contribute to

[1] Source: Atlas Enterprise Resource Planning System, November 2021.

the SRM process, and support UN Women personnel and management at the country level to implement measures to reduce risk. UN Women also makes use of an internal enterprise risk management system, which includes a high-level security risk for each office.

Work planning process and time reporting

The Global Security Adviser (Head of Security Service) develops an annual workplan and budget with extensive input from Security Service team members, who also consult with the regional and field offices under their area of responsibility to assess security and training needs. The workplan and budget are then submitted to DMA senior management for review and approval. Documents are then submitted to the Strategy, Planning, Resources and Effectiveness Division (SPRED) for further review, ELT approval and funds allocation.

***Table 2 – Security Services work planning outputs and funding for 2021 (in US$)[2]***

| Output[3] | Description | IB | Reserve | Non-Core | TOTALS |
|---|---|---|---|---|---|
| 1.1 | Organizational Security Compliance within UNSMS | 250,000 | 125,000 | 100,000 | 475,000 |
| 1.2 | Maintenance of UN Women Security Mainstreaming Process | - | 35,000 | - | 35,000 |
| 1.4 | UN Women Mandate Advocacy through participation within the Inter-Agency Security Management Network and other UNSMS platforms | - | - | 31,000 | 31,000 |
| 1.5 | Provision of UN Women proactive and reactive security advice and support | 265,213 | 744,617 | 120,055 | 1,129,885 |
| 1.6 | Provision of Organizational Resilience Management and Business Continuity | - | 264,864 | 20,000 | 284,864 |
| 1.7 | Provision of Occupational Health and Safety | - | 184,314 | 20,000 | 204,314 |
| | **TOTALS** | 515,213 | 1,353,795 | 291,055 | 2,160,063[4] |

*Source: Annual Workplan 2021, Resource Management System, February 2022*

The Security Service has tracked its workload outputs since 2016, as shown in Table 3, covering security, occupational safety and health, business continuity and crisis management, and others. The workload recorded does not include a field for the six outputs in the team's annual workplan; therefore, IAS could not assess how much of the workload relates to security versus other roles.

***Table 3 – Security Services workload data analysis by year and number of outputs[5]***

| Year | 2016 | 2017 | 2018 | 2019 | 2020 | 2021 |
|---|---|---|---|---|---|---|
| Assessments | 48 | 60 | 68 | 471 | 1,181 | 580 |
| Missions | 46 | 56 | 49 | 79 | 16 | 23 |
| Documents reviewed | 52 | 265 | 360 | 1,047 | 2,732 | 1,252 |
| Training and educational sessions delivered | 46 | 146 | 157 | 251 | 511 | 289 |
| Personnel attended educational sessions | 484 | 1,786 | 1,771 | 2,424 | 15,606 | 6,225 |

The data shows an increase in the number of activities taking place each year from 2016 to 2021. There is a large increase in 2019, with an even larger increase in 2020 and 2021 due in part to the COVID-19 pandemic. Despite this, the budget for the Security Service has stayed at roughly the same level over the period, or even slightly declined. Data accuracy could be enhanced if outputs were validated by supervisors on a periodic basis to avoid issues with data quality, especially in cases of spikes in recorded work tasks.

# III. AUDIT OBJECTIVES, SCOPE AND METHODOLOGY

The audit objectives were to assess the effectiveness of security management in the organization, with focus on the following key areas:

A. **Governance:** policy, organizational structure and positioning, resources, roles and responsibilities and organizational security culture.

[2] Resource Management System, February 2022.
[3] There was no Output 1.3 included in the work plan.
[4] Reportedly, the difference in total budget between the data for 2021 in RMS and in the Project Delivery Dashboard represents the planned versus allocated budget.
[5] Source: Security Service self-reported workload planning and scheduling tool, as of June 2022

B. **Security risk management:** security activities, controls and risk management including identification, mitigation, risk escalation protocols, and monitoring of key risks, including monitoring of residual risk.

C. **Security operations:** functions supporting security service provision.

D. **Oversight and monitoring**: security compliance and policy effectiveness.

The audit did not plan to cover occupational health and safety or business continuity and crisis management. While these areas are also the responsibility of the Security and Safety Service, they are topics in their own right and would require their own audit.

The audit work consisted of reviews of documents and systems, and interviews and discussions with personnel at headquarters and in Regional Offices. IAS also conducted benchmarking of good practices across UN agencies. As part of the audit, IAS administered an anonymous survey to Representatives and Heads of Offices in UN Women, with 26 responses received.

IAS also used its Summary Report on Meta-Synthesis of Results from Field Office Audits to consolidating its findings on security management observed during field audits.

IAS followed the *International Standards for the Professional Practice of Internal Auditing* in conducting this audit.

# IV. AUDIT RESULTS

## A. OVERALL ASSESSMENT AND ACHIEVEMENTS

This audit recognizes that the UN Women Security Service in headquarters has certain roles, responsibilities and parameters to ensure the effectiveness of security management. However, security management is effective only if all the responsible parties and executive management adequately manage the security risks at all levels of the organization, and timely and proper actions are embedded into all processes. While the Security Service has a responsibility to oversee and advise executive management, the audit did not only focus on the Security Service's work, but also covered other roles and processes that should contribute to effective security management.

Based on its review of governance, risk management and internal controls, IAS assessed Some Improvement Needed in security management in UN Women. The Security Service team has established a reasonably sound and effective control mechanism in addition to providing timely and efficient support to field offices whenever required, despite having limited resources.

IAS acknowledges the support of the Security Service team during the assignment and notes the following positive aspects and satisfactory controls:

- There is a strong UN-wide policy framework effectively leveraged by UN Women security experts (Security Service). Overall governance of security at UN Women follows the United Nations accountability framework.
- The Security Service developed a business continuity and crisis management app (BCCMA), which will help to solve long-running issues with business continuity and crisis management maintenance, tracking and dissemination of important security information to all personnel. One relevant piece of individual feedback from stakeholders surveyed about the app was that its roll-out could have been more consultative, targeting a wider range of users such as those who do not normally engage with these topics. To address this, the Security Service developed internet training and promotional material in various formats and offers training on the app when visiting field locations. Nonetheless, stakeholders interviewed generally considered roll-out of the app to be successful (although it is still ongoing) and its "self-service" and user-friendly model means that personnel are able to engage with the app in their own time and at their own pace. The total budget allocated to the activity in the 2021 annual workplan was US$ 5,000 from the reserve, with annual maintenance costing US$ 35,055.
- The Security Service complies with corporate requirements for work planning and operations and develops its outcomes based on security requirements. The Security Service tracks its workload outputs, indicating a large workload despite being a small and resource-stretched team. Four Regional Security Specialists cover six regions and 142 locations, some of whom are responsible for multiple regions across wide time zones.
- The Security Service developed and monitors the annual security compliance survey at UN Women, covering 142 locations.

In addition, a survey conducted by IAS during the audit found strong support for the Security Service and its security mandate throughout the organization. The team has been recognized as hard-working and professional, covering a large area of responsibility with limited resources. Importantly, the Security Service also represents the organization and its interests, including gender mainstreaming, in the Inter-Agency Security Management Network, participating in numerous working groups.

The audit notes some improvement needed with respect to the Security Service's positioning, authority and reporting lines. There is also a need to improve corporate attitudes and attention to security management as a critical priority for UN Women. Fully acknowledging the good work undertaken so far, the sections below provide detailed observations and recommendations to advance security management to a higher level of effectiveness.

## B. GOVERNANCE

### Observation 1: Security policy, roles, responsibilities and reporting lines

UN Women does not have its own security and safety policies, relying instead on the

UNSMS Security Policy Manual and Security Management Operation Manual.

The Security Service developed a two-page brief entitled, UN Women Security Framework of Accountability which explains key security roles described in the UNSMS Security Policy Manual as applicable to UN Women. While technically a brief and not a policy, this is an important document, which could be expanded. Elevating the framework to a formal policy would improve the authority, awareness of roles and individual management accountability and appreciation of security at UN Women. Additional information could also be added to the policy, as this observation will discuss. Ideally, the Security Service needs a separate policy (e.g. similar to the IAS charter) accompanied by an organization-wide security strategy and workplan (see Observation 2).

Most information required for the policy is already available from different sources: the Security Service intranet site explains the team's roles and provides guidance on topics including: personnel responsibilities; security risk management; occupational safety and health; business continuity and crisis management; gender considerations; security and safety education and mainstreaming; compliance; incident management; and other guidance such as country security budgeting.

While not in the audit scope, IAS noticed that the Security Service's responsibility for business continuity and crisis management, and occupational safety and health is also not formalized in policy. The Security Service team recently reworked the business continuity and crisis management policy and guidance into a mobile app that all UN Women personnel can access and use. The Security Service has also engaged a consultant to devise an occupational safety and health approach and policy framework for the organization.

While the role of Executive Director and Global Security Adviser (Head of Security Service) are included in the Security Framework of Accountability brief, the authority of the Security Service as a business process owner and accountability of other key players contributing to effective security management should be codified and expanded where needed in an official policy. For example, in addition to the oversight role of the Security Service and its regional advisers, the roles of Regional Directors, Regional Operations Managers and their offices in overseeing security risk management in the Country Offices in their regions ("the second line of defence") should be clearly defined, especially with regards to crisis management events (who does what when and how).

The UN Women Framework of Accountability does not mention the role of the "Designated Official". This is a critical role discussed within the UNSMS Security Policy Manual and while the definition is clear in that document, despite being mentioned several times, the role is not clear in relation to UN Women country management in the UN Women Framework.

The role of individual managers of offices and units ("the first line of defence") should be listed, including risk owners who directly deal with security risks and are responsible for complying with security measures. The policy should also include key security compliance controls, e.g. non-delegable attendance at the UN Security Management Team meetings and related training (IAS found that this was not always the case); individual accountability for validating the accuracy of annual certification of security compliance for field offices (see Observation 5 for non-compliance with training, etc); and mainstreaming security into strategy planning, programming and budgeting accordingly to ensure that UN Women collectively supports the Executive Director in fulfilling her responsibilities.

The UNSMS Security Policy Manual states that the "Senior Security Managers and/or Security Focal Points at Headquarters" (Global Security Adviser in the UN Women context) "advise the Executive Head and senior management on security matters and keep them updated on security management issues". However, the organization chart does not reflect this. Instead, the UN Women Global Security Adviser reports to the Deputy Director, DMA, who in turns reports to the Director, DMA, who reports to the Deputy Executive Director for Resource Management, Sustainability and Partnerships. There is no formal direct line of reporting to the Executive Director, which could potentially affect the Security Service's authority and access to executive leadership (noting that as of yet no specific issues have apparently arisen from the current arrangement). Reporting lines could also be better explained in a security policy including direct access to the Director, DMA and through them timely access to the Executive Leadership Team.

There is no mention of the concept of duty of care in the UNSMS Security Policy Manual. IAS understands that the matter is subject to considerable discussion about how best to treat the issue within the UN system and how it should be covered in occupational safety and health protocols.

The Security Framework of Accountability brief does not discuss the nature, extent and use of security budgets (see Observation 4). Much of this information is available in the form of general guidance via the Security Service's intranet page, but not officially in policy (in the Policy, Procedure and Guidance [PPG] system). Key information is missing, including the purpose of the security reserves, how security reserve funds are accumulated and the basis upon which they are allocated and spent. There is also no explanation of how such information is to be reported to senior management. See also Observation 4 on budget.

Lastly, there is no UN Women PPG to address personal expense reimbursement for security or business continuity charges incurred by individuals, sometimes heads of offices with budget approval authority. This is also not addressed in the UNSMS Security Management Operation Manual or the UNSMS Security Policy Manual. Currently, reimbursement of expenses is made via the F10 claim form or direct charges (through purchase orders or non-purchase order vouchers). There have been instances in which the person claiming the reimbursement is also responsible for its approval.

Prior to COVID-19, IAS found instances where the internet fees of the Head of Office's private residence were claimed and reimbursed on the basis that they were related to security and business continuity. This may not represent best value for money and if such charges were not authorized by the Security Service as a business process owner, this gap in certifying the validity of their own personal charges might lead to situations where potential waste or misuse of official resources could occur or not be detected in a timely manner. Therefore, for certain situations and thresholds, IAS recommends including guidance on how security funds can be accessed for reimbursement of security-related personal expenses.

Other agencies have separate security policies that cover key security topics relevant or unique to the organization's context that may not be covered in the UNSMS policy, including recognizing the authority and role of their security office as a business process owner and defining roles and accountability of other players. They also describe reporting lines, risk management and organizational structure, budget and other requirements. UN Women could take a similar approach with a focus on brevity and principles, including the minimum necessary information, much of which is already available on the Security Service's intranet page.

### Recommendation 1 (High):

The Global Security Adviser to consolidate available information into an official policy on security management, including:

(a) Clearly defining the authority of the Global Security Adviser to act as a fully-fledged business process owner with timely access to the Executive Director.

(b) A role for Regional Offices in terms of overseeing security risks and ensuring compliance with key security controls.

(c) Expanding and clarifying the Head of the Office role, including individual accountability with key expectations for successful performance in terms of complying with key security controls.

(d) Defining key principles for governing security budget management including the authority of the Security Service team to validate the appropriateness of security expenditure and personal charges.

(e) Reference to the concept of duty of care.

## Observation 2: Security strategy and work planning

UN Women does not have a security strategy that correspond to its business needs, strategies and interventions. Some stakeholders interviewed by IAS mentioned that UN Women is not always equipped to operate in crisis situations where security requirements increase and there is no workflow to discuss the requirements at strategic level and take informed decisions on local presence and related interventions. A corporate security strategy based on end-to-end risk assessment would define the security profile of the Entity vis-à-vis strategic priorities in the field and address institutional gaps and misalignments to ensure that the strategy of "no programme without security, no security without resources" is fully embedded into organizational processes and culture.

While country-level risk assessments are very detailed, an organization-wide end-to-end security risk assessment that informs UN Women's overall security strategy has not been performed. Much of the work relating to a security strategy happens at the UN-system level via the Inter-Agency Security Management Network, Security Management Teams, and UNSMS Policy and Operations Manuals which are quite generic and do not focus on UN Women's specific context. Therefore, a risk assessment of the end-to-end security management process and elements such as governance, communications, oversight and others would demonstrate the specific needs, challenges and a security posture for UN Women at both the corporate and field office levels and would provide a solid basis for developing the security strategy.

While the Security Service team has established annual workplans with six key outputs (see Background), the workplans do not always capture the "hidden" responsibilities of the Security Service. Mapping of outputs and activities needs to better visualize the team's work on advocacy, gender security policies, education, etc. See also Observation 3 on security personnel.

## Recommendation 2 (Medium):

The Global Security Adviser to:

(a) Perform an end-to-end risk assessment of security management vis-à-vis business needs, to inform the development of a UN Women security strategy.

(b) Develop a security strategy based on needs, risks, opportunities, good practices and lessons learned, establishing high-level priorities (where we need to be), ways to achieve them (how we are going to get there) and the resources needed.

(c) Map existing responsibilities against capacity (see Recommendation 3).

## Observation 3: Security personnel

Security personnel at UN Women

As mentioned in the Background, security personnel at UN Women are based at headquarters, Regional Offices and field offices. The Security Service includes five international professionals, one local national officer, four consultants and a security analyst. The team has also previously had support from a UN Volunteer (but the position expired) and may be supported by one or more interns at a given time.

The head of the Security Service has a deputy; however, this role has not been formalized in policy. There are four specialists in total, each of these four specialists is responsible for more than one region or area – one for ESARO and WCARO, one for ROAS and APRO, one for LAC, headquarters and occupational safety and health, and one Global Security Specialist - for ECARO and business continuity and crisis management. Each specialist has a large area of responsibility that can be difficult to manage, despite their expertise and work ethic.

An additional five security personnel are based in field offices and report to field office leadership: one in Afghanistan (P3), one in each of Haiti (SB3), Jordan (G6), Mali (G6) and Uganda (G6). Daily security management is assigned to personnel in the field offices in addition to their main responsibilities. Emergency deployment of Security Service headquarters personnel takes place when needed, including for example Afghanistan in 2021, Haiti and Ukraine in 2022.

The Security Service has benchmarked security personnel across UN entities. Based on their analysis, UN Women has the lowest number of security personnel compared to the Entity's physical presence and number of personnel. The need for security personnel in UN Women should be assessed at country, regional and headquarters levels compared with a possibility of co-sharing security services with other UN entities as part of UN reform implementation and to optimize reliance on UNDSS (see also Observation 7). It is important to note that no UN entity, except UNDSS, is mandated to perform security functions for another UN entity as this entails a range of legal and complex obligations. Full outsourcing cannot necessarily be relied upon in all cases.

UN Women has not finalized a functional analysis of the security management function to understand the Entity's security needs and the necessary and available human resources to meet those needs. This is an important accompaniment to a UN Women security strategy and end-to-end risk assessment (see Observation 2). A functional analysis of DMA, which includes the Security Service, was conducted in 2019, recently updated and was submitted to the Executive Director for approval.

Recruitment and reporting lines of field security personnel

Security personnel embedded in field offices (apart from the Regional Security Specialists) fall under the responsibility of the Head of Office, without any matrix/dual reporting to the Security Service. However, the Security Service does provide leadership and technical guidance to local security associates and coordinates with them on security matters.

Funding and recruitment of security personnel is handled locally, except in situations such as Ukraine in which headquarters-based crisis teams may mobilize temporary support. If a field office needed a dedicated security function, it would generally be the office's responsibility (via their Representative, Deputy, Operations Manager, etc.) to identify the need, ensure it is properly funded (whether core or non-core), secure the necessary approvals, complete the recruitment process and onboard the successful candidate.

There is no formal requirement for the Security Service to review terms of reference, job advertisements, be part of selection panels, validate best candidates, contracts, or workplans of security personnel in field offices; however, in general, the Security Service is included and has participated in some of these tasks when asked. This could be made a formal requirement to further ensure proper selection and coordination of field security personnel. Having a smaller team, virtually connected to the qualified network of local security personnel or focal points would improve cost-effectiveness. The Finance Management Section had a similar journey where it enhanced its capacity and support based on involvement in recruitment and reporting lines (including dual reporting lines for many field colleagues).

Security personnel needs analysis

The Security Service has a strong understanding of UN Women's security needs, but no overarching quantitative analysis of security needs or functional analysis of the Security Service has been conducted to ensure that all expected responsibilities are fully covered by qualified and sufficient security personnel, where needed, from non-core funding.

IAS analysed security needs based on personnel head count. While head count may not reflect the true security needs of an office, it indicates the size of the office and one scope of "what could go wrong" in a security context, in terms of personnel's security and safety.

*Table 4 – Security personnel at UN Women by region, including the Security Service*[6]

| Region | Other personnel | Dedicated security personnel | Total | % Security |
|---|---|---|---|---|
| LACRO | 605 | 1 | 606 | 0.2% |
| ROAS | 317 | 0.5 | 317.5 | 0.2% |
| APRO | 679 | 2.5 | 681.5 | 0.4% |
| ESARO | 452 | 2 | 454 | 0.4% |
| ECARO | 345 | 1 | 346 | 0.3% |
| WCARO | 317 | 1 | 318 | 0.3% |
| Headquarters | 652 | 3 | 655 | 0.3% |
| TOTAL | 3367 | 11 | 3378 | 0.5% |

Moreover from the risk level perspective (both self-reported and based on UN-wide risk analysis), the following offices have been rated as either Very High or High risk in past IAS annual risk assessments: Afghanistan, Bangladesh, Ethiopia, Haiti, Iraq, Mali, Myanmar, Nigeria, South Sudan and Uganda. In addition, Somalia, Libya and Yemen have been rated as having higher security risks. Based on the above data only 5 of these 13 offices have dedicated security personnel (to note that in three countries (Somalia, Libya and Yemen) with high security risks, UN Women does not have large presence).

While mainly programmatic in its scope and focus, the 2021 Evaluation of Crisis Response in Asia and the Pacific found that UN Women needs more personnel with crisis response capacities at different levels of seniority to support crisis response and avoid burnout and current personnel in crisis prone countries may not have adequate capacities in crisis response, and reliance on non-core funding and less stable contract modalities results in turnover and loss of institutional memory and affects UN Women's ability to ensure duty of care. The evaluation highlighted the importance and need for such personnel above what is currently available in UN Women (in the Asia Pacific region).

[6] Source: OneApp HR Database, March 2022.

Workload

The audit found that the Security Service has a good reputation among regional and field offices for providing professional and reliable support. This is supported by an audit survey and interviews with various stakeholders in the organization. The team's output tracking contains a large amount of work for a small team (which is also illustrated by the Regional Security Specialists covering multiple regions, while other UN entities specialists cover just one, or have a team of advisers at the regional level). The Security Service manages the situation through hard work and workload planning, but there is very little room for adjustment, particularly when managing leave and turnover. When personnel depart UN Women for other roles, the Security Service is left in a very challenging situation.

### Recommendation 3 (Medium):

The Global Security Adviser to finalize functional analysis of the security function at UN Women to understand current versus needed capacity to implement the security strategy (see Recommendation 2). The identified capacity gap should include a costing and proposal for potential funding from the security reserve, and a proposed mechanism to fund extra capacity from non-core funding (as this will mainly represent incremental support to the high-risk offices implementing the field programme).

### Recommendation 4 (Medium):

In the security policy recommended by this audit (see Recommendation 1), the Global Security Adviser to include a provision to review the terms of reference and selection process of security personnel hired by field offices and broaden its global security network similar to the Finance Management Section's Virtual Global Service Centre.

## Observation 4: Security budget management

As per the 2016 report by the Joint Inspection Unit entitled Safety and Security in the United Nations System, "the hybrid nature of the budget sources and their inherent lack of flexibility do not support a United Nations security management system that is based on structured risk analysis and designed to respond in a timely manner to crisis through the rapid redeployment of commensurate human or financial resources."

Security budget policy

There are no specific security budget-related provisions in the UN Women Financial Regulations and Rules, the Cost Recovery Policy or other PPG related to security. The cost recovery policy and accompanying guidance provide the general framework for recovering direct costs, as applied to all activities including security under the overall principal that core funding should not subsidize non-core funding. The Cost Recovery Policy states "In the past, the institutional budget has funded the UN system-wide security services. The cost of security has now increased exponentially over the years due to organizational expansion, growing security concerns and the development of associated UN security policies and systems together with the organizational resilience. The high costs and the strict security requirements imposed on all staff, including project personnel, have necessitated the recovery of security costs from all funding sources as direct project costs." It does not explain the process through which security costs are budgeted and recovered (see also Observation 1).

Security reserve

UN Women has a Security and Safety Compliance Enhancement Fund, a reserve for "budgetary allocation to assist field office raise [security] compliance levels." The UN Women intranet states that the Security and Safety Compliance Enhancement Fund pays for "one-time" security costs rather than day-to-day funding. The reserve is funded by charging a percentage on top of monthly payroll of personnel.

The security reserve accrual (account 23003, fund code W0903) rate decreased from 4 per cent for staff and 5.5 per cent for service contractors in 2019 to 2.5 per cent for staff and 3.5 per cent for service contractors in 2020. Every year, the balances under the different harmonized reserve rate activities are reviewed by Budget and rates adjusted to accommodate the requirements. The explanation for this change, which was made within DMA, was not formally communicated to DMA. Desk review of the W0903 fund code found that the expenses recorded there appear reasonable in nature and are related to security.

***Table 5 – Security reserve (fund code W0903) and other security expenditures [7]***

| | **Reserve and Expenditures elements[8]** | **2019** | **2020** | **2021** |
|---|---|---|---|---|
| 1 | Accrual rate charged against payroll | 4% for FTA and TA; 5.5% for SC | 2.5% for FTA and TA; 3.5% for SC | 2.5% for FTA and TA; 3.5% for SC |
| 2 | Reserve roll-forward[9] | | | |
| 2.1 | Accrued security cost opening balance (account 23003, fund code W0903) | 3,440,213 | 4,299,509 | 4,012,763 |
| 2.2 | Additions (Payroll journals applying % from #1) | 2,683,448 | 2,584,878 | 2,238,253 |
| 2.3 | Deductions (General ledger journals), including: | (1,824,152) | (2,871,624) | (2,794,142) |
| 2.3.1 | Security Service expenses charged to reserve balance (table 1) | 735,367 | 893,341 | 1,043,156 |
| 2.3.2 | Other Deductions | 1,088,785 | 1,978,257 | 1,750,986 |
| 2.4 | Accrued security cost closing balance | 4,299,509 | 4,012,763 | 3,456,875 |
| 3 | Other corporate security expenses (excluding Reserve and Security Service) | 4,191,836 | 3,983,648 | 3,731,782 |
| 3.1 | Core | 1,061,156 | 964,666 | 790,568 |
| 3.2 | Extrabudgetary | 251,260 | 272,813 | 280,829 |
| 3.3 | Institutional Budget | 395,271 | 387,746 | 537,124 |
| 3.4 | Non-Core | 2,484,149 | 2,358,423 | 2,121,772 |
| 3.5 | Regular Budget | 0.00 | 0.00 | 1,489 |

Based on the key security reserve and expenditure figures in Table 5:

- Neither the accrual rate nor the basis for the decrease in accrual rate from 2019 to 2020 is codified in policy (Row 1).
- While large accruals are raised each year under the security fund code (Row 2.2), the actual total expenses incurred under the same code is far lower (Row 2.3).
- Despite the point above, comparatively large security-related expenses are being incurred under other funding codes (Row 3), including core and Institutional Budget.
- Only some part of charges to the Reserve are overseen by the Security Service as a business process owner (Row 2.3.1).
- The accumulated reserve may not be fully utilized for the purposes for which it was originally created. While the accrual is increasing due to charges against payroll that increase office costs, the same offices might also incur security costs under core and IB funding types.

The audit found a lack of clarity (in the form of PPG) on how the reserve is managed; who has authority for managing it; governance procedures; and use of the reserve versus other funds. In support of the principles of transparency, accountability and prudence, the audit recommends that formal clear principles at the policy level are developed that define how funds are accumulated, and how they can be used, reconciled and reported on to senior management for decision-making. It could also define how changes to the policy should be made (as part of implementation of Recommendation 1).

Table 5, Row 3 and its breakdown shows that, to date, security expenses have been funded mainly through non-core programme budgets (3.4), extrabudgetary funds (Row 3.2), core funds (Row 3.1) and Institutional Budget (Row 3.3). Country Office core and Institutional Budget funding is already limited and should not be used for security costs especially if the organization has been already “taxed” for the security reserve, the main purpose of which it to ensure sufficient funding for volatile situations.

Total security funding and expenditure should be consolidated and reported on an annual basis to senior management to oversee investment in security and to support

[7] Source: Atlas Enterprise Resource Planning System, April 2022.

[8] This data does not include commitment control encumbrance amounts. Within the overall balance, UN Women ensures that there is an operational balance to fund 6 months of security reserve funded posts to address any natural fluctuations in the reserve accrual. Year end balances inform the current and subsequent years’ financial projections to ensure sustainability of commitments.

[9] Reserves include Security Service funding.

informed decision-making on security. In 2019-2021 security reserve yearly additions and annual expenditures were between US$6.9 million and US$6 million (Table 5, Rows 2.2 and 3), which IAS considers material for UN Women.

Other observations regarding security budgeting include the lack of strategic dialogue within headquarters analysing the global programmatic footprint and the necessary security considerations arising from it. While the guidance on security cost budgeting is incorporated in the security mainstreaming process and manual, it is not implemented regularly by programme personnel leading to underbudgeting of security costs and increasing security risks for planned interventions. New guidance on developing Strategic Notes includes instructions to address security needs. Any project-related security costs must be embedded in project budgets at the project formulation stage, again following the strategy of "no programme without security, no security without resources" (See Observations 1 and 2). Checking and budgeting a security feasibility for the planned interventions is not always the case in current project life cycle design, formulation and approval processes, which later becomes an implementation problem with regular or reserve funding often used as a backstopping measure.

Overall, UN Women experiences strong cost pressures on security. Year on year, the Security Service has experienced a small reduction in budget (see Table 1), which is in contrast to the expansion of UN Women programmes, premises and personnel numbers over the same period. The budget team maintains that the goal in situations such as this is to cost share security services as much as possible in the field, pooling resources with other UN entities. This happens in some cases where UN Women shares common premises, but this means to rely on the existence of a strong commitment from other UN entities with a larger security presence and support, which has traditionally been met with reluctance. The Security Service maintains that there are key challenges in cost sharing security, such as the unwillingness of other entities to be accountable for UN Women security. This could be one of the elements to include in Business Operations Strategy implementation in countries, including service level agreements or customer satisfaction principles signed by individual agencies.

## Recommendation 5 (Medium):

The Director, DMA with support from the Global Security Adviser and Budget Section to:

(a) Develop formal guidance, and policy provisions where applicable, defining how security funds are obtained and used, and how changes to the guidance should be made.

(b) Develop a mechanism for consolidating information on all security funding and spending, and report on it annually to senior management.

(c) Consider appointing Security Service as a coordinator to oversee the cost-effectiveness of security-related budgets and spending.

(d) Consider how to better ensure project-related security costs are embedded in project budgets at the project formulation stage.

## Observation 5: Security training and culture

The 2016 report by the Joint Inspection Unit entitled Safety and Security in the United Nations System notes "a culture of safety and security is the cornerstone of any security system; it provides a common understanding of the importance of and need for safe and secure operating environments. A security culture helps to develop alertness and understand the different contexts and security implications of the work undertaken by United Nations personnel where security is not seen as an obstacle but as an enabler. A security culture can be established through the appropriate induction and training of personnel at different levels, by maintaining awareness through regular practice and relevant information-sharing, by promoting best practices and by ensuring compliance with pertinent policies and security measures approved at the local level."

Overall, IAS believes that security awareness and culture in UN Women needs to be enhanced to move from a compliance culture of ticking boxes to the proactive risk management of security risks to enable the Entity's programme and operations and ensure its personnel and assets are protected.

Training

IAS analysed the effectiveness of training and communications. Security policies are socialized through direct mandatory training, train-the-trainer events, online guidance (intranet written guides and explanations), missions to field offices by the Security Service, security briefings, ongoing day-to-day work of Regional Security Specialists, updates and announcements from executive and senior leadership, the new Business Continuity and Crisis Management App (BCCMA), and the annual security compliance survey process and monitoring.

UNDSS and country UN Security Management Teams are responsible for local security briefings. As the UN Women policy framework is adopted from and aligned with the UNSMS and UNDSS frameworks, UN Women benefits from additional socialization through engagement with UNDSS at the field level. Key security risks may be discussed at UN Women senior management team meetings (but there was not much evidence of this) and via the country-specific UNSMS and Security Management Team network and meetings.

UNDSS developed the BSAFE mandatory training course, which is available to all UN entities in seven languages. BSAFE training was introduced and made mandatory for all UN Women personnel (including staff, consultants, contractors and others) from 18 November 2018. The responsibility to oversee corporate compliance with BSAFE is not clearly defined, with individual compliance delegated to individual personnel and their supervisors. BSAFE is available to UN Women personnel via the Agora online training system and also via UNDSS. UN Women does not manage or have control over it. Some users have reported issues in using it effectively.

As of November 2021, there are 3,605 active personnel in UN Women and Agora system data of active personnel showed that 1,979 of them had completed the training at that time (55 per cent). However, IAS would like to qualify that available data on different platforms on security training completion might be inaccurate or incomplete. Still, these statistics indicate that not all personnel have completed their mandatory BSAFE training, including some personnel categories (fixed-term staff and service contractors) expected to work from offices and engage in official missions. Of the 1,626 active personnel who did not complete the training as per the records, 1,200 were based in the field and 426 were based at headquarters.

However, the annual security and safety compliance survey results show an average compliance level for offices of greater than 95 per cent. The survey includes questions on whether “all personnel” have completed training. The security and safety compliance survey obtains a written confirmation from the head of office that all personnel have completed the training. There is an onus on the head of office to ensure the content is accurate. Such discrepancies may indicate the following:

- Offices are submitting inaccurate information in their security and safety compliance survey submissions without cross-validating it with other compliance dashboards, in this case mandatory training. This might indicate poor compliance culture.
- Headquarters, Regional Offices and field offices are unable to accurately track training completion rates and to hold managers and personnel accountable.

The audit survey results included several individual comments that asked for more training for personnel in their offices including refresher courses, regular training beyond the mandatory virtual options, more real-time training, more practical training, training on topics such as kidnapping and protests, and training for programme partners.

The Security Service organizes its training programme using a cascading approach to maximize coverage. It provides a variety of training courses, including a self-reported 251 “training and educational sessions” delivered in 2021 and 511 in 2020, but it is difficult to reach all offices and regions on a regular basis. Offices could be guided on how to devise their own local security training agenda/workplan based on their needs, including utilizing local training opportunities with UNDSS and other UN entities.

Culture

More could be done to socialize the desired security approach and risk management in the organization. This would partly be supported through a formalized security strategy, end-to-end risk management and risk appetite and tolerance definition (see Observation 2), plus regular corporate communications at the senior level. The audit would have expected to find more security-related communications from the Executive Director’s office to all personnel during the period under review (November 2019–November 2021).

There was no mention of physical security issues, indicators or analysis in the Quarterly Business Review for Q3 of 2021 (beyond brief mention of occupational safety and health). This is also true for the Quarterly Business Review Q2, 2021. In addition, Business Review Committee agenda had not discussed security management.

The lack of explicit attention to security at corporate governance meetings or review mechanisms may, in part, contribute to an organizational culture in which security is seen as a secondary issue. Efforts should be made to bring regular security messaging and indicators to the forefront; however, this alone should not be deemed sufficient. IAS observed that some security situations in the field differed from that which was reported in the annual security and safety compliance survey. In particular, there was a difference between individual reported security requirements which are validated by the head of offices and IAS' physical observations of those requirements, including security equipment (radios, satellite phones), compliance with BSAFE training and attendance at UN Security Management Team meetings. The gaps in reporting and actual status leads to false assurance that security risks are being managed while actual risks are still present. At the field office level, Heads of Offices need to formally accept accountability for security management outcomes and representations to ensure that accountability for lapses can be ascertained. This accountability framework could also be better enacted through the performance management process.

### Recommendation 6 (Medium):

The Global Security Adviser to:

(a) Include the BSAFE compliance statistics in the Quarterly Business Review statistics to improve UN Women's culture and awareness of security matters.

(b) Cross-validate some offices' security annual compliance certification with training completion data from HR.

(c) In collaboration with the Communications Section team, and as part of the security strategy, devise and implement a regular security communications protocol by senior management.

(d) Establish an accountability mechanism for field office security management for security risk management.

# C. SECURITY RISK MANAGEMENT

## Observation 6: Security risk management

Security risk management is handled at the corporate, regional and country levels both within UN Women and the broader United Nations Country Teams (UNCTs). The Security Management Team of each country's UNCT maintains a security risk management database that catalogues a long list of detailed and specific security risks impacting the country. Risks are rated along multiple axes, monitored and updated by security professionals. UN Women benefits from this strong inter-agency cooperation.

UN Women also has its own internal risk management processes, as part of the Enterprise Risk Management (ERM) framework and system. The ERM framework and risk database is applied by each field office. The database includes one standardized security risk that offices must rate and report to headquarters on an annual basis.

UN Women country level risk ratings

IAS sampled some field office self-reported risk assessments, reviewing their security risks. Of 18 field offices sampled, IAS noted 6 in which the security risk rating appeared misaligned when compared with the UNDSS security level. Myanmar, South Sudan, Iraq, Yemen, Libya and Pakistan had UN Women security risk ratings that were below the UNDSS country level (IAS notes that UN Women has a very limited presence in Libya and Yemen, which might justify the internal risk rating comparing to UNDSS security level). This may indicate a need for better review and quality assurance of UN Women security risk ratings. In addition, at least 15 field offices appeared to have no security risks in the register.

The Security Service explored the possibility of capturing Security Management Team-tracked security risks in the UN Women ERM system. However, it was decided that this may result in a potentially inaccurate duplication of work because the risks would be transferred from system to system and subjectively re-assessed by a local UN Women team, and also because the Security Management Team risk registers often have over one hundred risks per country. The proposal to rely on the UNCT risk database was ultimately not adopted, resulting in field offices generally having one security risk in the

ERM system, although some had none as mentioned above.

Corporate security risk reporting

The 2021 ERM Corporate Risk Update Report dated June 2021 includes a “Safety and Security” risk, which is owned by the Director, DMA. The risk description refers to “terrorism, targeted attacks, kidnapping, murder, robbery and accidents, riots, demonstrations, protests and civil unrest.” The risk likelihood rating is 4 out of 5 (or Likely). The risk consequence rating is 3 out of 5 (or Moderate). The overall rating is 12, Moderate. Based on the nature of this risk – including terrorism, attacks, kidnapping and murder – the consequence rating could be increased to 4 out of 5 (Severe). This would increase the overall rating to 16 (High). The report also includes risk number 2 on occupational safety and health, rating this as 15 out of 25 (high). This risk is owned jointly by the Directors of HR and DMA. There is no specific risk on crisis management or business continuity, which may reflect prevailing organizational attitudes to certain risks. It may also indicate the need for greater education on setting risk ratings.

While matters have come up in an ad hoc manner, corporate security risks have not been regularly discussed at UN Women’s Senior Management Team or Business Review Committee to ensure that senior management is aware of security challenges and related mitigating actions. Senior management can review and revise the risk ratings reported in the risk updates.

See also Observation 2 on end-to-end security risk assessment.

## Recommendation 7 (Medium):

The Global Security Adviser to enhance corporate security risk management and guide field offices in their risk assessment as follows:

(a) Accept responsibility for overseeing security-related risks in the corporate register listed in the periodic Enterprise Risk Management Report.

(b) Guide field offices in validating risks and mitigating actions with other available information, e.g. annual security compliance certification.

(c) Working with the ERM team, put in place measures to monitor and cross-validate (for consistency) country level security risks with the safety and security risks in the ERM report, and compliance certification for high risk profile countries.

(d) Ensure each field office has one security risk in the ERM system that references the more detailed Security Risk Management risk register and includes an action plan to periodically review the UNSMT risk register to ensure key risks are covered.

(e) Coordinate with existing ERM reporting, devise a mechanism for the periodic corporate reporting of key security risks at the field office level to senior management.

## Observation 7: Security support from third parties

Field security management is supported by UNDSS which is financed on a cost sharing basis by UN entities, i.e. Jointly Financed Activities. These Jointly Financed Activities cover UNDSS staff salaries and benefits as well as UNDSS operating expenses. In turn, UNDSS provides leadership, overall support and oversight for UNSMS; however, the services to be provided are not formalized in a legal or service level agreement.

UN Women does not have a bilateral agreement (or Memorandum of Understanding) with UNDSS but has made several requests that UNDSS sign one. Despite this, UNDSS invoices UN Women annually for “safety and security services.” In 2019, UNDSS charged US$ 1 million and US$ 1.4 million in 2020. The invoice does not include a detailed list of what the charges include. In addition to the above costs, UN Women contributes to common costs which include local security of shared premises which are usually charged by UNDP. Moreover, security costs include items such as local security personnel or focal points, equipment, or service contracts with private guards. In 2019 and 2020, US$ 4.2 million and US$ 4 million (respectively) were charged to security expense accounts (see Observation 4).

Without itemized billing based on a service level agreement, it is difficult for UN Women to analyse and explain differences between the fees paid and services delivered by UNDSS. In fact, there is no function overseeing this arrangement in UN Women. UNDSS services are decentralized across many offices. The Security Service is best placed to analyse this and report holistically; however, there is limited data on which to do so and nothing to compare it to in the form of a legal agreement on itemized services provided. As agreements are made at the inter-agency level, it is difficult for any one agency, particularly a smaller agency such as UN Women, to raise issues and challenge the bill.

UN Women offices assess whether any UNDSS shortfalls need to be addressed with additional internal measures. One such example is in Afghanistan where the office had to establish its own radio room because the local UNDSS office had stopped offering this service. Another example is that over the past six–seven years UNDSS has promulgated a gradual release of its safety service, as this service is not featured in any policy or General Assembly resolution. Currently safety management has been assigned to the Security Service with no additional resources provided. Safety risks might be more likely to happen and more frequent than security risks and proper policies and processes are needed to address these risks.

### Recommendation 8 (Medium):

The Global Security Adviser to:

(a) Continue to request that UNDSS sign a Memorandum of Understanding and service level agreement to define the quality and timeliness of the services it provides.

(b) Include a question on the quality and timeliness of UNDSS services in the internal UN Women annual compliance survey that, when consolidated, could be raised with UNDSS as a performance indicator.

## D. SECURITY OPERATIONS

### Observation 8: Operational support for security

The Security Service conducts official missions to perform training, security assessments and to respond to emerging crises, providing support and guidance to manage UN Women personnel and premises. Regional Security Specialists typically perform an average of eight missions per year (see workload analysis in background section).

IAS analysed travel booking times using data catalogued in the Procurement and Travel and Expense Dashboard. The dashboard records the time taken to approve the travel from the creation of a travel request to its approval date. Sometimes, the travel request is created later in the booking process, so this is not always accurate. However, Security Service travel requests took an average 10.3 days to approve. Nine of 203 travel requests took more than 14 days to approve. While 10.3 days may appear reasonable, the Security Service often travels in response to emerging crises, in which timely mission travel can be decisive. Reportedly, when the Security Service team used the ECA Regional Office Operations team to obtain tickets, the process reportedly took between 1 and 24 hours from when the request was submitted until the ticket was issued, irrespective of whether the request was submitted during working days or at the weekend.

To avoid delays, standard workflow timelines could be agreed with support provided by headquarters teams such as procurement and finance, as well as for approval signatures. If need be, this could be considered a kind of exceptional arrangement given the unique importance of the security team to the organization, as well as its need to travel at a moment’s notice.

As a side note, in 2019, IAS conducted an audit of travel management which was rated as Major Improvement Needed in both its effectiveness and efficiency. However, most of the recommendations arising from the audit have not been implemented due to lack of resources and initial investment in enhancing the travel management process and oversight function.

### Recommendation 9 (Medium):

The Director, DMA, to streamline an internal workflow between the Security Service and supporting functions, such as travel, particularly in deploying security missions which may require 24 hours turnaround. As part of this, key performance indicators could be established and tracked. In addition, contingency protocols could be established including the use of Regional Offices or self-ticketing.

### Observation 9: Security and safety equipment

Security equipment is used by offices to protect personnel and premises, including armoured vehicles, personal protective equipment (PPE), radios, satellite phones and other items. Offices are responsible for procuring their own security equipment. Related to security, the organization has a large amount of safety equipment (e.g. first aid, fire extinguishers, alarms, etc.), which represents a significant responsibility for the Security Service and may require additional resources to effectively manage them.

The Security Service does not have the capacity to proactively seek out all security-related procurements and support them, and there is no requirement for it to do so. If asked, the Security Service provides expert advice on security procurements. The team relies on its network of Regional Security Specialists to be aware of any important security procurements under way. Regional Security Specialists could review annual field office procurement plans to look for security procurements. Moreover, Heads of Office must attest to the content and submission of any security compliance elements; however, there is no consequence if it is found that submissions are incorrect.

The Security Service manages the annual security compliance survey process. This includes five questions on security equipment covering: emergency power supply; emergency food, fuel, water, medical, sanitary and shelter supplies; individual emergency bags; personal protective equipment; and security personal protective equipment (body armour, helmets, etc.). This is considered the minimum necessary security equipment for field offices to have. Some offices have more advanced security needs including armoured vehicles. This aspect is not included in the compliance assessment. The compliance survey could include a prompt to discuss with the Security Service if any needs have not been met, or if the office plans to conduct security-related procurement, e.g. armoured vehicles.

There is no centralized list of security assets in UN Women. The asset in service report is a list of all assets, but it has no unique indicator for security assets. Understanding the list also relies on decoding the manually entered asset description for which there are no standards of entry. IAS recommends that security assets be tracked and reported on periodically at a corporate level.

### Recommendation 10 (Medium):

The Global Security Adviser, together with the Procurement function, to:

(a) Track security goods and services entries in office procurement planning and, based on risk tolerance and materiality for some procurement actions, review technical specifications for procurement of material items (potentially including a field office security equipment tracker in the procurement planning module so it is easy to filter and consolidate).

(b) Devise an accountability mechanism for the security and safety compliance survey reporting when it is found to be significantly inaccurate.

## E. SECURITY MONITORING AND COMPLIANCE

### Observation 10: Security monitoring and compliance

The Security Service is responsible for monitoring and reporting on security compliance to senior management, facilitating the security compliance business process for the organization. To achieve this, the Security Service devised a security compliance reporting and monitoring tool entitled the Security and Safety Compliance Survey (SSCS).

Each year, each of 142 locations in the organization completes the survey. It has ten categories with 128 individual questions. The Head of Office attests to and approves the content of the survey. The survey is reviewed by the Regional Security Specialists and approved by the Global Security Adviser. The data is then presented in the security dashboard and compliance rates are tracked and made available to all personnel.

Reported compliance rates are very high. The average self-reported compliance rate for 2021 was 96.6 per cent and 97.3 per cent in 2020. The rate has been higher than 90 per cent since at least 2017. In 2020, the lowest compliance rate was 83 per cent and 30 offices rated themselves as 100 per cent compliant.

As discussed in Observation 5, there is a risk that inaccurate data is reported. Offices report very high security training completion rates, yet analysis of actual training data shows the completion rate may not be as high as officially reported. IAS noted that in some offices where 100 per cent compliance was reported, several requirements had not actually been fully complied with (e.g. satellite phones, radios in the vehicles, access for disabled personnel). Cross-validation of the data submitted in the security and safety compliance survey, at least on a sample basis, could help to improve the process.

In addition, the compliance survey review process could be further formalized, retaining evidence of detailed review of specific surveys and support for the approved compliance ratings. The survey could also better distinguish between sub-offices and other physical presences that often exist within countries. It is important for the security business process owner to have an oversight mechanism for corporate security risk management, not just a compliance monitoring process.

Heads of Office attest to the completeness and accuracy of the annual compliance survey. Should it be found that the survey information is inaccurate, there could be an accountability process to ensure necessary consequences are enacted.

### Recommendation 11 (Medium):

The Global Security Adviser to:

a) Ensure that regional security specialists perform and document periodic spot checks of self-assessments so all the offices in their regions are covered, prioritizing higher risk offices.

b) Include key statistics on security compliance in the Quarterly Business Review.

# V. RECOMMENDATIONS AND MANAGEMENT ACTION PLAN

| Observation | Recommendation | Process | Responsible Unit | Priority | Action Plan | Implementation date |
|---|---|---|---|---|---|---|
| 1. Security policy, roles, responsibilities, and reporting lines | 1. The Global Security Adviser to consolidate available information into an official policy on security management, including:<br>a) Clearly defining the authority of the Global Security Adviser to act as a fully-fledged business process owner with timely access to the Executive Director.<br>b) A role for Regional Offices in terms of overseeing security risks and ensuring compliance with key security controls.<br>c) Expanding and clarifying the Head of the Office role, including individual accountability with key expectations for successful performance in terms of complying with key security controls.<br>d) Defining key principles for governing security budget management including the authority of the Security Service team to validate the appropriateness of security expenditure and personal charges.<br>e) Reference to the concept of duty of care. | Governance | Security Services | High | The new UNSMS FoA has just been completed and the promulgation of such is in the process. It is the intention of the UN Women Security & Safety Services to update the UN Women Security FoA to include the majority of the recommendations.<br>Further discussion with IAS to be completed before the action plan is instigated, noting contentious issues such as the validation of security expenditure and reference to Duty of Care, need to be clear. | December 2022 |
| 2. Security strategy and work planning | 2. The Global Security Adviser to:<br>(a) Perform an end-to-end risk assessment of security management, to inform the development of a UN Women security strategy.<br>(b) Develop a security strategy based on needs, risks, opportunities, good practices and lessons learned, establishing high-level priorities (where we need to be), ways to achieve them (how we are going to get there) and the resources needed.<br>(c) Map existing responsibilities against capacity (see Recommendation 3). | Governance | Security Services | Medium | This recommendation is agreed however, this is a monumental task and will require significant resources. A dedicated consultant will be needed to achieve this recommendation, noting that funding for 2022 has already been allocated. | June 2023 |
| 3. Security Personnel | 3. The Global Security Adviser to perform ongoing functional analysis of the security function at UN Women to understand current versus needed capacity to implement the security strategy (see Recommendation 2). The identified capacity gap should include a costing and proposal for potential funding from the security reserve, and a proposed mechanism to fund extra capacity from non-core funding (as this will mainly represent incremental support to the high-risk offices implementing the field programme). | Governance | Security Services | Medium | The recommendation is agreed and indeed, this has been completed firstly in 2019 and indeed most recently with a communicated proposal already reviewed by the Executive Director, receiving 'Approval in Principle'. The next step is a formal Business Case to be submitted to the UN Women Business Review Committee (BRC) for review and recommendation to the Executive Director for final decision, which is in preparation stage. If additional functional analysis is required, additional resources will be required to complete the additional work. | Submission to BRC for review and recommendation: October 2022<br>Further analysis: January 2023 |
|  | 4. In the security policy recommended by this audit (see Recommendation 1), the Global Security Adviser to include a provision to review the terms of reference and selection process of security personnel hired by field offices | Governance | Security Services | Medium | We concur with this recommendation and will make all efforts to implement, however, this is in the remit of Human Resources policy and thus not entrusted to Security and Safety. This will | February 2023 |

|  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|
|  | and broaden its global security network similar to the Finance Management Section's Virtual Global Service Centre. |  |  |  | require internal collaboration with HR and Security and Safety Services. |  |
| 4. Security Budget Management | 5. The Director, DMA with support from the Global Security Adviser and Budget Section to:<br>a) Develop formal guidance, and policy provisions where applicable, defining how security funds are obtained and used, and how changes to the guidance should be made.<br>b) Develop a mechanism for consolidating information on all security funding and spending, and report on it annually to senior management.<br>c) Consider appointing Security Service as a coordinator to oversee the cost-effectiveness of security-related budgets and spending.<br>d) Consider how to better ensure project-related security costs are embedded in project budgets at the project formulation stage. | Governance | DMA | Medium | UN Women management agrees with this recommendation, and the Security & Safety team will engage both with DMA, SPRED and PPID to support implementation, while recognizing that full implementation of this recommendation will require robust consultation and collaboration across teams | June 2023 |
| 5. Security Training and Culture | 6. The Global Security Adviser to:<br>a) Include the BSAFE compliance statistics in the Quarterly Business Review statistics to improve UN Women's culture and awareness of security matters.<br>b) Cross-validate some offices' security annual compliance certification with training completion data from HR.<br>c) In collaboration with the Communications Section team, and as part of the security strategy, devise and implement a regular security communications protocol by senior management.<br>d) Establish an accountability mechanism for field office security management for security risk management. | Governance | Security Services | Medium | We are not sure that the BSAFE statistics are accurate given that the stats should be drawn from multiple platforms. If Security and Safety were to complete this recommendation, it may be a duplication of work as BSAFE is a mandatory training, managed by UN Women HR and not Security & Safety Services.<br>As noted above, BSAFE data is retained on different platforms not accessible to Safety and Security, therefore cross validation will be at the least difficult to achieve, more likely impossible. Please note that the current compliance process requires the attestation by the country Representative to the contents including education and is therefore easier to validate at source.<br>We already collaborate closely with the communications section and Security and Safety is seen as an example of best practice and innovative when communicating. Indeed our latest Podcast Series is the first in UN Women and completed in collaboration with communications. | Completed |
| 6. Security Risk Management | 7. The Global Security Adviser to enhance corporate security risk management and guide field offices in their risk assessment as follows:<br>a) Accept responsibility for overseeing security-related risks in the corporate register listed in the periodic Enterprise Risk Management Report.<br>b) Guide field offices in validating risks and mitigating actions with other available information, e.g., annual security compliance certification.<br>c) Working with the ERM team, put in place measures to monitor and cross-validate (for consistency) country level security risks with the safety and security risks in the ERM report, and compliance certification for high risk | Security Risk Management | Security Services | Medium | We concur with the recommendation, noting that the UN Women Security and Safety Services has the most advanced compliance process in the UNSMS, that is being replicated by others, and therefore much of the recommendation already exists.<br>a) The role of ensuring that the risks reported through the enterprise risk management process and the related system remains with the Risk Owners and Risk Focal Points. However, security risks are overseen through the UN Women Security Compliance Process and will continue to be. | January 2023 |

| | | | | | | |
|---|---|---|---|---|---|---|
| | profile countries.<br>d) Ensure each field office has one security risk in the ERM system that references the more detailed Security Risk Management risk register and includes an action plan to periodically review the UNSMT risk register to ensure key risks are covered.<br>e) Coordinate with existing ERM reporting, devise a mechanism for the periodic corporate reporting of key security risks at the field office level to senior management. | | | | b) A recent meeting with ERM colleagues, re-affirmed that only one ERM risk should be identified by each office, this being – Safety and Security risk. As part of the revision of the risk assessment guidance, additional guidance will be provided by the ERM team to regional risk focal points, to ensure that as part of the validation process, the proper evaluation of Safety and Security risk in the unit level risk register is undertaken.<br>c) Similarly, guidance will be provided by the ERM team to ensure that the mitigation actions included in the ERM risk registers are aligned to the completion of the associated UN Women Security and Safety Compliance Business Process, and aligned to the UNSMS Security Risk Management process outputs and associated risk levels. Thus ensuring that the identified prevention and mitigation actions, include matters related to and permit the use of the UN Women Security and Safety Compliance Business Process to ascertain overall compliance, identifying risk prevention, mitigation, and funding source. The ERM and Security & Safety team will collaboratively consider the feasibility of the establishment of a joint process, to monitor and cross-validate security related risks reported under the ERM process.<br>d) Based on recommendations from UNBoA, beginning from 2023, mandatory measures are being introduced to include all the standardized risks in the ERM OneApp system and will be rated accordingly by each office; this will include the safety and security risk. Understanding that potentially, changes to security and safety 'Risk' are dependent on the fluidity of changes to the country level security and safety paradigm occurring frequently; a single risk entry will be completed, supported by the UN Women Security and Safety Compliance Business Process, which is aligned to the UNSMS SRM process outputs and adaptable to regular or frequent change. See point b) above this is the case currently and a reporting mechanism already exists for security risks. We will coordinate with ERM colleagues on how best they are able to report. | |
| 7. Security Support from Third Parties | 8. The Global Security Adviser to:<br>a) Continue to request that UNDSS sign a Memorandum of Understanding and service level agreement to define the quality and timeliness of the services it provides.<br>b) Include a question on the quality and timeliness of UNDSS services in the internal UN Women annual compliance survey that, when consolidated, could be raised with UNDSS as a performance indicator. | Security Operations | Security Services | Medium | We concur with this recommendation and indeed are and will continue to be a participant in the Inter-Agency Security Management Network Working Group on this task.<br>We will look to add this function in the 2022 review process for implementation in 2023 | January 2023 |

| | | | | | | |
|---|---|---|---|---|---|---|
| 8. Operational Support for Security | 9. The Director DMA, to streamline an internal workflow between the Security and Safety Services and supporting functions, such as travel, particularly in deploying security missions which may require 24 hours turnaround. As part of this, key performance indicators could be established and tracked. In addition, contingency protocols could be established including the use of Regional Offices or self-ticketing. | Security Operations | Security Services | Medium | We concur with this recommendation; we have previously raised this on numerous occasions and are currently discussing with DMA. We do note however, that we are a requestor and Director DMA is the decision maker and as such implementation may not be forthcoming, or leastways not in the near future as workloads are high given the new ERP system activities of DMA. We do note and have communicated these current procedures are cumbersome, restrictive, result in higher costs and impede delivery. We have indicated that field level processes appear to be the opposite, quick, enabling, cheaper and supportive, turning around a travel request in less than 24 hours. | November 2022 |
| 9. Security Equipment | 10. The Global Security Advisor, together with the Procurement function, to:<br>a) Track security goods and services entries in office procurement planning and, based on risk tolerance and materiality for some procurement actions, review technical specifications for procurement of material items (potentially including a field office security equipment tracker in the procurement planning module so it is easy to filter and consolidate).<br>b) Devise an accountability mechanism for the security and safety compliance survey reporting when it is found to be significantly inaccurate. | Security Operations | Security Services | Medium | We concur with the recommendation with regard the development, however, this is a Procurement function, and such a process will require significant resources for 142 locations. We are happy to work with Procurement in the development of a field-based equipment tracker to do this function. We confirm that we already do provide upon request specifications for equipment already as part of our Compliance Business Process, within the SSCAP Security & Safety Compliance Action Plan step.<br>The compliance process employed by UN Women is an 'Active' real time process with the results communicated to the Executive Director and Senior management team through the management 'Dashboard'. We will work with management and HR to develop an accountability mechanism for inaccurate reporting, given the already established attestation to content. | February 2023 |
| 10. Security Monitoring and Compliance | 11. The Global Security Adviser to:<br>a) Ensure that regional security specialists perform and document periodic spot checks of self-assessments so all the offices in their regions are covered, prioritizing higher risk offices.<br>b) Include key statistics on security compliance in the Quarterly Business Review. | Security Monitoring and Compliance | Security Services | Medium | Spot checks are completed during missions by the Regional Security Specialists as only face to face checks can be certain of content. We will look to add documenting such within the compliance survey process in our review of 2022 for implementation in 2023. Statistics are reported on at least a quarterly basis via the DMA report to the Executive Director presently, whilst as noted previously, the compliance process employed by UN Women is an 'Active' real time process with the results communicated to the Executive Director and Senior management team through the management 'Dashboard', updated every 24 hours. | Completed |

# ANNEX 1: DEFINITIONS OF AUDIT TERMS, RATINGS AND PRIORITIES

## A. AUDIT RATINGS

| | |
|---|---|
| **Satisfactory** | The assessed governance arrangements, risk management practices and controls were adequately established and functioning well. Issues identified by the audit, if any, are unlikely to affect the achievement of the objectives of the audited entity/area. |
| **Some Improvement Needed** | The assessed governance arrangements, risk management practices and controls were generally established and functioning, but need some improvement. Issues identified by the audit do not significantly affect the achievement of the objectives of the audited entity/area. |
| **Major Improvement Needed** | The assessed governance arrangements, risk management practices and controls were established and functioning, but need major improvement. Issues identified by the audit could significantly affect the achievement of the objectives of the audited entity/area. |
| **Unsatisfactory** | The assessed governance arrangements, risk management practices and controls were either not adequately established or not functioning well. Issues identified by the audit could seriously compromise the achievement of the objectives of the audited entity/area. |

## B. PRIORITIES OF AUDIT RECOMMENDATIONS

| | |
|---|---|
| **High (Critical)** | Prompt action is required to ensure that UN Women is not exposed to high risks. Failure to take action could result in major negative consequences for UN Women. |
| **Medium (Important)** | Action is required to ensure that UN Women is not exposed to risks. Failure to take action could result in negative consequences for UN Women. |
| **Low** | Action is desirable and should result in enhanced control or better value for money. Low priority recommendations, if any, are dealt with by the audit team directly with the management, either during the exit meeting or through a separate memo subsequent to the fieldwork. Therefore, low priority recommendations are not included in this report. |

# ANNEX 2: Roles and responsibilities for security management

The UN Women Framework of Accountability sets out the following roles and responsibilities:

1. The UN Women Executive Director is ultimately responsible for meeting the goals of UNSMS within UN Women through implementing the strategy in all UN Women programmes and activities.
2. Directors, Chiefs and Managers have oversight and responsibility for safety and security within their areas.
3. UN Women Global Security Adviser (Head of Security Section) is the headquarters security focal point for liaising with United Nations Department of Safety and Security (UNDSS) at headquarters and field levels.
4. The Country Security Focal Point is appointed by the Designated Official to the UN Country Team (UNCT), in consultation with UNDSS and the Security Management Team.
5. The UN Women Security Focal Point participates and represents UN Women in the UN Security Management Team. Usually this is the responsibility of the Head of the Office at the duty station and should not be delegated unless the Head of Office is on official leave.
6. The Country Security Management Team advises the Designated Official on all security-related matters at the duty station.
7. UN Women Security Service personnel advise and assist the UN Women Country Representative, Head of Office, the Designated Official and the UN SMS Security Adviser on their security responsibilities.
    8. Security Wardens facilitate coordination of security arrangements, information and instructions.
    9. All UN Women personnel must abide by the UNSMS and UN Women security policies, administrative instructions, plans and procedures at all times.

Specific responsibilities of the Security Section include (but are not limited to):

- Security mainstreaming – inclusion and implementation of security considerations at all levels of UN Women activities and throughout the programme cycle.
- Security risk management – identifying future harmful events that may affect the achievement of objectives; assessing them for likelihood and impact; and determining an appropriate response.
- Security advisory role – guidance to headquarters leadership, Head of Offices and Country Security Focal Points on a range of policy and operational issues.
- Gender mainstreaming – mainstreaming of gender security in policy development through participation in a range of inter-agency working groups and targeted evaluation of gender security policy provisions within UNSMS.
- Security and Safety Compliance Business Process – evaluating ongoing/current compliance status of field offices, providing an action plan and funding to enable increased compliance with country-specific requirements.
- Operational support – surge missions and rapid deployment in response to a crisis or on request, security support for high-level events and delivery of educational programmes independently or as part of inter-agency initiatives.
- Organizational resilience management – business continuity management and crisis management, planning, maintenance, testing and response regime.
- Occupational safety and health – concerned with the safety, health and welfare of people at work.

## UN WOMEN IS THE UN ORGANIZATION DEDICATED TO GENDER EQUALITY AND THE EMPOWERMENT OF WOMEN. A GLOBAL CHAMPION FOR WOMEN AND GIRLS, UN WOMEN WAS ESTABLISHED TO ACCELERATE PROGRESS ON MEETING THEIR NEEDS WORLDWIDE.

UN Women supports UN Member States as they set global standards for achieving gender equality, and works with governments and civil society to design laws, policies, programmes and services needed to ensure that the standards are effectively implemented and truly benefit women and girls worldwide. It works globally to make the vision of the Sustainable Development Goals is a reality for women and girls and stands behind women's equal participation in all aspects of life, focusing on four strategic priorities: Women lead, participate in and benefit equally from governance systems; Women have income security, decent work and economic autonomy; All women and girls live a life free from all forms of violence; Women and girls contribute to and have greater influence in building sustainable peace and resilience, and benefit equally from the prevention of natural disasters and conflicts and humanitarian action. UN Women also coordinates and promotes the UN system's work in advancing gender equality.

UN WOMEN
GENERATION EQUALITY

220 East 42nd Street
New York, New York 10017, USA
Tel: 212-906-6400
Fax: 212-906-6705

www.unwomen.org
www.facebook.com/unwomen
www.twitter.com/un_women
www.youtube.com/unwomen
www.flickr.com/unwomen